

Modicon M580

Manuale di sicurezza

Traduzione delle istruzioni originali

QGH46985.05
11/2021

Informazioni di carattere legale

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nella presente guida sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari. La presente guida e il relativo contenuto sono protetti dalle leggi vigenti sul copyright e vengono forniti esclusivamente a titolo informativo. Si fa divieto di riprodurre o trasmettere la presente guida o parte di essa, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione, o in altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

Schneider Electric non concede alcun diritto o licenza per uso commerciale della guida e del relativo contenuto, a eccezione di una licenza personale e non esclusiva per consultarli "così come sono".

I prodotti e le apparecchiature di Schneider Electric devono essere installati, utilizzati, posti in assistenza e in manutenzione esclusivamente da personale qualificato.

Considerato che le normative, le specifiche e i progetti possono variare di volta in volta, le informazioni contenute nella presente guida possono essere soggette a modifica senza alcun preavviso.

Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per le conseguenze risultanti dall'uso delle informazioni ivi contenute.

Facendo parte di un gruppo di aziende responsabili e inclusive, stiamo aggiornando i contenuti della nostra comunicazione che potrebbero contenere una terminologia non inclusiva. Tuttavia, fino a quando il processo non sarà completato, potrebbero ancora essere presenti termini standard di business che alcuni dei nostri clienti potrebbero ritenere inappropriati.

Sommario

Informazioni di sicurezza	9
Prima di iniziare	10
Avviamento e verifica	11
Funzionamento e regolazioni	12
Informazioni sul manuale	13
Funzione di sicurezza M580	15
Funzione di sicurezza M580	16
Standard di certificazione	20
Certificazioni	21
Standard e certificazioni	25
Moduli supportati del sistema di sicurezza M580	26
Moduli certificati del sistema di sicurezza M580	27
Moduli non interferenti	29
Cybersicurezza per il sistema di sicurezza M580	34
Cybersicurezza per il sistema di sicurezza M580	34
Ciclo di vita dell'applicazione	35
Ciclo di vita dell'applicazione	35
Moduli I/O M580 Safety	45
Funzioni condivise dei moduli di I/O di sicurezza M580	46
Presentazione dei moduli I/O M580 Safety	46
Panoramica della diagnostica per i moduli di I/O di sicurezza M580	48
Modulo di ingresso analogico BMXSAI0410	50
Modulo di ingresso analogico di sicurezza BMXSAI0410	50
Connettore di cablaggio BMXSAI0410	52
BMXSAI0410 Esempi di cablaggio dell'applicazione di ingresso	54
BMXSAI0410 Struttura dei dati	61
Modulo di ingresso digitale BMXSDI1602	65
Modulo di ingresso digitale di sicurezza BMXSDI1602	65
Connettore di cablaggio BMXSDI1602	67
BMXSDI1602 Esempi di cablaggio dell'applicazione di ingresso	73
BMXSDI1602 Struttura dei dati	94
Modulo di uscita digitale BMXSDO0802	98
Modulo di uscita digitale di sicurezza BMXSDO0802	98

Connettore di cablaggio BMXSDO0802	100
BMXSDO0802 Esempi di cablaggio dell'applicazione di uscita	102
BMXSDO0802 Struttura dei dati.....	108
Modulo di uscita relè digitale BMXSRA0405	113
Modulo di uscita relè digitale di sicurezza BMXSRA0405	113
Connettore di cablaggio BMXSRA0405	113
BMXSRA0405 Esempi di cablaggio dell'applicazione di uscita	116
BMXSRA0405 Struttura dei dati	125
Alimentatori di sicurezza M580	130
Alimentatori di sicurezza M580	131
Diagnostica del modulo di alimentazione di sicurezza M580	134
DDT di sicurezza M580.....	136
Convalida di un sistema di sicurezza M580	138
Architetture del modulo di sicurezza M580.....	139
Architettura di sicurezza della CPU e del coprocessore di sicurezza M580	139
Architettura di sicurezza del modulo di ingresso analogico BMXSAI0410.....	143
Architettura di sicurezza del modulo di ingresso digitale BMXSDI1602	144
Architettura di sicurezza del modulo di uscita digitale BMXSDO0802	145
Architettura di sicurezza del modulo di uscita relè digitale BMXSRA0405	146
Valori SIL e MTTF del modulo di sicurezza M580	147
Calcoli del livello di integrità della sicurezza	147
Calcolo delle prestazioni e dei tempi per il sistema di sicurezza M580.....	154
Tempo di sicurezza del processo.....	154
Impatto delle comunicazioni CIP Safety sul tempo di reazione del sistema di sicurezza	163
Libreria di sicurezza	166
Libreria di sicurezza.....	166
Separazione dei dati in un sistema di sicurezza M580	170
Separazione dei dati in un progetto di sicurezza M580	171
Come trasferire i dati tra le aree dello spazio dei nomi	174
Comunicazioni del sistema di sicurezza M580	176

Sincronizzazione dell'ora.....	177
Configurazione della sincronizzazione dell'ora con firmware della CPU 3.10 o precedente.....	177
Sincronizzazione dell'ora per firmware della CPU 3.20 o successivo.....	181
Comunicazioni peer-to-peer	183
Comunicazione peer-to-peer	183
Architettura peer-to-peer con firmware della CPU 3.10 o precedente	184
Configurazione del DFB S_WR_ETH_MX nella logica di programma del PAC mittente.....	191
Configurazione del DFB S_RD_ETH_MX nella logica di programma del PAC ricevente.....	193
Architettura peer-to-peer con firmware della CPU 3.20 o successivo.....	196
Configurazione del DFB S_WR_ETH_MX2 nella logica di programma del PAC mittente	204
Configurazione del DFB S_RD_ETH_MX2 nella logica di programma del PAC ricevente.....	206
M580 Comunicazioni black channel	210
Comunicazione tra la CPU M580 e gli I/O di sicurezza.....	213
Comunicazioni tra PAC M580 Safety e I/O	213
Diagnostica di un sistema di sicurezza M580.....	215
Diagnostica della CPU e del coprocessore di sicurezzaM580.....	216
Diagnostica di condizioni bloccanti	216
Diagnostica di condizioni non bloccanti.....	219
Diagnostica mediante LED della CPU di sicurezza M580	221
Diagnostica mediante LED del coprocessore di sicurezza M580.....	224
LED per l'accesso alla scheda di memoria	226
Diagnostica dell'alimentatore di sicurezza del modulo M580	229
Diagnostica mediante LED dell'alimentatore	229
Diagnostica degli ingressi analogici del BMXSAI0410.....	231
Diagnostica DDDT BMXSAI0410	231
Diagnostica dei LED degli ingressi analogici del BMXSAI0410	232
Diagnostica degli ingressi digitali del BMXSDI1602	235
Diagnostica DDDT BMXSDI1602	235
Diagnostica dei LED degli ingressi digitali del BMXSDI1602.....	237
Diagnostica delle uscite digitali del BMXSDO0802	241

Diagnostica DDDT BMXSDO0802	241
Diagnostica dei LED delle uscite digitali del BMXSDO0802	243
Diagnostica delle uscite relè digitali del BMXSRA0405	247
Diagnostica DDDT BMXSRA0405	247
Diagnostica dei LED delle uscite relè digitali del BMXSRA0405	248
Utilizzo di un sistema di sicurezza M580	251
Aree di processo, sicurezza e dati globali in Control Expert	252
Separazione dei dati in Control Expert	253
Modalità operative, stati operativi e task	257
Modalità operativi del PAC M580 Safety	257
Stati operativi del PAC M580 Safety	262
Sequenze di avvio	267
Task del PAC di sicurezza M580	271
Creazione di un progetto di sicurezza M580	275
Creazione di un progetto di sicurezza M580	275
Firma Safe	275
Blocco delle configurazioni del modulo I/O M580 di sicurezza	283
Blocco delle configurazioni del modulo I/O M580 di sicurezza	283
Inizializzazione dei dati in Control Expert	286
Inizializzazione dei dati in Control Expert per il PAC M580 Safety	286
Lavorare con le tabelle di animazione in Control Expert	287
Tabelle di animazione e schermate operatore	287
Aggiunta di sezioni codice	292
Aggiunta di codice a un processo di sicurezza M580	292
Richiesta diagnostica	296
Comandi Scambia e Azzera	299
Gestione della sicurezza dell'applicazione	302
Protezione dell'applicazione	302
Protezione con password dell'area sicura	310
Protezione di Unità programma, sezione e subroutine	314
Protezione del firmware	316
Protezione Web/Memorizzazione dati	318
Perdita della password	320
Gestione della sicurezza della workstation	327
Gestione dell'accesso a Control Expert	327

Diritti d'accesso	330
Modifiche a Control Expert per il sistema di sicurezza M580	340
Trasferimento e importazione di codice e progetti di sicurezza M580 in Control Expert	340
Salvataggio e ripristino di dati tra un file e il PAC.....	341
CCOTF per un PAC di sicurezza M580.....	341
Modifiche dei tool del PAC di sicurezza M580.....	343
CIP Safety	345
Introduzione di CIP Safety per PAC Safety M580	346
Comunicazione CIP Safety	346
Configurazione della CPU CIP Safety M580	350
Configurazione dell'OUNID CPU.....	350
Configurazione del dispositivo CIP Safety di destinazione	352
Panoramica di configurazione del dispositivo CIP Safety	352
Configurazione del dispositivo CIP Safety con l'utilizzo di uno strumento offerto dal fornitore.....	354
Configurazione dei DTM del dispositivo di sicurezza	356
Lavorare con i DTM.....	356
DTM dispositivo di sicurezza - Informazioni su file e fornitore	359
DTM del dispositivo di sicurezza - Numero di rete di sicurezza	360
DTM dispositivo di sicurezza - Verifica e convalida della configurazione	362
DTM del dispositivo di sicurezza - Connessioni I/O	363
DTM del dispositivo di sicurezza - Impostazioni di connessione I/O.....	366
Impostazioni dell'indirizzo IP del dispositivo di sicurezza	366
Operazioni con CIP Safety	368
Trasferimento di un'applicazione CIP Safety da Control Expert al PAC	368
Struttura della richiesta di apertura di sicurezza di tipo 2	369
Operazioni del dispositivo CIP Safety	370
Interazioni tra le operazioni del PAC di sicurezza e la connessione di destinazione.....	372
Comandi DTM CIP Safety	376
Diagnostica CIP Safety	378
DDDT del dispositivo CIP Safety.....	378

Codici di errore del dispositivo CIP Safety	381
DDDT CPU indipendente CIP Safety	385
Diagnostica DTM CPU	385
Diagnostica di connessione del dispositivo CIP Safety	386
Appendici	389
IEC 61508	390
Informazioni generali su IEC 61508.....	391
Policy SIL.....	393
Oggetti di sistema	398
Bit di sistema M580 Safety	399
Parole di sistema M580 Safety	401
Riferimenti SRAC	404
Glossario	409
Indice	415

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.



L'aggiunta di questo simbolo a un'etichetta di "Pericolo" o "Avvertimento" indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.



Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un **AVVISO** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Prima di iniziare

Non utilizzare questo prodotto su macchinari privi di sorveglianza attiva del punto di funzionamento. La mancanza di un sistema di sorveglianza attivo sul punto di funzionamento può presentare gravi rischi per l'incolumità dell'operatore macchina.

▲ AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

- Non utilizzare questo software e la relativa apparecchiatura di automazione su macchinari privi di protezione per le zone pericolose.
- Non avvicinarsi ai macchinari durante il funzionamento.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Questa apparecchiatura di automazione con il relativo software permette di controllare processi industriali di vario tipo. Il tipo o il modello di apparecchiatura di automazione adatto per ogni applicazione varia in funzione di una serie di fattori, quali la funzione di controllo richiesta, il grado di protezione necessario, i metodi di produzione, eventuali condizioni particolari, la regolamentazione in vigore, ecc. Per alcune applicazioni può essere necessario utilizzare più di un processore, ad esempio nel caso in cui occorra garantire la ridondanza dell'esecuzione del programma.

Solo l'utente, il costruttore della macchina o l'integratore del sistema sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina e possono quindi determinare l'apparecchiatura di automazione e i relativi interblocchi e sistemi di sicurezza appropriati. La scelta dell'apparecchiatura di controllo e di automazione e del relativo software per un'applicazione particolare deve essere effettuata dall'utente nel rispetto degli standard locali e nazionali e della regolamentazione vigente. Per informazioni in merito, vedere anche la guida National Safety Council's Accident Prevention Manual (che indica gli standard di riferimento per gli Stati Uniti d'America).

Per alcune applicazioni, ad esempio per le macchine confezionatrici, è necessario prevedere misure di protezione aggiuntive, come un sistema di sorveglianza attivo sul punto di funzionamento. Questa precauzione è necessaria quando le mani e altre parti del corpo dell'operatore possono raggiungere aree con ingranaggi in movimento o altre zone pericolose, con conseguente pericolo di infortuni gravi. I prodotti software da soli non possono proteggere l'operatore dagli infortuni. Per questo motivo, il software non può in alcun modo costituire un'alternativa al sistema di sorveglianza sul punto di funzionamento.

Accertarsi che siano stati installati i sistemi di sicurezza e gli asservimenti elettrici/meccanici opportuni per la protezione delle zone pericolose e verificare il loro corretto funzionamento prima di mettere in funzione l'apparecchiatura. Tutti i dispositivi di blocco e di sicurezza relativi alla sorveglianza del punto di funzionamento devono essere coordinati con l'apparecchiatura di automazione e la programmazione software.

NOTA: Il coordinamento dei dispositivi di sicurezza e degli asservimenti meccanici/elettrici per la protezione delle zone pericolose non rientra nelle funzioni della libreria dei blocchi funzione, del manuale utente o di altre implementazioni indicate in questa documentazione.

Avviamento e verifica

Prima di utilizzare regolarmente l'apparecchiatura elettrica di controllo e automazione dopo l'installazione, l'impianto deve essere sottoposto ad un test di avviamento da parte di personale qualificato per verificare il corretto funzionamento dell'apparecchiatura. È importante programmare e organizzare questo tipo di controllo, dedicando ad esso il tempo necessario per eseguire un test completo e soddisfacente.

⚠ AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

- Verificare che tutte le procedure di installazione e di configurazione siano state completate.
- Prima di effettuare test sul funzionamento, rimuovere tutti i blocchi o altri mezzi di fissaggio dei dispositivi utilizzati per il trasporto.
- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Eseguire tutti i test di avviamento raccomandati sulla documentazione dell'apparecchiatura. Conservare con cura la documentazione dell'apparecchiatura per riferimenti futuri.

Il software deve essere testato sia in ambiente simulato che in ambiente di funzionamento reale..

Verificare che il sistema completamente montato e configurato sia esente da cortocircuiti e punti a massa, ad eccezione dei punti di messa a terra previsti dalle normative locali (ad esempio, in conformità al National Electrical Code per gli USA). Nel caso in cui sia necessario effettuare un test sull'alta tensione, seguire le raccomandazioni contenute nella documentazione dell'apparecchiatura al fine di evitare danni accidentali all'apparecchiatura stessa.

Prima di mettere sotto tensione l'apparecchiatura:

- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.
- Chiudere lo sportello del cabinet dell'apparecchiatura.
- Rimuovere tutte le messa a terra temporanee dalle linee di alimentazione in arrivo.
- Eseguire tutti i test di avviamento raccomandati dal costruttore.

Funzionamento e regolazioni

Le seguenti note relative alle precauzioni da adottare fanno riferimento alle norme NEMA Standards Publication ICS 7.1-1995 (fa testo la versione inglese):

- Indipendentemente dalla qualità e della precisione del progetto nonché della costruzione dell'apparecchiatura o del tipo e della qualità dei componenti scelti, possono sussistere dei rischi se l'apparecchiatura non viene utilizzata correttamente.
- Eventuali regolazioni involontarie possono provocare il funzionamento non soddisfacente o non sicuro dell'apparecchiatura. Per effettuare le regolazioni funzionali, attenersi sempre alle istruzioni contenute nel manuale fornito dal costruttore. Il personale incaricato di queste regolazioni deve avere esperienza con le istruzioni fornite dal costruttore delle apparecchiature e con i macchinari utilizzati con l'apparecchiatura elettrica.
- L'operatore deve avere accesso solo alle regolazioni relative al funzionamento delle apparecchiature. L'accesso agli altri organi di controllo deve essere riservato, al fine di impedire modifiche non autorizzate ai valori che definiscono le caratteristiche di funzionamento delle apparecchiature.

Informazioni sul manuale

Ambito del documento

Il presente Manuale di sicurezza descrive i moduli del sistema di sicurezza M580, con particolare riferimento alle modalità con cui soddisfano i requisiti di sicurezza dello standard IEC 61508. Fornisce informazioni dettagliate sull'installazione, l'esecuzione e la manutenzione corrette del sistema allo scopo di proteggere le persone e di evitare danni dell'ambiente, delle apparecchiature e della produzione.

La presente documentazione è dedicata a personale qualificato con conoscenze dei sistemi di sicurezza funzionale e Control Expert Safety. Messa in servizio e funzionamento del sistema M580 Safety possono essere eseguiti solo da personale adeguatamente formato autorizzato a mettere in servizio e a utilizzare i sistemi in conformità con gli standard di sicurezza funzionale.

NOTA:

- La versione originale del presente manuale è la versione inglese.
- Per eventuali richieste di sostituzione o problemi di qualità relativi alla gamma M580, rivolgersi al Centro di assistenza clienti per il supporto tecnico. Ulteriori informazioni sono disponibili nella sezione *Supporto / I nostri contatti* del sito Web di Schneider Electric al seguente indirizzo:

www.se.com/b2b/en/support/

Nota di validità

Questo documento è valido per TMEcoStruxure Control Expert Safety 15.0 o versioni successive.

Per informazioni circa le norme ambientali e la conformità dei prodotti (RoHS, REACH, PEP, EOL, e così via), visitare www.se.com/ww/en/work/support/green-premium/.

Le caratteristiche tecniche delle apparecchiature descritte in questo documento sono consultabili anche online. Per accedere alle informazioni online, consultare la homepage di Schneider Electric www.se.com/ww/en/download/.

Le caratteristiche descritte in questo manuale dovrebbero essere uguali a quelle che appaiono online. In base alla nostra politica di continuo miglioramento, è possibile che il contenuto della documentazione sia revisionato nel tempo per migliorare la chiarezza e la precisione. Nell'eventualità in cui si noti una differenza tra il manuale e le informazioni online, fare riferimento in priorità alle informazioni online.

Documenti correlati

Titolo della documentazione	Codice di riferimento
M580 Safety SRAC — SRAC Verification Plan	EIO000004540 (Inglese)
Modicon M580, Guida alla pianificazione del sistema di sicurezza	QGH60283 (Inglese), QGH60284 (Francese), QGH60285 (Tedesco), QGH60286 (Spagnolo), QGH60287 (Italiano), QGH60288 (Cinese)
EcoStruxure™ Control Expert, Safety, Block Library	QGH60275 (Inglese), QGH60278 (Francese), QGH60279 (Tedesco), QGH60280 (Italiano), QGH60281 (Spagnolo), QGH60282 (Cinese)
Piattaforma controller Modicon - Sicurezza informatica, Manuale di riferimento	EIO000001999 (Inglese), EIO000002001 (Francese), EIO000002000 (Tedesco), EIO000002002 (Italiano), EIO000002003 (Spagnolo), EIO000002004 (Cinese)
Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente	NHA58880 (Inglese), NHA58881 (Francese), NHA58882 (Tedesco), NHA58883 (Italiano), NHA58884 (Spagnolo), NHA58885 (Cinese)
Modicon M580, Hardware, Manuale di riferimento	EIO0000001578 (Inglese), EIO0000001579 (Francese), EIO0000001580 (Tedesco), EIO0000001582 (Italiano), EIO0000001581 (Spagnolo), EIO0000001583 (Cinese)
Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente	HRB62666 (Inglese), HRB65318 (Francese), HRB65319 (Tedesco), HRB65320 (Italiano), HRB65321 (Spagnolo), HRB65322 (Cinese)
Modicon M580, Guida di pianificazione del sistema per le topologie complesse	NHA58892 (Inglese), NHA58893 (Francese), NHA58894 (Tedesco), NHA58895 (Italiano), NHA58896 (Spagnolo), NHA58897 (Cinese)
EcoStruxure™ Automation Device Maintenance, Guida utente	EIO0000004033 (Inglese), EIO0000004048 (Francese), EIO0000004046 (Tedesco), EIO0000004049 (Italiano), EIO0000004047 (Spagnolo), EIO0000004050 (Cinese)
Unity Loader, Guida utente	33003805 (Inglese), 33003806 (Francese), 33003807 (Tedesco), 33003809 (Italiano), 33003808 (Spagnolo), 33003810 (Cinese)
EcoStruxure™ Control Expert, Modalità di funzionamento	33003101 (Inglese), 33003102 (Francese), 33003103 (Tedesco), 33003104 (Spagnolo), 33003696 (Italiano), 33003697 (Cinese)
EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento	EIO0000002135 (Inglese), EIO0000002136 (Francese), EIO0000002137 (Tedesco), EIO0000002138 (Italiano), EIO0000002139 (Spagnolo), EIO0000002140 (Cinese)

È possibile scaricare tutta la documentazione tecnica disponibile, incluso questo documento, ed altre informazioni tecniche dal sito web www.se.com/en/download/.

Funzione di sicurezza M580

Contenuto del capitolo

Funzione di sicurezza M580	16
----------------------------------	----

Introduzione

Questo capitolo introduce la funzione di sicurezza M580 per il sistema di sicurezza M580 e per ogni modulo di sicurezza.

Funzione di sicurezza M580

Presentazione della funzione di sicurezza M580 di Schneider Electric

Tramite Control Expert con sicurezza si può programmare, configurare e gestire un'applicazione di sicurezza. Durante la progettazione e la programmazione di un'applicazione di sicurezza, applicare le funzioni di sicurezza solo a componenti di un loop di sicurezza.

NOTA: In un loop di sicurezza si devono includere solo moduli di sicurezza, le relative impostazioni di configurazione e i relativi dati.

Dopo la messa in servizio, mentre il sistema di sicurezza M580 funziona in modalità di sicurezza, il sistema di sicurezza legge periodicamente gli ingressi di sicurezza, elabora la logica di sicurezza del programma applicativo, esegue la diagnostica e applica i risultati logici alle uscite di sicurezza.

Se la CPU o la diagnostica I/O rileva un errore, il sistema di sicurezza pone la parte di sistema coinvolta in uno stato sicuro. A seconda della natura dell'errore rilevato, l'ambito della risposta può porre un singolo canale di I/O, un modulo di I/O o l'intero sistema nello stato sicuro.

Lo stato sicuro è sempre uno stato non alimentato. Ad esempio:

- Se il modulo di ingresso analogico BMXSAI0410 o il modulo di ingresso digitale BMXSDI1602 rileva una condizione interna pericolosa, imposta il valore degli ingressi nella CPU a "0" (stato non alimentato). Questo stato permane finché la condizione scatenante non viene eliminata.
- Se il modulo di uscita digitale BMXSDO0802 o il modulo di uscita relè digitale BMXSRA0405 rileva una condizione interna pericolosa, imposta le uscite allo stato non alimentato. Questo stato permane finché la condizione scatenante non viene eliminata e il modulo non viene riavviato.
- Se il modulo di uscita digitale BMXSDO0802 o il modulo di uscita relè digitale BMXSRA0405 rileva un errore di comunicazione su un collegamento black channel alla CPU, il modulo di uscita imposta le uscite allo stato di posizionamento di sicurezza.

NOTA: è possibile utilizzare Control Expert Safety per configurare lo stato di posizionamento di sicurezza (alimentato, non alimentato o mantenimento dell'ultimo valore) nel caso in cui la comunicazione black channel tra la CPU e il modulo di uscita si interrompa.

- Se un BMEP58•040S standalone o una CPU BMEH58•040S Hot Standby rileva un errore di comunicazione su un collegamento black channel con un modulo di ingresso di sicurezza, lo stato degli ingressi interessati viene impostato a "0" (stato non alimentato) finché il black channel non ritorna operativo e la CPU non può nuovamente leggere i valori di ingresso attuali.

Loop di sicurezza

Un loop di sicurezza è l'insieme di apparecchiature e logica che esegue un processo di sicurezza. Un progetto di sicurezza può comprendere più loop di sicurezza. Per ogni loop di sicurezza occorre verificare quanto segue:

- Il tempo di sicurezza del processo, pagina 154 deve essere maggiore del tempo di reazione del sistema, pagina 154.
- La somma dei valori PFD o PFH, pagina 147 per tutti i componenti del loop di sicurezza non deve superare il valore massimo consentito per:
 - livello di integrità della sicurezza (1, 2, 3 o 4)
 - modo di funzionamento (bassa domanda o alta domanda)
 - intervallo del test di prova

In un loop di sicurezza si devono includere solo moduli di sicurezza. Sebbene nel progetto di sicurezza sia possibile includere dei moduli non interferenti, pagina 29, questi vanno utilizzati soltanto per i task non di sicurezza (MAST, FAST, AUX0 o AUX1).

⚠ AVVERTIMENTO

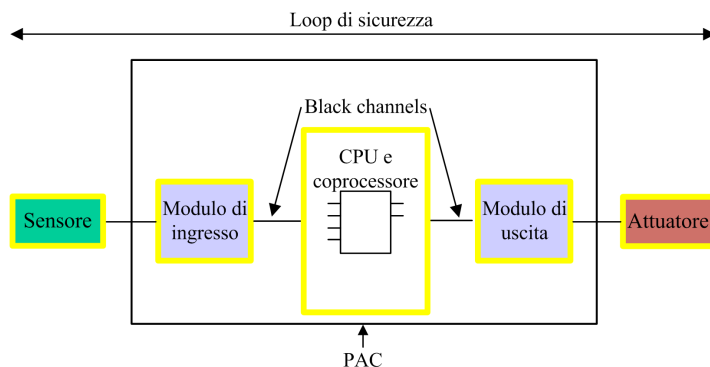
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Per eseguire le funzioni di sicurezza, utilizzare esclusivamente moduli di sicurezza.
- Non utilizzare ingressi o uscite di moduli non interferenti per le funzioni non di sicurezza.
- Non utilizzare le variabili dell'Area globale per le funzioni relative alla sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Vedere la sezione *Separazione dei dati in un progetto di sicurezza M580*, pagina 171 per una descrizione delle variabili dell'area globale.

Loop di sicurezza:



L'apparecchiatura di sicurezza include i seguenti moduli di sicurezza Schneider Electric M580:

- CPU BME•58•040S e coprocessore BMEP58CPROS3:

La CPU e il coprocessore insieme eseguono i task di lettura degli ingressi di sicurezza, elaborano la logica di sicurezza, eseguono la diagnostica e applicano i risultati alle uscite. Tutti questi task fanno parte del loop di sicurezza. Anche le porte utilizzate per le comunicazioni sul black channel fanno parte del loop di sicurezza. Gli altri componenti della CPU, invece, come la porta USB, la scheda di memoria SD e l'area di memoria statica ad accesso casuale non volatile (nvSRAM), non fanno parte del loop di sicurezza.

NOTA: All'avvio del sistema, sia a freddo che a caldo, la CPU e il coprocessore non caricano i dati memorizzati nella nvSRAM nel task di sicurezza (i dati della nvSRAM vengono utilizzati solo nei task non di sicurezza MAST, FAST e AUX). La CPU e il coprocessore, invece, applicano inizialmente le impostazioni di configurazione predefinite della scheda di memoria SD, quindi applicano i valori ricevuti direttamente dagli ingressi durante il funzionamento.

- I/O di sicurezza (BMXSAI0410, BMXSDI1602, BMXSDO0802 e BMXSRA0405):

Le funzioni di invio dei segnali di ingresso, di ricezione dei segnali di uscita e dell'esecuzione della diagnostica fanno parte del loop di sicurezza.

- Alimentatori BMXCPS4002S, BMXCPS4022S e BMXCPS3522S:

Questi alimentatori di sicurezza forniscono il rilevamento della sovratensione e questo fa parte del loop di sicurezza. Dato che l'affidabilità di ogni alimentatore (ossia il tasso di errore pericoloso) è oltre 100 volte superiore alla soglia dello standard SIL3, questi alimentatori di sicurezza non vengono inclusi nei calcoli del livello di integrità relativi al loop di sicurezza.

Il loop di sicurezza include anche le seguenti apparecchiature di sicurezza:

- Sensori, attuatori e relativo cablaggio con i moduli di I/O. Gli I/O di sicurezza eseguono la diagnostica del cablaggio dei sensori e degli attuatori per contribuire alla gestione del loop di sicurezza.

NOTA: Quando si progetta l'applicazione di sicurezza, occorre identificare le caratteristiche dei sensori e degli attuatori (in particolare i valori PFD/PFH).

Standard di certificazione

Contenuto del capitolo

Certificazioni.....	21
Standard e certificazioni	25

Introduzione

Questo capitolo descrive gli standard di certificazione validi per il sistema di sicurezza M580 e i moduli che lo compongono.

Certificazioni

M580 Standard di certificazione PAC di sicurezza

Il PAC di sicurezza M580 è certificato da TÜV Rheinland Group per l'uso in applicazioni fino a:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1

Per informazioni più dettagliate sulla classificazione SIL, vedere [Descrizione della classificazione SIL](#), pagina 394.

Specifiche dei PLC

- IEC 61131-2: controller programmabili - Parte 2: Requisiti per apparecchiature e test.
- IEC/EN 61010-2-201, UL 61010-2-201, CSA -C22.2 N. 61010-2-201: Requisiti di sicurezza per le apparecchiature elettriche - Parte 2-201: requisiti particolari per le apparecchiature di controllo.

Specifiche ambientali

Consultare [Standard e certificazioni M580](#), pagina 25 per i livelli dei test ambientali.

Specifiche per aree Ex

Per USA e Canada: località a rischio di classe I, divisione 2, gruppi A, B, C e D

- CSA 22.2 No213, ANSI/ISA12.12.01 e FM3611

Per gli altri paesi: CE ATEX (direttiva 2014/34/UE) o IECEx in atmosfera definita Zona 2 (gas) e/o Zona 22 (polvere)

- CEI/EN 60079-0; CEI/EN 60079-7; CEI/EN 60079-15

Specifiche per i sistemi di automazioni delle centrali elettriche

- IEC/EN 61000-6-5: Compatibilità elettromagnetica - Parte 6-5: Standard generici - Immunità per ambienti di sottostazioni e centrali elettriche.
- IEC/EN 61850-3: Reti di comunicazione e sistemi per l'automazione delle centrali elettriche - Parte 3: Requisiti generali

Consultare M580 Standard e certificazioni, pagina 25 per le limitazioni dell'installazione.

Specifiche ferroviarie

- EN 50126 / IEC 62278: Applicazioni ferroviarie: specifica e dimostrazione di affidabilità, disponibilità, mantenibilità e sicurezza (RAMS).
- EN 50128 / IEC 62279: Applicazioni ferroviarie - Sistemi di comunicazione, segnalazione ed elaborazione - Software per sistemi di controllo e protezione per il settore ferroviario.
- EN 50129 / IEC 62245: Applicazioni ferroviarie - Sistemi di comunicazione, segnalazione ed elaborazione - Sistemi elettronici di segnalazione legati alla sicurezza.
- EN 50155 / IEC 60571: Applicazioni ferroviarie - Materiale rotabile - Apparecchiature elettroniche.
- EN 50121-3-2 / IEC 62236-3-2: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 3-2: Materiale rotabile - Apparecchiatura.
- EN 50121-4 / IEC 62236-4: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 4: Emissioni e immunità degli apparati di segnalazione e telecomunicazioni.
- EN 50121-5 / IEC 62236-5: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 5: Emissione e immunità degli apparati e degli impianti di alimentazione fissi.
- EN 50125-1: Ferrovie - Condizioni ambientali per le apparecchiature - Parte 1: Materiale rotabile e apparecchiatura a bordo.
- EN 50125-3: Ferrovie - Condizioni ambientali per le apparecchiature - Parte 3: Apparecchiature per la segnalazione e le telecomunicazioni.
- EN 50124-1: Ferrovie - Coordinamento dell'isolamento - Parte 1: Requisiti di base: distanze di isolamento in aria e dispersione per tutte le apparecchiature elettriche ed elettroniche.

Consultare M580 Standard e certificazioni, pagina 25 per le limitazioni dell'installazione.

Specifiche di sicurezza funzionale

- IEC/EN 61000-6-7: Compatibilità elettromagnetica - Parte 6-7: Standard generici - Requisiti di immunità per apparecchiature destinate all'esecuzione di funzioni in un sistema legato alla sicurezza (sicurezza funzionale) in ubicazioni industriali.
- IEC 61326-3-1: Apparecchiature elettriche per la misura, il controllo e l'uso in laboratorio - Parte 3-1: Requisiti di immunità per sistemi di sicurezza e per apparecchiature destinate all'esecuzione di funzioni di sicurezza - Applicazione industriale generale.
- IEC 61508: Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili correlati alla sicurezza - Parte 1-7, edizione 2.0.
- IEC 61511-1: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 1: Struttura, definizioni, requisiti hardware e software.
- IEC 61511-2: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 2: Direttive per l'applicazione della norma IEC 61511-1.
- IEC 61511-3: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 3: Guida per la determinazione dei livelli di integrità di sicurezza richiesti.

Specifiche dei macchinari di sicurezza

- IEC/EN 62061: Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici/elettronici/elettronici programmabili correlati alla sicurezza.
- ISO EN 13849-1: Sicurezza dei macchinari - Componenti di sicurezza dei sistemi di controllo - Parte 1: Principi generali per la progettazione.

Sicurezza funzionale nelle specifiche di sistema

- EN 54-2: Sistemi di rilevamento e allarme antincendio Parte 2: Apparecchiature di controllo e segnalazione.
- EN 50156-1: Apparecchiature elettriche per forni e apparecchiature ausiliarie - Parte 1: Requisiti per la progettazione e l'installazione dell'applicazione.
- EN 50130-4: Sistemi di allarme - Parte 4: Compatibilità elettromagnetica. Famiglia di prodotti standard: Requisiti di immunità per componenti di impianti antincendio, antintrusione, arresto, TVCC, controllo accessi e sistemi di allarme sociale.
- EN 298: Sistemi automatici di comando per bruciatori e sistemi di apparecchi a gas o a combustibile liquido.
- NFPA 85: Boiler and Combustion Systems Hazards Code.

- NFPA 86: Standard for Ovens and Furnaces.
- NFPA 72: National Fire Alarm and Signaling Code.

Note:

Per un elenco completo di standard certificati da TÜV (completi di date e numero di revisione), fare riferimento al certificato TÜV all'indirizzo Web:

www.certipedia.com o www.fs-products.com.

Standard e certificazioni

Download

Fare clic sul collegamento corrispondente alla lingua preferita per scaricare gli standard e le certificazioni (formato PDF) validi per i moduli in questa linea di prodotti:

Titolo	Lingue
Piattaforme Modicon M580, M340 e X80 I/O, standard e certificazioni	<ul style="list-style-type: none"><li data-bbox="663 440 935 461">• Inglese: EIO0000002726<li data-bbox="663 472 955 493">• Francese: EIO0000002727<li data-bbox="663 505 946 526">• Tedesco: EIO0000002728<li data-bbox="663 537 935 558">• Italiano: EIO0000002730<li data-bbox="663 570 955 591">• Spagnolo: EIO0000002729<li data-bbox="663 602 932 623">• Cinese: EIO0000002731

Moduli supportati del sistema di sicurezza M580

Contenuto del capitolo

Moduli certificati del sistema di sicurezza M580.....	27
Moduli non interferenti.....	29

Introduzione

Un progetto di sicurezza M580 può includere moduli di sicurezza e non di sicurezza. È possibile utilizzare:

- Moduli di sicurezza nel task SAFE.
- Moduli non di sicurezza solo per task non di sicurezza (MAST, FAST, AUX0 e AUX1).

NOTA: È possibile aggiungere a un progetto di sicurezza solo i moduli non di sicurezza che non interferiscono con la funzione di sicurezza.

Utilizzare solo il software di programmazione Control Expert di Schneider Electric per programmare, mettere in servizio e utilizzare l'applicazione di sicurezza M580.

- Control Expert L Safety fornisce tutta la funzionalità di Control Expert L ed è utilizzabile con CPU di sicurezza BMEP582040S e BMEH582040S.
- Control Expert XL Safety fornisce tutta la funzionalità di Control Expert XL ed è utilizzabile per l'intera gamma di CPU di sicurezza BMEP58•040S e BMEH58•040S.

Questo capitolo elenca i moduli di sicurezza e non di sicurezza supportati dal sistema di sicurezza M580.

Moduli certificati del sistema di sicurezza M580

Moduli certificati

Il PAC di sicurezza M580 è un sistema di sicurezza certificato da TÜV Rheinland Group, in base a:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

Si basa sulla famiglia M580 di controllori logici programmabili (PAC). Sono certificati i seguenti moduli di sicurezza Schneider Electric M580:

- CPU standalone BMEP582040S
- CPU standalone BMEP584040S
- CPU BMEP586040S standalone
- CPU Hot Standby BMEH582040S
- CPU Hot Standby BMEH584040S
- CPU Hot Standby BMEH586040S
- Coprocessore BMEP58CPROS3
- Modulo di ingresso analogico BMXSAI0410
- Modulo di ingresso digitale BMXSDI1602
- Modulo di uscita digitale BMXSDO0802
- Modulo di uscita relè digitale BMXSRA0405
- Alimentatore BMXCPS4002S
- Alimentatore BMXCPS4022S
- Alimentatore BMXCPS3522S

NOTA: Oltre ai moduli di sicurezza elencati sopra, è possibile includere nel progetto moduli non interferenti, non di sicurezza, pagina 29.

NOTA: L'offerta Modicon Safety comprende fino a SIL3 (reg. IEC 61508) e PLe (reg. ISO 13849), ossia compatibile anche SIL1/SIL2 e PLa, b,c,d.

NOTA:

- Ogni volta che nel documento viene indicato SIL2 o SIL3 senza un riferimento standard, si tratta di IEC 61508 / IEC 61511.
- Ogni volta che viene indicato SIL2, si intende anche SIL3 per quanto riguarda EN 50126 / EN 50128 / EN 50129.
- Ogni volta che viene indicato SIL3, si intende anche SIL4 per quanto riguarda EN 50126 / EN 50128 / EN 50129.

Sul sito web di TÜV Rheinland Group www.certipedia.com o www.fs-products.com si possono trovare le informazioni più aggiornate sulle versioni dei prodotti certificati.

Sostituzione di una CPU

È possibile sostituire una CPU BME•58•040S con un'altra BME•58•040S. La sostituzione, tuttavia, non può avvenire se vengono superate le seguenti limitazioni:

- numero di I/O
- numero di derivazioni di I/O
- numero di variabili
- dimensione memoria applicazione

Consultare gli argomenti:

- *Compatibilità della configurazione in Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* per una descrizione delle applicazioni di Control Expert compatibili con CPU di sicurezza e Hot Standby.
- *Caratteristiche prestazionali della CPU e del coprocessore M580* del documento *Modicon M580, Guida alla pianificazione del sistema di sicurezza* per una descrizione delle limitazioni della CPU.

Moduli non interferenti

Introduzione

Un progetto di sicurezza M580 può includere moduli di sicurezza e non di sicurezza. È possibile utilizzare moduli non di sicurezza solo per task non di sicurezza. È possibile aggiungere a un progetto di sicurezza solo i moduli non di sicurezza che non interferiscono con la funzione di sicurezza.

Definizione di un modulo non interferente

▲ ATTENZIONE

USO INCORRETTO DI DATI CORRELATI ALLA SICUREZZA

Confermare che non vengono utilizzati dati di ingresso né dati di uscita dai moduli non interferenti per controllare le uscite correlate alla sicurezza. I moduli non di sicurezza possono elaborare solo dati non di sicurezza.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Un modulo non interferente è un modulo che non può interferire con la funzione di sicurezza. Per moduli M580 in-rack (BME_x, BMX_x, PMX_x e PMEx), esistono due tipi di moduli non interferenti:

- **Tipo 1:** è possibile installare un modulo di tipo 1 nello stesso rack dei moduli di sicurezza (ovunque si posizioni il modulo di sicurezza, nel rack principale o di estensione).
- **Tipo 2:** non è possibile installare un modulo di tipo 2 non interferente nello stesso rack principale dei moduli di sicurezza (ovunque si posizioni il modulo di sicurezza, nel rack principale o di estensione).

NOTA: i moduli di tipo 1 e 2 sono elencati sul sito Web TÜV Rheinland all'indirizzo www.certipedia.com.

Per moduli Mx80 non in-rack, tutta l'apparecchiatura Ethernet (DIO o DRS) può essere considerata come non interferente e perciò utilizzabile come parte di un sistema di sicurezza M580.

Moduli non interferenti di tipo 1 per applicazioni SIL3

I seguenti moduli non di sicurezza possono essere definiti come moduli non interferenti di tipo 1 in un sistema di sicurezza M580.

NOTA: L'elenco di moduli non di sicurezza non interferenti di tipo 1 può cambiare di volta in volta. Per l'elenco corrente, visitare il sito Web TÜV Rheinland all'indirizzo www.certipedia.com.

Tipo di modulo	Codice prodotto modulo
Backplane a 4 slot	BMEXBP0400
Backplane a 8 slot	BMEXBP0800
Backplane a 12 slot	BMEXBP1200
Backplane a 4 slot	BMXXBP0400
Backplane a 6 slot	BMXXBP0600
Backplane a 8 slot	BMXXBP0800
Backplane a 12 slot	BMXXBP1200
Backplane a 6 slot con doppio slot per alimentatori ridondanti	BMEXBP0602
Backplane a 10 slot con doppio slot per alimentatori ridondanti	BMEXBP1002
Comunicazione: adattatore derivazione Ethernet avanzato X80 1 CH	BMXCRA31210
Comunicazione: adattatore derivazione Ethernet avanzato X80 1 CH	BMECRA31210
Comunicazione: modulo Ethernet con servizi Web standard	BMENOC0301
Comunicazione: modulo Ethernet con inoltro IP	BMENOC0321
Comunicazione: modulo Ethernet con servizi Web FactoryCast	BMENOC0311
Comunicazione: modulo di estensione rack	BMXXBE1000
Comunicazione: AS-Interface	BMXEIA0100
Comunicazione: Dati globali	BMXNGD0100
Comunicazione: convertitore in fibra MM/LC 2CH 100 Mb	BMXNRP0200
Comunicazione: convertitore in fibra SM/LC 2CH 100 Mb	BMXNRP0201
Comunicazione: modulo di comunicazione M580 IEC 61850	BMENOP0300
Comunicazione: server OPC UA integrato	BMENUA0100
Conteggio: modulo SSI 3 CH	BMXEAE0300
Conteggio: contatore alta velocità a 2 can	BMXEHC0200
Conteggio: contatore alta velocità a 8 can	BMXEHC0800

Tipo di modulo	Codice prodotto modulo
Movimento: uscita treno di impulsi 2 canali indipendenti	BMXMSP0200
Analogico: Modulo HART 8 ingressi di corrente analogica isolati	BMEAH10812
Analogico: Modulo HART a 4 uscite di corrente analogica isolate	BMEAH00412
Analogico: 4 ingressi U/I isolati analogici ad alta velocità	BMXAMI0410
Analogico: 4 U/I Ingressi analogici non isolati ad alta velocità	BMXAMI0800
Analogico: 8 ingressi U/I isolati analogici ad alta velocità	BMXAMI0810
Analogico: 4 ingressi analogici U/I 4 uscite U/I	BMXAMM0600
Analogico: 2 uscite U/I analogiche isolate	BMXAMO0210
Analogico: 4 uscite U/I analogiche isolate	BMXAMO0410
Analogico: 8 uscite analogiche di corrente non isolate	BMXAMO0802
Analogico: 4 TC/RTD ingressi analogici isolati	BMXART0414.2
Analogico: 8 TC/RTD ingressi analogici isolati	BMXART0814.2
Digitale: 8 ingressi digitali 220 Vca	BMXDAI0805
Digitale: 8 ingressi digitali da 100 a 120 Vca isolati	BMXDAI0814
Digitale: 16 In digitali 24Vca/24Vcc Source	BMXDAI1602
Digitale: 16 ingressi digitali 48 Vca	BMXDAI1603
Digitale: 16 ingressi digitali da 100 a 120 Vca isolati 20 pin	BMXDAI1604
Digitale: 16 canali di ingresso supervisionati dig da 100 a 120 Vca 40 pin	BMXDAI1614
Digitale: 16 canali di ingresso supervisionati dig da 200 a 240 Vca 40 pin	BMXDAI1615
Digitale: 16 uscite triac dig da 100 a 240 Vca 20 pin	BMXDAO1605
Digitale: 16 uscite triac dig da 24 a 240 Vca 40 pin	BMXDAO1615
Digitale: 16 In digitali 24Vcc Sink	BMXDDI1602
Digitale: 16 In digitali 48Vcc Sink	BMXDDI1603
Digitale: 16 In digitali 125Vcc Sink	BMXDDI1604T
Digitale: 32 In digitali 24Vcc Sink	BMXDDI3202K
Digitale: 64 In digitali 24Vcc Sink	BMXDDI6402K
Digitale: Trans 8 In digitali 24Vcc 8Q Source	BMXDDM16022
Digitale: Relè 8 In digitali 24Vcc 8Q	BMXDDM16025
Digitale: Trans 16 In digitali 24Vcc 16Q Source	BMXDDM3202K

Tipo di modulo	Codice prodotto modulo
Digitale: Dig 16Q Trans Source 0,5A	BMXDDO1602
Digitale: Dig 16 O Trans Sink	BMXDDO1612
Digitale: 32 uscite digitali Trans source	BMXDDO3202K
Digitale: 64 uscite digitali Trans source	BMXDDO6402K
Digitale: 8Q 125Vcc dig	BMXDRA0804T
Digitale: Relé isolati 8Q dig 24 Vcc o da 24 a 240 Vca	BMXDRA0805
Digitale: 16 canali di uscita relè non isolati dig da 5 a 125 Vcc o da 25 a 240 Vca	BMXDRA0815
Digitale: 16 uscite digitali relè	BMXDRA1605
Digitale: Relè uscita NC dig da 5 a 125 Vcc o da 24 a 240 Vca	BMXDRC0805
Digitale: 16 In digitali 24/125Vcc TSTAMP	BMXERT1604
Switch opzionale di rete Mx80	BMENOS0300
Ingresso frequenza turbomacchina 2 CH	BMXETM0200
Il modulo Master Profibus DP/DPV1 supporta	PMEPXM0100
Modulo RTU avanzato Mx80	BMENOR2200H

Moduli non interferenti di tipo 2 per applicazioni SIL2/3

I seguenti moduli non di sicurezza in-rack possono essere considerati non interferenti di tipo 2 in un sistema di sicurezza M580.

NOTA: L'elenco di moduli non di sicurezza non interferenti di tipo 2 può cambiare di volta in volta. Per l'elenco corrente, visitare il sito Web TÜV Rheinland all'indirizzo www.certipedia.com.

Tipo di modulo	Codice prodotto modulo
Comunicazione: Adattatore derivazione Ethernet X80 standard a 1 can	BMXCRA31200
Alimentazione CA standard	BMXCPS2000
Alimentazione CC isolata standard	BMXCPS2010
Alimentazione da 24 a 48 VDC isolata di alta potenza	BMXCPS3020
Alimentazione standard ridondante 125 VCC	BMXCPS3522
Alimentazione standard ridondante 24/48 VCC	BMXCPS4022
Alimentazione CA standard ridondante	BMXCPS4002

Tipo di modulo	Codice prodotto modulo
Alimentazione CA alta potenza	BMXCPS3500
Alimentazione CC alta potenza	BMXCPS3540T
Comunicazione: Modulo bus 2 porta RS485/232	BMXNOM0200
Digitale: 32 In digitali 12/24Vcc Sink o Source	BMXDDI3232
Digitale: 32 In digitali 48Vcc Sink	BMXDDI3203
Master CANopen X80	BMECXM0100
Modulo peso	PMESWT0100
Modulo diagnostico partner	PMXCDA0400
Modulo di comunicazione Ethernet TCP Open universale	PMEUCM0302

NOTA: Tutte le apparecchiature autorizzate di un sistema M580 collegate a moduli di sicurezza tramite Ethernet sono considerate come non interferenti. Di conseguenza, tutti i moduli delle gamme Quantum e STB Advantys (non collegabili nello stesso rack dei moduli M580 Safety) sono non interferenti di Tipo 2.

Cybersicurezza per il sistema di sicurezza M580

Contenuto del capitolo

Cybersicurezza per il sistema di sicurezza M580.....	34
--	----

Introduzione

Questo capitolo elenca la documentazione disponibile per sviluppare un approccio alla sicurezza informatica per il PAC di sicurezza M580.

Cybersicurezza per il sistema di sicurezza M580

Riferimenti relativi alla sicurezza informatica

Lo scopo delle misure di cybersicurezza è di ridurre al massimo la vulnerabilità del sistema di protezione implementato nei confronti dei cyberattacchi. Per informazione su come mettere in atto queste misure per il sistema di sicurezza M580, vedere *Cybersicurezza piattaforma controller Modicon, Manuale di riferimento* (Numero di riferimento EIO0000001999 (EN)).

Ciclo di vita dell'applicazione

Contenuto del capitolo

Ciclo di vita dell'applicazione.....35

Introduzione

Ciclo di vita dell'applicazione

Introduzione

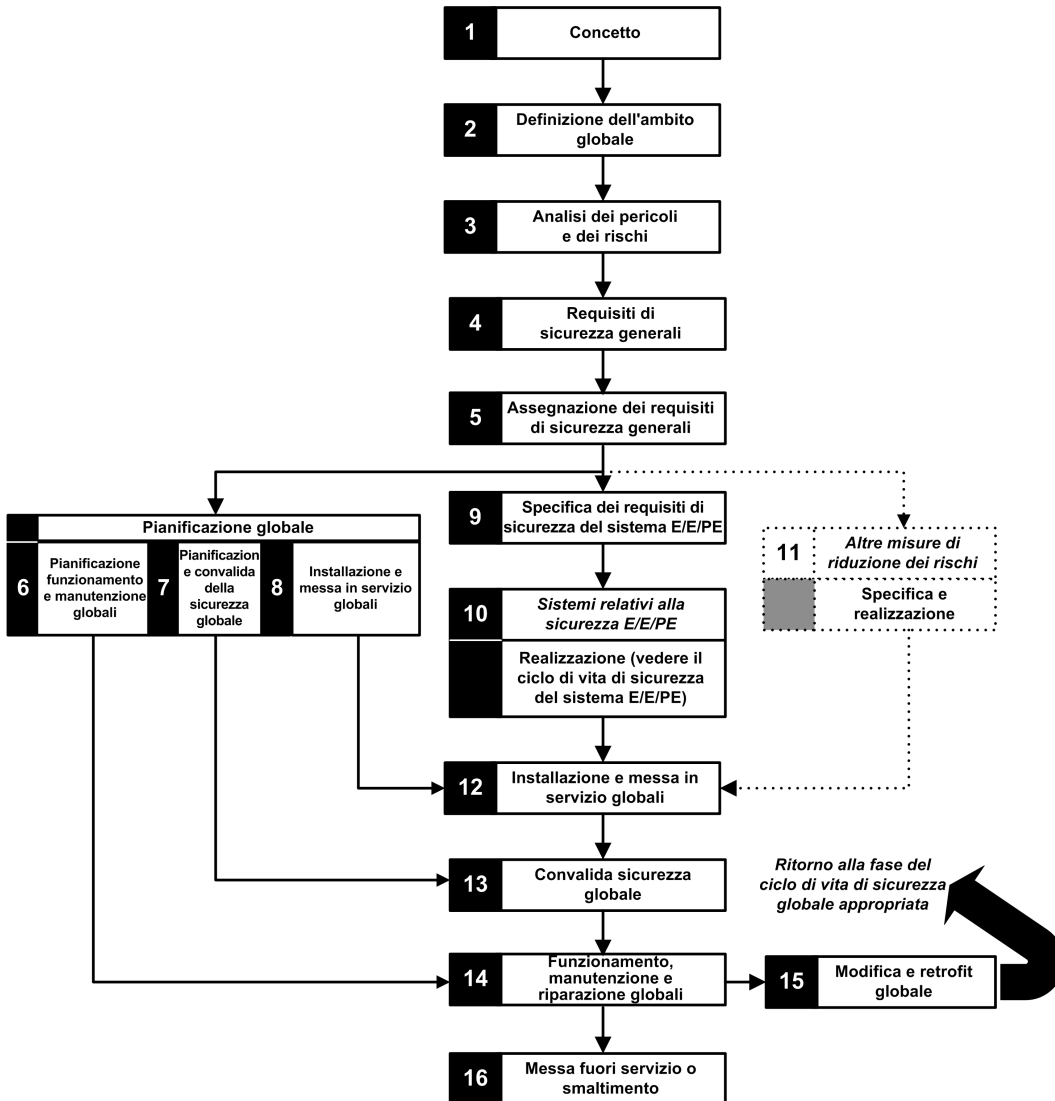
Quando si progetta un'applicazione sicura, occorre seguire le raccomandazioni di una delle norme di sicurezza che si applicano al campo di impiego in questione. La maggior parte delle norme di applicazione deriva o è collegata alla norma generica IEC 61508 che comprende, ad esempio, la norma sull'industria di processo (IEC 61511), le norme sui macchinari (IEC 62061 e ISO 13489), la norma sull'industria nucleare (IEC 61513), le norme per applicazioni ferroviarie (EN 5012x) e così via.

La norma IEC 61508 definisce il ciclo di vita di un'applicazione con una sequenza di passi. Ogni passo ha un ruolo definito, richiede documenti in ingresso e produce documenti di uscita. La decisione di utilizzare un sistema integrato di sicurezza (Safety Integrated System, SIS) viene presa al termine del passo Allocazione dei requisiti di sicurezza (passo 5).

Questa sezione definisce le verifiche relative all'uso di un sistema di sicurezza M580 che occorre effettuare nei passi seguenti:

9.	Specifica dei requisiti di sicurezza del sistema E/E/PE
10.	Realizzazione dei sistemi di sicurezza E/E/PE
12.	Installazione e messa in servizio globali
13.	Convalida sicurezza globale
14.	Funzionamento, manutenzione e riparazione globali
15.	Modifica e retrofit globale

Lo schema seguente presenta il ciclo di vita di sicurezza generale:



Passaggio 9: Specifica dei requisiti di sicurezza del sistema E/E/PE

Questa fase ha luogo una volta che l'analisi dei rischi è conclusa e ha fornito, tra l'altro, le seguenti informazioni:

- Definizione delle funzioni di sicurezza integrate
- Prestazioni richieste (durata, riduzione dei rischi, SIL...)
- Modalità di guasto delle funzioni

In questo passo dovrebbero essere generate le specifiche dei requisiti di sicurezza che includono, come minimo, le seguenti informazioni necessarie per progettare un'applicazione sicura con un PAC di sicurezza di qualsiasi tipo.

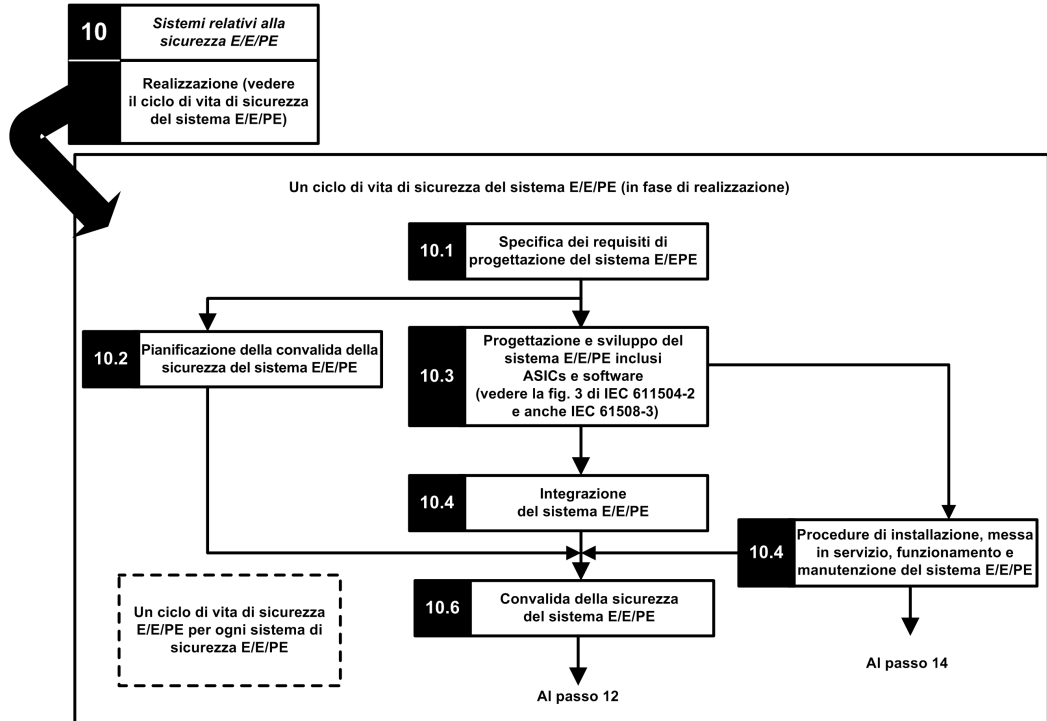
- Stato sicuro delle funzioni di sicurezza integrate
- Analisi delle modalità operative del SIS (incluso il comportamento in Run, Stop, sequenza di accensione, manutenzione, riparazione...)
- Intervallo di test delle SIF
- MTTR (tempo medio di riparazione) del SIS
- Scelta della SIF, in stato alimentato o non alimentato
- Prestazioni del logic solver (tempo di reazione, precisione ...)
- Requisiti di prestazioni
 - Tolleranza guasti
 - Integrità
 - Frequenza max. di intervento spurio (STR)
 - Frequenza max. di guasti pericolosi
- Specifiche ambientali (dati EMC, meccanici, chimici, relativi al clima...)

Passaggio 10: Realizzazione dei sistemi di sicurezza E/E/PE

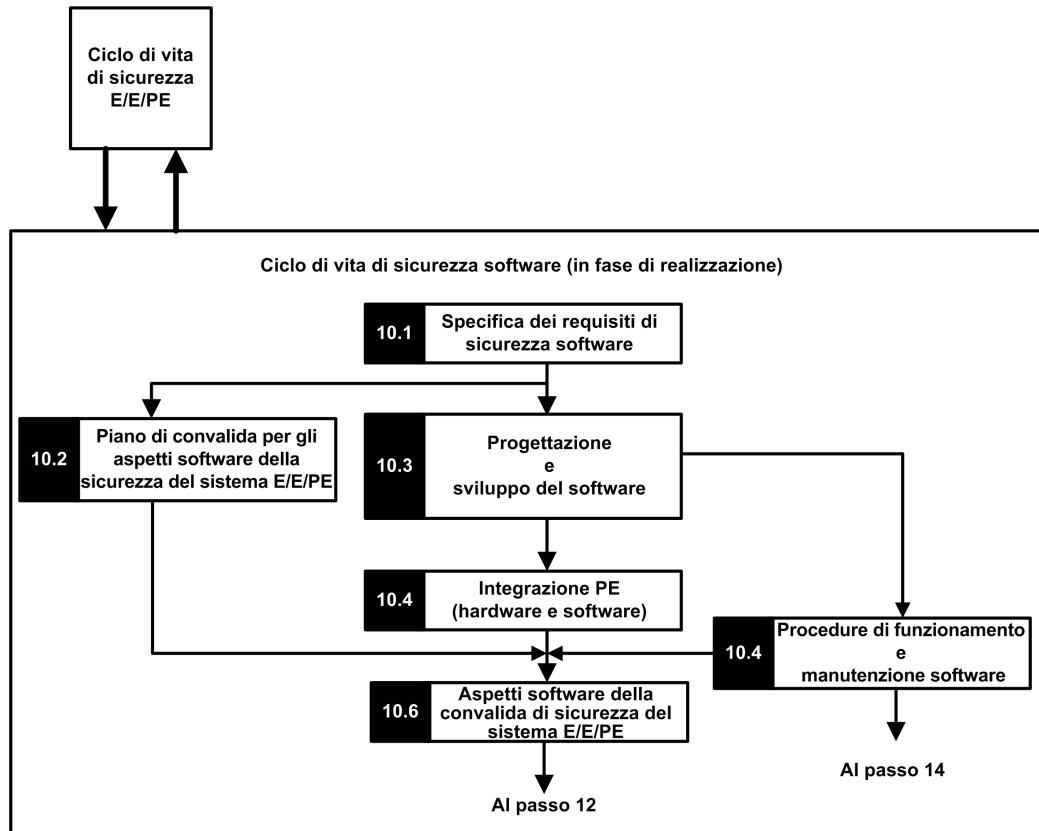
La norma IEC 61508 divide questo passo in 2 sottocicli di vita, uno per la realizzazione del sistema e l'altro per la realizzazione del software.

Realizzazione del sistema:

Dal passo 10



Realizzazione del software:



L'obiettivo del primo sottopasso (10.1) è quello di convertire i requisiti di sicurezza del SIS in specifiche per la progettazione hardware, test dell'hardware, progettazione software, test del software e test di integrazione. In questa fase si devono fornire come minimo le informazioni necessarie per progettare un'applicazione sicura utilizzando un M580 di sicurezza:

- Architettura hardware che tiene conto dei seguenti fattori:
 - Rispetto delle regole M580 sulla combinazione di moduli non di sicurezza e di sicurezza: tutti i moduli di sicurezza (moduli di IO sicuri e CPU/COPRO sicure) sono collocati in rack in cui il rack principale e le sue estensioni sono alimentati da un alimentatore sicuro e contengono solo moduli sicuri o moduli non interferenti del tipo 1.
 - Consumo elettrico per rack.
 - Regole di derating.

- Architettura di alimentazione:
 - Solo alimentatori SELV/PELV.
- Architettura software:
 - Incluso l'uso di variabili globali M580; una variabile globale non dovrebbe evitare l'intervento di un'azione di sicurezza a meno che non si utilizzi un "protocollo di applicazione sicuro".
- Integrazione hardware (cablaggio, cabinet, ecc.):
 - Protezione fusibili
 - Accessori per la diagnostica del cablaggio.
- Interfacce uomo-macchina:
 - Incluso l'uso di variabili globali M580; una variabile globale non dovrebbe evitare l'intervento di un'azione di sicurezza a meno che non si utilizzi un "protocollo di applicazione sicuro".
- Interfacce elettriche/numeriche:
 - Stato di sicurezza.
 - Sensore e attuatore.
- Algoritmo
- Prestazioni (inclusa definizione di periodo task, watchdog e timeout) e previsione di un comportamento corretto tramite la formula:

$$\sum_{\text{tutti } i \text{ task}} \frac{Exe_{task}}{Periodo_{task}} < 80\%$$

NOTA: la formula è applicabile solo quando il task MAST non è in modalità ciclica.

- Comportamento in caso di:
 - Configurazione sblocco
 - Modalità di manutenzione
 - Ingresso manutenzione
 - Canale non valido
 - Anomalia di cablaggio
 - Stato del canale
 - Stato del modulo
- Gestione dell'UID dei moduli di IO sicuri (definire quando un UID deve essere modificato).

- Server NTP:
 - Scelta del PAC come server NTP o server NTP esterno (in base all'uso di orodatazione degli I/O nell'applicazione di processo).
 - Ridondanza dei server
 - Perdita di server

Con i successivi passi secondari le specifiche vengono precisate in una specifica tecnica dettagliata, viene eseguita la progettazione stessa, si effettuano tutti i test pianificati e si redigono i rapporti.

Passaggio 12: Installazione e messa in servizio globali

Lo scopo di questo passo è quello di definire i requisiti per l'installazione, la pianificazione dei task, l'attrezzaggio, la procedura di messa in servizio, passando quindi a costruire il sistema e a verificarne la regolarità.

- Per applicazioni Hot Standby, verificare che il timeout di posizionamento di sicurezza, pagina 157 del moduli di uscita di sicurezza sia adatto alle condizioni definite per le operazioni di scambio, pagina 158 e switchover, pagina 160 e verificare il tempo di mantenimento CRA.
- Verificare che il timeout di posizionamento di sicurezza (S_TO) per i moduli di uscita di sicurezza sia maggiore almeno del più grande tra 40 ms o $(2,5 * T_{SAFE})$, dove T_{SAFE} è pari al periodo del task SAFE configurato.
- Cancellare ogni applicazione pre-esistente nel PLC, oppure utilizzare un'applicazione configurata senza dispositivi di sicurezza CIP prima di installare il dispositivo di sicurezza in una rete Ethernet di sicurezza (con dispositivi di sicurezza CIP).

In un sistema di sicurezza M580 la procedura di messa in servizio dovrebbe comprendere i seguenti punti:

- Verificare l'integrità di Control Expert, verificare la versione di Control Expert.
- Correttezza delle versioni firmware della CPU e del coprocessore tramite controllo delle parole di sistema %SW14 (versione firmware del processore del PLC) e %SW142 (versione firmware del coprocessore).
- Correttezza di ogni indirizzo modulo (posizione nel rack, interruttori CRA).
- Correttezza del cablaggio:
 - Verifica punto per punto: dalla variabile interna al modulo di I/O, fino all'attuatore/sensore.
 - Fusibili.
 - Apparecchiatura per diagnostica del cablaggio.
- Al termine della procedura, tutti i moduli di sicurezza sono in modalità "blocco" (è consigliabile che sia l'applicazione di sicurezza stessa a verificare questa condizione).

- Correttezza della configurazione di ogni modulo (inclusi i timeout):
 - Leggere la configurazione sulla schermata di Control Expert e confrontarla con la specifica.
- Tutte le applicazioni di sicurezza sono state ricompilate tramite l'opzione **Ricompila tutto il progetto**, quindi scaricate su ciascun PLC e il loro SAId salvato insieme all'archivio delle applicazioni.
- Il periodo del task e il watchdog del task sono corretti.
- Codici prodotto e versione dei moduli.
- Uso esclusivo di alimentazione SELV/PELV.
- Se i dispositivi CIP Safety vengono utilizzati nell'applicazione di sicurezza:
 - La firma ID di configurazione di sicurezza (SCID) può essere verificata (opzione abilitata nel DTM di CIP Safety in Control Expert) e la configurazione di destinazione bloccata in seguito alla verifica utente.
 - Per confermare che la configurazione di origine creata dall'utente con lo strumento software Control Expert è stata inviata e salvata correttamente nell'origine CIP Safety M580, confrontare visivamente tutti i valori dei parametri di configurazione di destinazione CIP Safety visualizzati nei DDDT di destinazione (in modalità connesso con PAC, utilizzando una tabella di animazione) con i valori dei parametri visualizzati e configurati nella *Scheda di verifica di configurazione*, pagina 362 del DTM di destinazione. Tutti i valori devono essere uguali.
 - Verificare tutte le configurazioni di connessione di sicurezza dopo la loro applicazione nell'origine CIP Safety M580 per confermare che ciascuna connessione di destinazione stia funzionando nel modo previsto.
 - Prima di installare i dispositivi CIP Safety su una rete di sicurezza, effettuare la messa in servizio di tutti i dispositivi di sicurezza con MaId e Velocità di trasmissione se necessario.
- La verifica utente è lo strumento per mezzo del quale convalidare tutti i download di applicazioni

Passaggio 13: Convalida sicurezza globale

Lo scopo di questo passo è quello di dimostrare che il sistema integrato di sicurezza (SIS) soddisfa i requisiti. Vengono eseguiti tutti i test e prodotti i rapporti definiti nel passo 7 del "ciclo di vita di sicurezza". Dovrebbe comprendere:

- Verificare l'assenza di condizioni di overrun durante gli stati del sistema (verifica del bit di sistema %S19 nei task MAST, FAST, AUX0 e che il tempo di esecuzione massimo e corrente del task SAFE (%SW42 e %SW43) sia inferiore al periodo del task SAFE.

$$\sum_{\text{tutti i task}} \frac{Exe_{task}}{Periodo_{task}} < 80\%$$

- Verificare la formula di carico della CPU:
NOTA: è possibile utilizzare le parole di sistema da %SW110 a %SW115, pagina 401 per eseguire una valutazione in tempo reale del carico medio dei task della CPU (se tutti i task sono periodici, %SW116 deve essere inferiore a 80).
- Verifica dei modi operativi speciali (sblocco modulo, ingresso di manutenzione, canale non valido, difetto di cablaggio).
- Per applicazioni Hot Standby, verificare che tutti i task siano correttamente sincronizzati attraverso il collegamento Hot Standby controllando e utilizzando i bit MAST_SYNCHRONIZED, FAST_SYNCHRONIZED e SAFE-SYNCHRONIZED in T_M_ECPU_HSBY DDT. Vedere *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* per una descrizione del DTT_M_ECPU_HSBY.

Passaggio 14: Funzionamento, manutenzione e riparazione globali

- Esecuzione dei test di prova nel periodo appropriato.
- Monitoraggio del codice SAId vedere la nota.
NOTA: Se SAId non è cambiato, significa che la porzione di sicurezza dell'applicazione non è stata modificata. Per informazioni dettagliate sul comportamento del codice SAId, vedere il blocco funzione S_SYST_STAT_MX.
- Monitoraggio dello stato di blocco configurazione su ogni modulo di sicurezza.
- Registrazione delle operazioni di riparazione.
- Se un modulo viene sostituito, il dispositivo di sostituzione deve essere configurato adeguatamente e l'utente deve verificarne il funzionamento. Eseguire (come minimo) le operazioni di messa in servizio relative a questo modulo.
- Registrazione degli scostamenti.

Passaggio 15: Modifica e retrofit globale

Qualsiasi modifica deve essere considerata come un nuovo progetto. Può essere utile un'analisi dell'impatto per definire la parte del sistema di sicurezza precedente che può essere mantenuta e la parte che deve essere riprogettata.

NOTA: Se la modifica di un'applicazione non riguarda l'applicazione SAFE, è possibile utilizzare la firma di origini SAFE per verificare che nessuna modifica indesiderata sia stata inserita nel codice SAFE. La firma di origini SAFE verifica *a priori* che l'applicazione non sia stata modificata. La firma di origini SAFE non sostituisce SAId, che è l'unico strumento in grado di confermare in modo affidabile che un PAC stia eseguendo la stessa applicazione SAFE convalidata.

Moduli I/O M580 Safety

Contenuto del capitolo

Funzioni condivise dei moduli di I/O di sicurezza M580	46
Modulo di ingresso analogico BMXSAI0410	50
Modulo di ingresso digitale BMXSDI1602	65
Modulo di uscita digitale BMXSDO0802.....	98
Modulo di uscita relè digitale BMXSRA0405.....	113

Introduzione

Questo capitolo descrive i moduli I/O M580 Safety.

Funzioni condivise dei moduli di I/O di sicurezza M580

Introduzione

Questa sezione descrive le funzioni condivise o comuni dei moduli di I/O di sicurezza M580.

Presentazione dei moduli I/O M580 Safety

Introduzione

I seguenti quattro moduli di I/O di sicurezza M580 sono certificati per l'uso nelle applicazioni di sicurezza:

- BMXSAI0410 (ingresso analogico)
- BMXSDI1602 (ingresso digitale)
- BMXSDO0802 (uscita digitale)
- BMXSRA0405 (uscita relè digitale)

I quattro moduli di I/O di sicurezza permettono di collegare il PAC di sicurezza ai sensori e agli attuatori che fanno parte del loop di sicurezza. Ogni modulo di I/O di sicurezza include un processore di sicurezza dedicato. Questi moduli di I/O possono essere installati nel backplane locale o nelle derivazioni RIO.

Requisiti per l'installazione e per la custodia

Installare l'apparecchiatura di sicurezza M580 in modo che soddisfi i seguenti requisiti:

- Il grado di inquinamento 2 secondo IEC 60950 per la sicurezza delle apparecchiature per la tecnologia dell'informazione; e
- lo standard IEC 60529 per la protezione degli ingressi IP54, in modo tale che:
 - la presenza di polvere non interferisca con il funzionamento dell'apparecchiatura e
 - gli spruzzi d'acqua non possano danneggiare l'apparecchiatura o il funzionamento.

In genere questi standard vengono rispettati collocando l'apparecchiatura di sicurezza in un involucro di sicurezza, ad esempio un cabinet.

Altitudine di funzionamento massima

L'altitudine operativa massima per i moduli di I/O di sicurezza M580 è 2000 m sul livello del mare.

Comunicazione tra PAC e I/O

La CPU e il coprocessore di sicurezza M580 insieme controllano tutti gli scambi sul backplane, mentre gli I/O di sicurezza rispondono ai comandi di CPU e coprocessore. I moduli di I/O di sicurezza possono essere installati in un rack X Bus BMXXBP**** o in un rack Ethernet BMEXBP****.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza nel rack principale locale avvengono tramite il backplane.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza installati in una derivazione RIO avvengono attraverso un modulo adattatore installato nella derivazione RIO:

- un adattatore BMEXRA31210 per un rack Ethernet, oppure
- un adattatore BMXCRA31210 per un rack X Bus.

NOTA: con il firmware della CPU 3.20 o successivo, la comunicazione con il PAC e gli I/O di sicurezza richiede un BM•CRA31210 con firmware 2.60 o successivo.

NOTA: un adattatore BMXCRA31200 non può essere utilizzato per collegare i moduli di I/O di sicurezza al PAC di sicurezza M580.

Opzionalmente, si possono utilizzare i moduli ripetitori a fibre ottiche BMXNRP0200 oppure BMXNRP0201 per estendere il collegamento fisico tra la CPU e il coprocessore nel rack locale e l'adattatore nella derivazione RIO. I moduli ripetitori a fibre ottiche migliorano l'immunità ai disturbi della rete RIO e garantiscono al contempo il mantenimento della massima disponibilità dinamica della rete e il livello di integrità di sicurezza.

Il protocollo di comunicazione tra gli I/O di sicurezza e il PAC consente gli scambi sulla rete. Questo protocollo permette ad entrambi i dispositivi di verificare l'accuratezza dei dati ricevuti, di rilevare eventuali dati corrotti e di determinare se il modulo di trasmissione diventa non operativo. Pertanto, un loop di sicurezza può includere qualsiasi adattatore RIO e backplane non interferente, pagina 29.

Alimentazione esterna utilizzata con gli I/O di sicurezza digitali

I moduli digitali BMXSDI1602 e BMXSDO0802 richiedono un alimentatore esterno a tensione ultra bassa protetta 24 Vcc (SELV/PELV) per fornire alimentazione ai sensori e agli attuatori. I moduli di I/O di sicurezza supervisionano l'alimentatore di processo non di sicurezza per rilevare eventuali condizioni di sovratensione e sottotensione.

PERICOLO

RICHIESTO ALIMENTATORE SELV/PELV CATEGORIA DI SOVRATENSIONE II

Utilizzare solo un alimentatore SELV/PELV di categoria di sovratensione II, con uscita massima di 60 Vcc, per alimentare sensori e attuatori.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

Panoramica della diagnostica per i moduli di I/O di sicurezza M580

Introduzione

Ogni modulo di I/O di sicurezza M580 dispone delle seguenti funzioni di diagnostica:

- Autotest all'avvio del modulo
- Autotest continuo al runtime integrato
- LED di diagnostica del modulo e del canale

Inoltre, i moduli di I/O di sicurezza digitali eseguono anche la diagnostica del cablaggio.

Autotest all'accensione

All'accensione, i moduli di I/O eseguono un'ampia serie di autotest. Se i risultati di questi test sono:

- Positivi: i moduli sono considerati funzionanti e sono operativi.
- Negativi: i moduli non sono considerati funzionanti e non sono operativi. In questo caso, gli ingressi vengono impostati a 0 e le uscite vengono disattivate.

NOTA: Se a un modulo di ingresso digitale o un modulo di uscita digitale non è collegata l'alimentazione 24 Vdc esterna, gli autotest all'accensione non vengono eseguiti e il modulo non si avvia.

Autotest continuo al runtime integrato

Durante il runtime, i moduli di I/O eseguono continuamente una serie di autotest. I moduli di ingresso verificano di potere leggere i dati provenienti dai sensori in tutto il campo. I moduli di uscita verificano che lo stato attuale dell'uscita corrisponda allo stato richiesto.

LED

Ogni modulo I/O di sicurezza dispone di una serie di LED di diagnostica del modulo e del canale sul lato anteriore del modulo:

- I quattro LED superiori (**Run**, **Err**, **I/O** e **Lck**) descrivono insieme lo stato del modulo.
- Le due o quattro (a seconda del modulo) file inferiori di LED, insieme alle quattro file di LED superiori, descrivono lo stato di ogni canale di ingresso o di uscita.

Per maggiori informazioni sulla lettura dei LED del modulo, vedere la sezione relativa alla diagnostica mediante LED dei seguenti moduli di I/O di sicurezza:

- modulo di ingresso analogico di sicurezza BMXSAI0410 , pagina 232
- modulo di ingresso digitale di sicurezza BMXSDI1602 , pagina 237
- modulo di uscita digitale di sicurezza BMXSDO0802 , pagina 243
- modulo di uscita relè digitale di sicurezza BMXSRA0405 , pagina 248

Diagnostica del cablaggio dei moduli digitali

Sia il modulo di ingresso digitale di sicurezza che il modulo di uscita digitale di sicurezza possono rilevare le seguenti condizioni di diagnostica del cablaggio del canale:

- Conduttore aperto (o interrotto).
- Cortocircuito a 0 V verso terra.
- Cortocircuito a 24 Vcc.
- Circuiti incrociati tra due canali.

NOTA: La disponibilità di queste funzioni di diagnostica dipende dalla struttura di cablaggio specifica del modulo con i rispettivi dispositivi di campo. Per maggiori informazioni, vedere gli esempi di cablaggio dell'applicazione per i seguenti moduli di I/O digitali di sicurezza:

- modulo di ingresso digitale di sicurezza BMXSDI1602 , pagina 73
- modulo di uscita digitale di sicurezza BMXSDO0802 , pagina 102

Modulo di ingresso analogico BMXSAI0410

Introduzione

Questa sezione descrive il modulo di ingresso analogico di sicurezza BMXSAI0410 M580.

Modulo di ingresso analogico di sicurezza BMXSAI0410

Introduzione

Il modulo di ingresso analogico di sicurezza BMXSAI0410 presenta le seguenti caratteristiche:

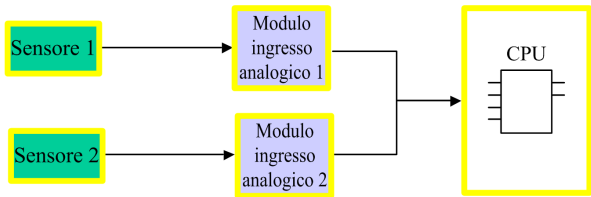
- 4 canali di ingresso di corrente analogici isolati da 4...20 mA.
- 12500 conteggi risoluzione, nel campo dati 0...25 mA.
- Rilevamento di corrente fuori campo per valori di corrente inferiori a 3,75 mA o maggiori di 20,75 mA.
- Supporta i seguenti standard SIL3 (IEC61508):
 - Il modulo è in grado di raggiungere fino a Categoria 2 (Cat2) / Performance Level d (PLd) utilizzando 1 canale di ingresso (valutazione uno su uno (1oo1)). È quindi possibile ottenere Cat1 e Cat2 / PL a, b, c, d utilizzando 1 canale di ingresso.
 - Il modulo è in grado di raggiungere fino a Categoria 4 (Cat4) / Performance Level e (PLe) utilizzando 2 canali di ingresso (valutazione uno su due (1oo2)). È quindi possibile ottenere Cat3 e Cat4 / PL d, e utilizzando 2 canali di ingresso.
- Visualizzazione diagnostica mediante LED, pagina 232 fornita per il modulo e per ogni canale di ingresso.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 258. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 257).

Alta disponibilità

È possibile configurare l'applicazione di sicurezza con vari livelli di prestazioni e disponibilità, utilizzando canali e moduli di ingresso singoli o ridondanti, nel seguente modo:

Progettazione:	Livelli della funzione di sicurezza:			
Canali di ingresso => Moduli	SIL	Cat	PL	Alta disponibilità?
Da canale di ingresso singolo a modulo di ingresso singolo, pagina 56	SIL3	Cat 2	PLd	–
Da canale di ingresso singolo a moduli di ingresso ridondanti, pagina 57	SIL3	Cat 2	PLd	✓
Da canali di ingresso ridondanti a modulo di ingresso singolo, pagina 58	SIL3	Cat 4	PLe	–
Da canali di ingresso ridondanti a moduli di ingresso ridondanti, pagina 59	SIL3	Cat 4	PLe	✓
✓ : Fornito – : Non fornito				

La seguente figura illustra la configurazione degli ingressi analogici ridondanti:



Il valore di corrente dell'ingresso analogico del sensore 1 e del sensore 2 vengono inviati dal modulo di ingresso 1 e dal modulo di ingresso 2, rispettivamente, a una CPU di sicurezza attraverso un black channel. La CPU esegue un blocco funzione dedicato (S_AIHA), in ciascuno dei due programmi di logica compilati separati, per gestire e selezionare i dati provenienti dai due moduli di ingresso. Questo blocco funzione opera nel seguente modo:

- Se lo stato dei dati di ingresso provenienti dal modulo 1 è corretto, i dati di ingresso provenienti da questo modulo vengono utilizzati nella funzione di sicurezza.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 non è corretto, ma lo stato dei dati di ingresso provenienti dal modulo 2 è corretto, vengono utilizzati i dati di ingresso del modulo 2.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 e dal modulo 2 non è corretto, il sistema attiva la funzione di sicurezza.

Connettore di cablaggio BMXSAI0410

Introduzione

Il modulo di ingresso analogico BMXSAI0410 include 4 ingressi analogici. Il modulo dispone di due coppie di contatti per ogni ingresso: due contatti di canale (Ch) positivi e due contatti comuni (Com) negativi.

Per ogni ingresso:

- i due contatti del canale (Ch n) sono collegati internamente e
- anche i due contatti comuni (Com n) sono collegati internamente.

Per collegare un sensore analogico a un ingresso, è possibile utilizzare un contatto del canale o un contatto comune per tale ingresso.

Morsettiere

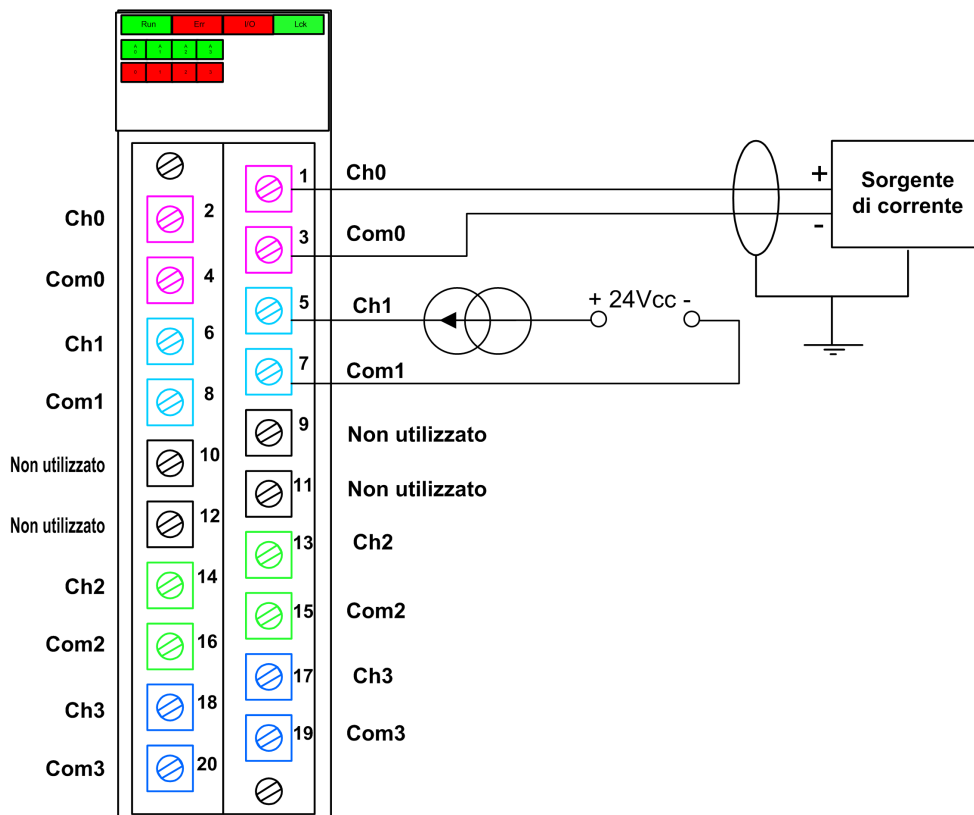
Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera tipo Cage Clamp BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Connettore di cablaggio

L'esempio seguente presenta uno schema di cablaggio generico per ingressi sul modulo:



NOTA: Il modulo rileva una condizione di conduttore interrotto e la segnala come condizione di corrente fuori campo (inferiore a 3,75 mA) impostando l'elemento `00R` della struttura `T_U_ANA_SIS_CH_IN`, pagina 63 a "1".

Mappatura degli ingressi ai contatti del connettore

La seguente sezione fornisce una descrizione di ogni contatto del modulo di ingresso analogico BMXSAI0410:

Descrizione del contatto	Numero del contatto sulla morsettieria		Descrizione del contatto
Ingresso (+) del canale 0	2	1	Ingresso (+) del canale 0
Ingresso (-) del canale 0	4	3	Ingresso (-) del canale 0

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Ingresso (+) del canale 1	6	5	Ingresso (+) del canale 1
Ingresso (-) del canale 1	8	7	Ingresso (-) del canale 1
Non usato	10	9	Non usato
Non usato	12	11	Non usato
Ingresso (+) del canale 2	14	13	Ingresso (+) del canale 2
Ingresso (-) del canale 2	16	15	Ingresso (-) del canale 2
Ingresso (+) del canale 3	18	17	Ingresso (+) del canale 3
Ingresso (-) del canale 3	20	19	Ingresso (-) del canale 3

NOTA: Dato che i due contatti positivi di ogni ingresso sono collegati internamente, si deve usare solo un contatto positivo per un canale di ingresso. Analogamente, dato che i due contatti negativi di ogni ingresso sono collegati internamente, si deve usare solo un contatto negativo per ogni canale di ingresso.

Ad esempio, per collegare un sensore analogico al canale di ingresso 0, si può collegare:

- il conduttore positivo del sensore al contatto 1 o 2.
- il conduttore negativo del sensore al contatto 3 o 4.

BMXSAI0410 Esempi di cablaggio dell'applicazione di ingresso

Introduzione

È possibile cablare il modulo di ingresso analogico di sicurezza BMXSAI0410 a dei sensori analogici per raggiungere la conformità SIL3 in molti modi diversi, a seconda dei seguenti fattori:

- lo standard richiesto di Category (Cat2 o Cat4) e Performance Level (PLd o PLe)
- i requisiti di alta disponibilità dell'applicazione.

▲ ATTENZIONE

RISCHIO DI FUNZIONAMENTO ANOMALO

Il livello di integrità di sicurezza (SIL) massimo è determinato dalla qualità del sensore e dalla lunghezza dell'intervallo del test di prova per IEC 61508. Se si utilizzano sensori non conformi alla qualità dello standard SIL previsto, cablare sempre questi sensori in modo ridondante a due canali.

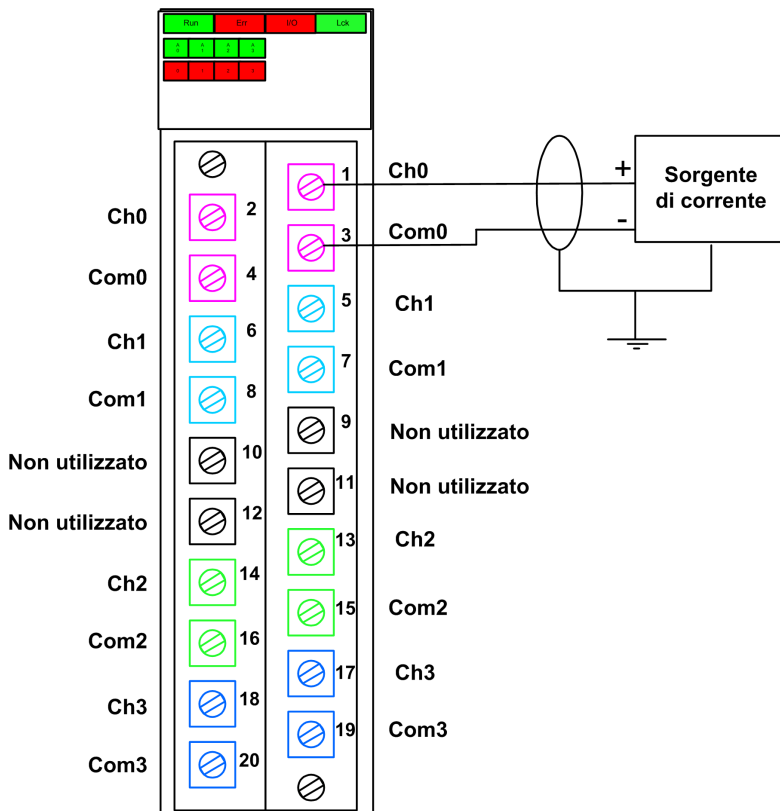
Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di ingresso digitale SIL3:

- Cat2/PLd:
 - un solo sensore collegato a un ingresso.
- Cat2/PLd con alta disponibilità:
 - due sensori cablati a due punti di ingresso su moduli di ingresso diversi.
- Cat4/PLe:
 - due sensori, ognuno dei quali cablato a un punto di ingresso diverso sullo stesso modulo di ingresso.
- Cat4/PLe con alta disponibilità:
 - due coppie di sensori (per un totale di quattro sensori): i sensori della prima coppia sono singolarmente cablati a un punto di ingresso diverso su un modulo e i sensori della seconda coppia sono singolarmente cablati a un punto di ingresso diverso su un secondo modulo.

SIL3 Cat2/PLd

L'esempio seguente presenta un solo sensore collegato a un punto di ingresso su un singolo modulo di ingresso. La CPU esegue la valutazione 1oo1D sul singolo valore monitorato:



⚠ ATTENZIONE

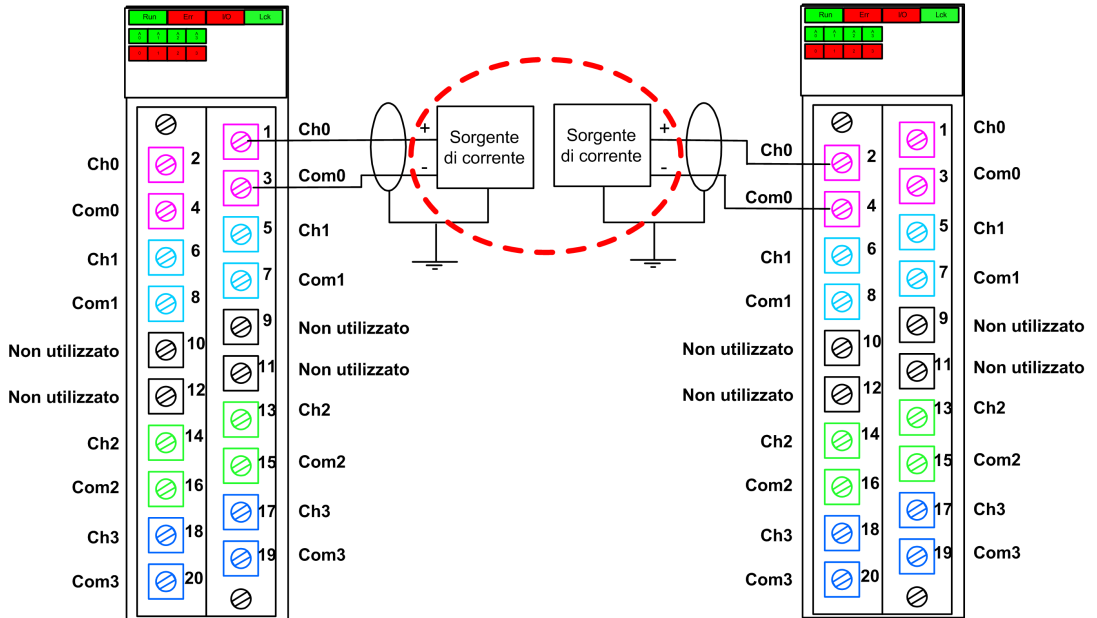
RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 2/Performance Level d secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare un sensore qualificato idoneo.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

SIL3 Cat2/PLd con alta disponibilità

L'esempio seguente presenta due sensori che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso su vari moduli di ingresso. La CPU esegue la valutazione 1oo1D del singolo valore monitorato:



NOTA: In questa configurazione, utilizzare il blocco funzione `S_AIHA` nel task SAFE per gestire i due valori delle variabili di processo forniti dai due sensori.

⚠ ATTENZIONE

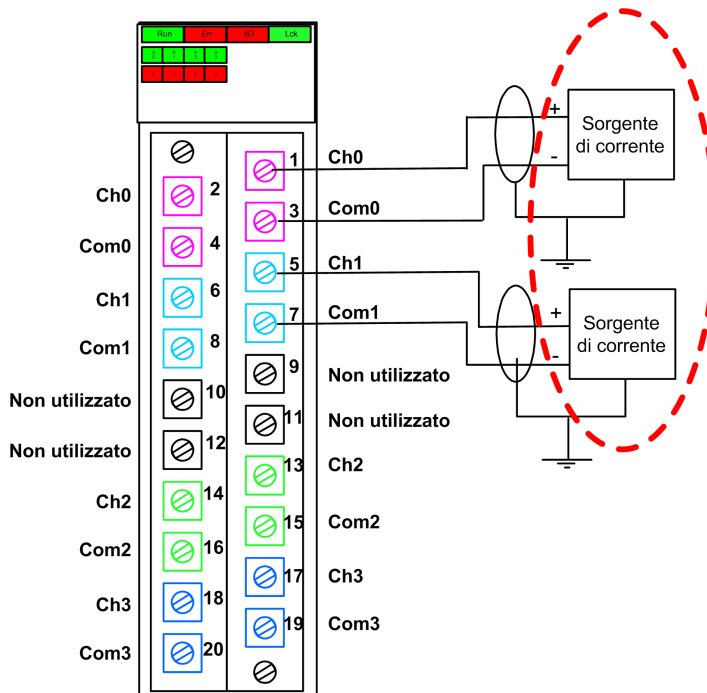
RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 2/Performance Level d secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare un sensore qualificato idoneo.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

SIL3 Cat4/PLe

L'esempio seguente presenta due sensori che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso sullo stesso modulo di ingresso. La CPU esegue una valutazione 1oo2D dei valori concorrenti forniti dai due sensori per la stessa variabile di processo:



NOTA: In questa configurazione, utilizzare il blocco funzione `S_AI_COMP` nel task `SAFE` per effettuare una valutazione 1oo2D dei valori concorrenti provenienti dai due sensori.

⚠ ATTENZIONE

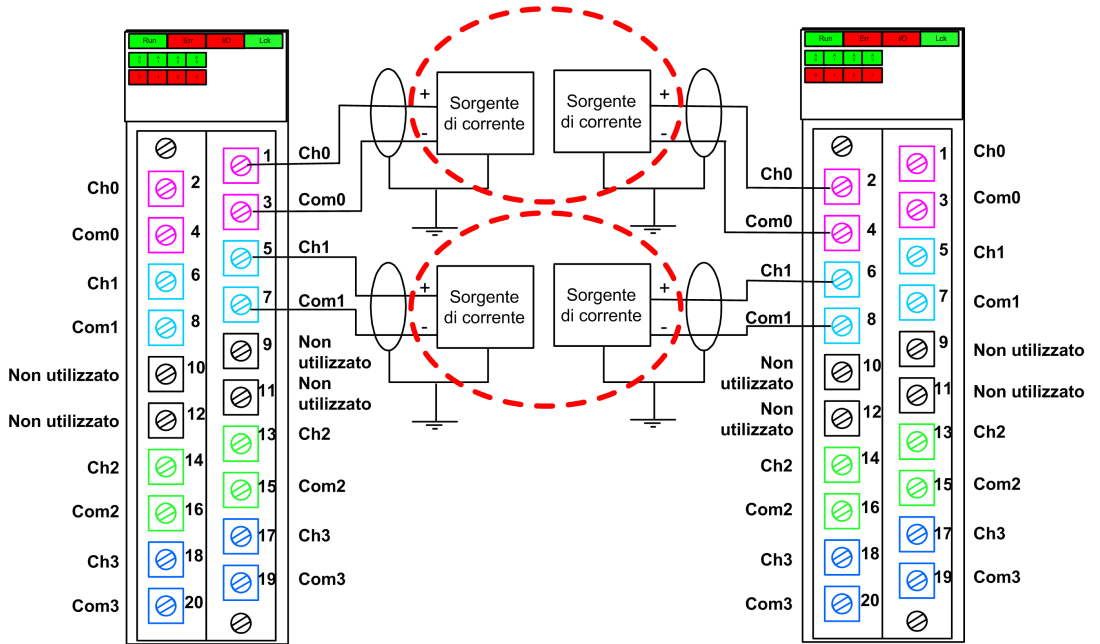
RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare un sensore qualificato idoneo.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

SIL3 Cat4/PLe con alta disponibilità

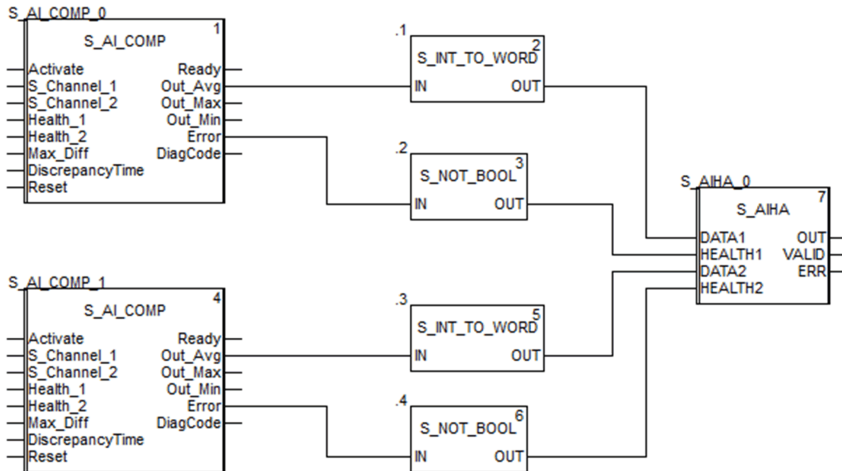
L'esempio seguente presenta due coppie sensori ridondanti che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso su due diversi moduli di ingresso (due ingressi in ogni modulo). Questa configurazione permette alla CPU di eseguire una valutazione 1oo2D:



NOTA: In questa configurazione occorre utilizzare i blocchi funzione S_AI_COMP e S_AIHA nell'ambito del task SAFE per gestire i quattro segnali di ingresso:

- S_AI_COMP per eseguire la valutazione 1oo2 di due coppie di valori provenienti dai due sensori collegati allo stesso modulo.
- S_AIHA per gestire la funzione di alta disponibilità.

Il seguente diagramma dei blocchi funzione illustra la configurazione del segmento di codice indicato sopra:



⚠ ATTENZIONE

RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare un sensore qualificato idoneo.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

BMXSAI0410 Struttura dei dati

Introduzione

Il tipo di dati derivati `T_U_ANA_SIS_IN_4` del dispositivo (DDDT) è l'interfaccia tra il modulo di ingresso analogico `BMXSAI0410` e l'applicazione eseguita nella CPU. Il DDDT `T_U_ANA_SIS_IN_4` include i tipi di dati `T_SAFE_COM_DBG_IN` e `T_U_ANA_SIS_CH_IN`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT `T_U_ANA_SIS_IN_4`

La struttura DDDT `T_U_ANA_SIS_IN_4` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il modulo funziona correttamente. 0: il modulo non funziona correttamente. 	RO
SAFE_COM_STS ¹	BOOL	<ul style="list-style-type: none"> 1: comunicazione del modulo valida. 0: comunicazione del modulo non valida. 	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Struttura di debug comunicazione sicura.	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> 1: configurazione del modulo bloccata. 0: configurazione del modulo non bloccata. 	RO
CH_IN	ARRAY[0...3] di T_U_ANA_SIS_CH_IN	Array di struttura del canale.	–
MUID ²	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED	ARRAY[0...9] di INT	-	–
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.</p> <p>2. Questo valore autogenerato può essere modificato eseguendo il comando Crea > Rinnova ID & Ricrea tutto nel menu principale di Control Expert.</p>			

Struttura T_SAFE_COM_DBG_IN

La struttura T_SAFE_COM_DBG_IN include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso ¹
S_COM_EST	BOOL	<ul style="list-style-type: none"> 1: comunicazione con il modulo stabilita. 0: la comunicazione con il modulo non è stabilita o è disturbata. 	RO
M_NTP_SYNC	BOOL	<p>Con firmware della CPU 3.10 o precedente:</p> <ul style="list-style-type: none"> 1: il modulo è sincronizzato con il server NTP. 0: il modulo non è sincronizzato con il server NTP. <p>NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con firmware della CPU 3.10 o precedente:</p> <ul style="list-style-type: none"> 1: la CPU è sincronizzata con il server NTP. 0: la CPU non è sincronizzata con il server NTP. <p>NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.</p>	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	<p>Ritardo di comunicazione tra due valori ricevuti dal modulo:</p> <ul style="list-style-type: none"> 1...65534: il tempo, in ms, trascorso dalla ricezione da parte della CPU dell'ultima comunicazione del modulo. 65535: la CPU non ha ricevuto una comunicazione dal modulo. 	RO
COM_TO	UINT	<p>Valore di timeout di comunicazione proveniente dal modulo.</p> <p>NOTA: Può essere utile modificare questo valore di lettura/scrittura per renderlo equivalente o maggiore del tempo di comunicazione effettivo per il modulo (ad es. in una derivazione RIO remota).</p>	R/W
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO

Elemento	Tipo di dati	Descrizione	Accesso ¹
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO

Struttura T_U_ANA_SIS_CH_IN

La struttura T_U_ANA_SIS_CH_IN include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
FCT_TYPE	WORD	<ul style="list-style-type: none"> 1: il canale è attivato. 0: il canale non è attivato. 	RO
CH_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il canale è funzionante. 0: è stato rilevato un errore sul canale che non è operativo. <p>Formula: CH_HEALTH = non (OOR o IC) e SAFE_COM_STS</p>	RO
VALUE	INT	<p>Valore di ingresso analogico.</p> <p>Formula: VALUE = se (SAFE_COM_STS e non(IC)) allora READ_VALUE diverso da 0</p>	RO
OOR	BOOL	<ul style="list-style-type: none"> 1: Il valore della corrente di ingresso del canale è fuori intervallo, per i seguenti motivi: <ul style="list-style-type: none"> <3,75 mA >20,75 mA 0: il valore di corrente di ingresso del canale non è fuori intervallo. 	RO
IC	BOOL	<ul style="list-style-type: none"> 1: canale non valido rilevato dal modulo. 0: il canale è dichiarato internamente operativo dal modulo. 	RO

1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.

Modulo di ingresso digitale BMXSDI1602

Introduzione

Questa sezione descrive il modulo di ingresso digitale di sicurezza BMXSDI1602 M580.

Modulo di ingresso digitale di sicurezza BMXSDI1602

Introduzione

Il modulo di ingresso di sicurezza BMXSDI1602 presenta le seguenti caratteristiche:

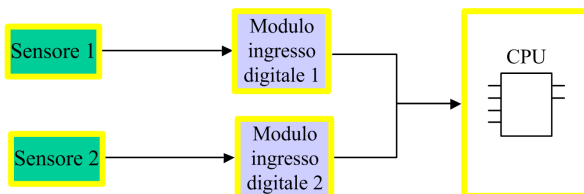
- 16 ingressi del tipo 3 (IEC61131-2), in due gruppi elettricamente non isolati di 8 ingressi.
- Tensione di ingresso nominale 24 Vcc.
- Si ottiene quanto segue:
 - SIL3 IEC61508, SILCL3 IEC62061.
 - SIL4 EN5012x.
 - Categoria 2 (Cat2) / Performance Level d (PLd) ISO13849 ottenuta con 1 canale di ingresso (valutazione uno su uno (1oo1D)).
 - Categoria 4 (Cat4) / Performance Level e (PLe) ISO13849 ottenuta con 2 canali di ingresso (valutazione uno su due (1oo2D)).
- Compatibile con sensori di prossimità a 2 o 3 fili.
- Fornisce in opzione due uscite 24 Vcc (VS1 e VS2) per la supervisione di cortocircuito 24 Vcc:
 - VS1 per monitorare il cortocircuito sugli ingressi 0...3 (rank A e B).
 - VS2 per monitorare il cortocircuito sugli ingressi 4...7 (rank A e B).
- Monitoraggio della tensione di alimentazione esterna 24 Vcc.
- Visualizzazione diagnostica mediante LED, pagina 237 fornita per il modulo e per ogni canale di ingresso.

- Diagnostica del cablaggio del canale configurabile (attiva/disattiva), pagina 74 in grado di rilevare le seguenti condizioni:
 - Conduttore aperto (o interrotto).
 - Cortocircuito a 0 V verso terra.
 - Cortocircuito a 24 Vcc (se l'alimentazione al sensore è fornita internamente).
 - Circuiti incrociati tra i due canali (se l'alimentazione al sensore è fornita internamente).
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 258. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 257).

Alta disponibilità

È possibile usare due sensori collegati a due canali di ingresso diversi situati su moduli di ingresso diversi per monitorare lo stesso valore fisico, aumentando così la disponibilità del sistema.

La figura seguente illustra le configurazioni di ingressi digitali ridondanti:



Il valore di stato dell'ingresso del sensore 1 e del sensore 2 vengono inviati dal modulo di ingresso 1 e dal modulo di ingresso 2, rispettivamente, a una CPU di sicurezza attraverso un black channel. La CPU esegue un blocco funzione dedicato, S_DIHA, per gestire e selezionare i dati provenienti dai due moduli di ingresso. Questo blocco funzione opera nel seguente modo:

- Se lo stato dei dati di ingresso provenienti dal modulo 1 è corretto, i dati di ingresso provenienti da questo modulo vengono utilizzati nella funzione di sicurezza.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 non è corretto, ma lo stato dei dati di ingresso provenienti dal modulo 2 è corretto, vengono utilizzati i dati di ingresso del modulo 2.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 e dal modulo 2 non è corretto, lo stato dell'ingresso è impostato allo stato sicuro ("0") per attivare la funzione di sicurezza.

Per maggiori dettagli su come cablare il modulo per l'alta disponibilità, vedere la descrizione degli esempi di cablaggio dell'applicazione di ingresso, pagina 73.

Connettore di cablaggio BMXSDI1602

Introduzione

Il modulo di ingresso BMXSDI1602 digitale presenta 16 ingressi in due gruppi di 8 ingressi. Il primo gruppo è composto dagli ingressi 0...3 (rank A e B) e il secondo gruppo è composto dagli ingressi 4...7 (rank A e B). Questi due gruppi non sono isolati tra di loro.

L'alimentazione può essere fornita ai sensori sia direttamente da un alimentatore esterno, sia internamente tramite gli alimentatori VS1 e VS2. Le due strutture sono presentate più avanti.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera tipo Cage Clamp BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario un alimentatore di processo a tensione ultra bassa protetta (SELV/PELV) di categoria di sovratensione II da 24 Vcc. Schneider Electric raccomanda di impiegare un alimentatore che non esegua il ripristino automatico dell'alimentazione dopo un'interruzione di corrente.

PERICOLO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Utilizzare solo un alimentatore di processo di tipo SELV/PELV con uscita massima di 60 V.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

Fusibile

Per proteggere l'alimentatore esterno dai cortocircuiti e da eventuali condizioni di sovratensione, è necessario un fusibile rapido.

AVVISO

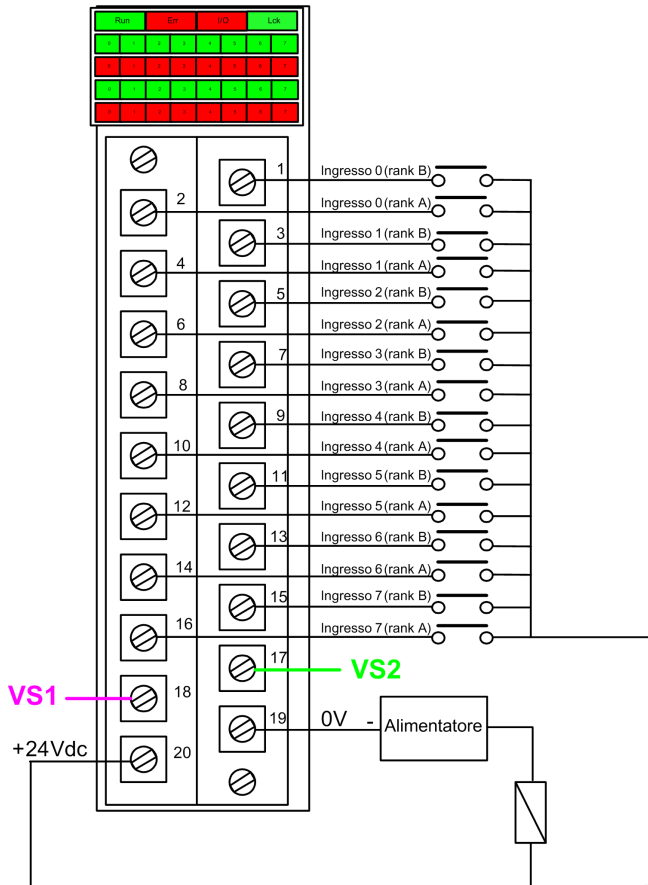
SCELTA ERRATA DEL FUSIBILE

Utilizzare fusibili rapidi per proteggere i componenti elettronici del modulo di ingresso digitale da una condizione di sovracorrente. Una scelta errata del fusibile può causare danni al modulo di ingresso.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Connettore di cablaggio: sensori con alimentazione esterna

Nella seguente struttura, i sensori sono alimentati direttamente da un alimentatore esterno:



Alimentazione: 24Vdc

fusibile: fusibile ad azione veloce da 0,5 A

NOTA: L'alimentazione dei sensori dall'esterno limita la diagnostica dei canali che il modulo può effettuare. In questa configurazione di cablaggio, il modulo può rilevare:

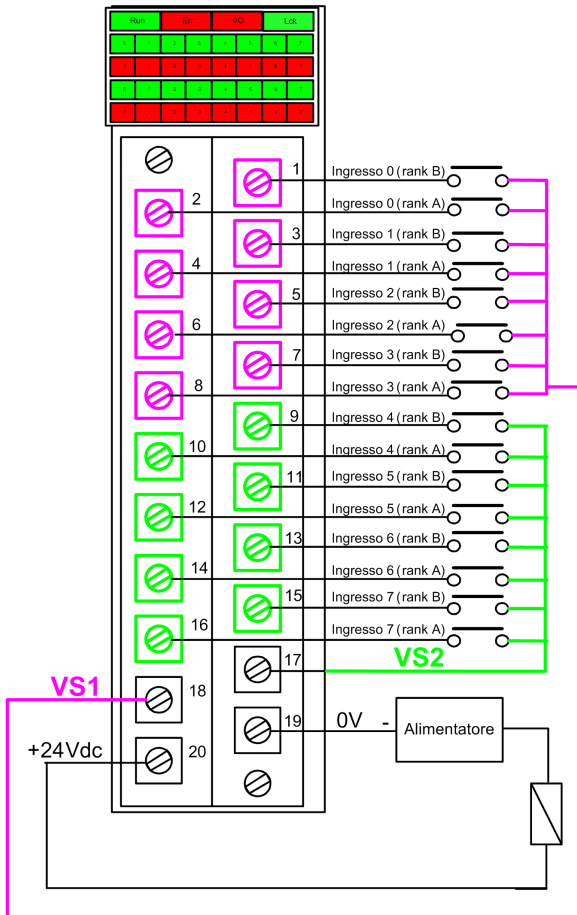
- Una condizione di conduttore interrotto (o aperto), se attivato per il canale in Control Expert.
- Una condizione di cortocircuito verso terra.

Tuttavia, in questa configurazione il modulo non è in grado di rilevare:

- Una condizione di cortocircuito a 24 Vcc.
- Una condizione di circuito incrociato con un altro ingresso di cablaggio.

Connettore di cablaggio: sensori con alimentazione interna VS

Nella seguente configurazione, i sensori per i canali 0...3 sono alimentati dall'alimentatore VS1 monitorato e i sensori per i canali 4...7 sono alimentati dall'alimentatore VS2 monitorato:



Se si usa questa configurazione, applicare l'alimentazione interna ai gruppi di canali nel seguente modo:

- Utilizzare VS1 per alimentare i canali 0...3 (rank A e B).
- Utilizzare VS2 per alimentare i canali 4...7 (rank A e B).

NOTA: In questa configurazione, il modulo può rilevare:

- Una condizione di cortocircuito a 24 Vcc, se attivato per il canale in Control Expert.
- Una condizione di circuito incrociato con un altro ingresso di cablaggio.
- Una condizione di conduttore interrotto (o aperto), se attivato per il canale in Control Expert.
- Una condizione di cortocircuito verso terra.

Mappatura degli ingressi ai contatti del connettore e ai canali Control Expert

La seguente tabella fornisce una descrizione di ogni contatto del modulo di ingresso BMXSDI1602 e assegna ogni contatto al relativo canale, come indicato nella scheda **Configurazione** del canale per il modulo in Control Expert Safety:

Canale Control Expert	Descrizione del contatto	Numero del contatto sulla morsettieria		Descrizione del contatto	Canale Control Expert
0	Ingresso 0 (rank A)	2	1	Ingresso 0 (rank B)	8
1	Ingresso 1 (rank A)	4	3	Ingresso 1 (rank B)	9
2	Ingresso 2 (rank A)	6	5	Ingresso 2 (rank B)	10
3	Ingresso 3 (rank A)	8	7	Ingresso 3 (rank B)	11
4	Ingresso 4 (rank A)	10	9	Ingresso 4 (rank B)	12
5	Ingresso 5 (rank A)	12	11	Ingresso 5 (rank B)	13
6	Ingresso 6 (rank A)	14	13	Ingresso 6 (rank B)	14
7	Ingresso 7 (rank A)	16	15	Ingresso 7 (rank B)	15
–	Alimentatore VS1	18	17	Alimentatore VS2	–
–	Alimentazione di processo 24 Vcc	20	19	Alimentazione di processo 24 Vcc	–

BMXSDI1602 Esempi di cablaggio dell'applicazione di ingresso

Introduzione

È possibile cablare il modulo di ingresso digitale di sicurezza BMXSDI1602 a dei sensori per raggiungere la conformità SIL3 in molti modi diversi, a seconda dei seguenti fattori:

- lo standard richiesto di Category (Cat2 o Cat4) e Performance Level (PLd o PLe)
- i requisiti di alta disponibilità dell'applicazione.

⚠ ATTENZIONE

RISCHIO DI FUNZIONAMENTO ANOMALO

Il livello di integrità di sicurezza (SIL) massimo è determinato dalla qualità del sensore e dalla lunghezza dell'intervallo del test di prova per IEC 61508. Se si utilizzano sensori non conformi alla qualità dello standard SIL previsto, cablare sempre questi sensori in modo ridondante a due canali.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di ingresso digitale SIL3:

- Cat2/PLd:
 - un sensore singolo collegato a un ingresso
- Cat2/PLd con alta disponibilità:
 - un sensore singolo collegato a due punti di ingresso su moduli di ingresso diversi
 - due sensori cablati a due punti di ingresso su moduli di ingresso diversi
- Cat4/PLe:
 - un sensore singolo collegato a due punti di ingresso sullo stesso modulo di ingresso
 - due sensori, ognuno dei quali cablato a un punto di ingresso diverso sullo stesso modulo di ingresso
- Cat4/PLe con alta disponibilità:
 - due sensori, ognuno dei quali cablato a due punti di ingresso diversi su moduli di ingresso diversi

Diagnostica di ingresso configurabile in Control Expert

Per il modulo di ingresso digitale di sicurezza BMXSDI1602, usare la relativa pagina **Configurazione** in Control Expert per:

- Attivare **Rilevamento cortocircuito a 24V** per ogni canale alimentato. Questo test esegue le seguenti operazioni di diagnostica del cablaggio degli attuatori per un canale:
 - Rilevamento cortocircuito a 24V.
 - Rilevamento circuiti incrociati tra due canali di uscita.

Il principio è quello fornire l'alimentazione ai sensori, per gruppi di 8 canali (con VS1 per i canali da 0 a 3 (rank A e B) e VS2 per i canali da 4 a 7 (rank A e B)). Un impulso di OFF viene applicato periodicamente a queste uscite di alimentazione con un periodo inferiore a 1 secondo e una durata inferiore a 1 ms. Durante questo impulso, se la corrente immessa nell'ingresso non è pari a 0, il modulo considera che l'ingresso è in cortocircuito.

- Attivare **Rilevamento filo aperto** per ognuno degli otto canali, che esegue la seguente diagnostica di cablaggio per quel canale:
 - Rilevamento di conduttore aperto (o interrotto) (ovvero il canale di ingresso non è collegato al sensore)
 - Rilevamento di cortocircuito a 0 Vcc verso terra.

L'obiettivo è creare artificialmente e quindi misurare una corrente di dispersione (dispersione) sulla linea (con un resistore in parallelo al sensore) quando il sensore è aperto. Se la corrente di dispersione ($0,4 \text{ mA} < \text{dispersione} < 1,3 \text{ mA}$) non può essere misurata dalla linea di ingresso dal modulo, la linea esterna viene considerata interrotta (o in una condizione di cortocircuito verso terra). La diagnostica viene eseguita con un periodo inferiore a 10 ms.

- Per un sensore a contatto secco si consiglia di collegare in parallelo al sensore una resistenza da 33 K Ω .
- Con DDP a 2 o 3 fili la corrente di dispersione deve scendere entro i limiti definiti sopra. Occorre definire il valore della resistenza da impostare in parallelo al sensore, considerando la corrente di dispersione naturale del sensore e la resistenza interna dell'ingresso (7,5 K Ω).

⚠ AVVERTIMENTO

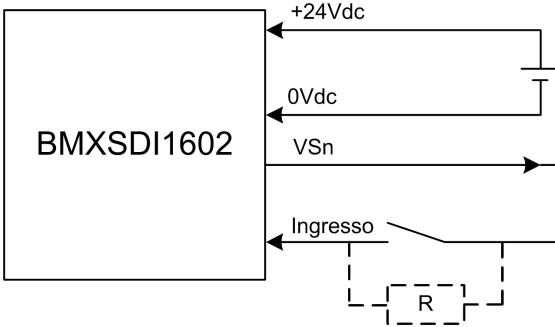
RISCHIO DI FUNZIONAMENTO IMPREVISTO

Schneider Electric consiglia di attivare la diagnostica disponibile fornita in Control Expert per rilevare o escludere le condizioni elencate sopra. Se un test di diagnostica non è attivato o non è disponibile in Control Expert, sarà necessario applicare un'altra misura di sicurezza per rilevare o escludere queste condizioni.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat2/PLd

Sensore singolo collegato a un ingresso, alimentato da VS interno:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

Dato che il sensore è alimentato internamente tramite un contatto VS, vale la seguente diagnostica di cablaggio per il canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali ¹	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

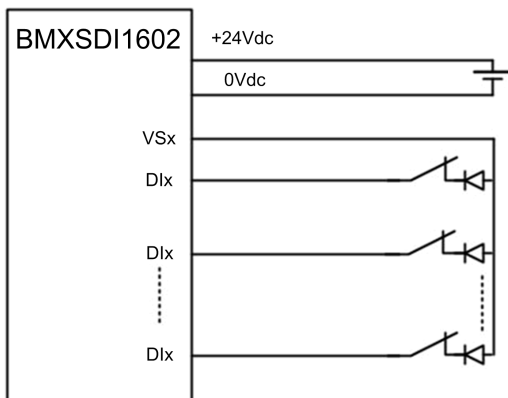
⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

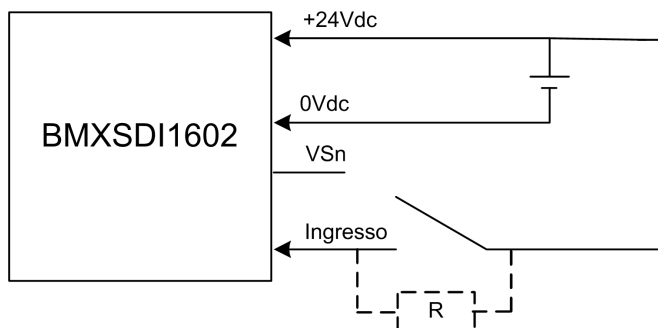
Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA: Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.



Sensore singolo collegato con un ingresso alimentato da alimentatore esterno:



Dato che il sensore è alimentato dall'esterno, si applica la seguente diagnostica del cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc	No	-
Circuiti incrociati tra due canali	No	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS (nel caso descritto sopra di un sensore singolo collegato con un ingresso alimentato da alimentatore esterno). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

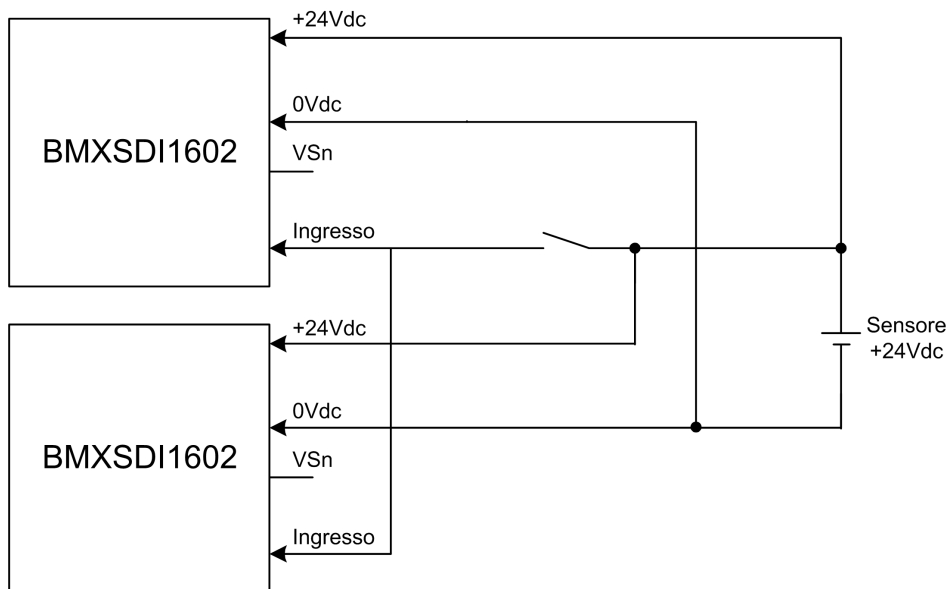
RISCHIO DI CORTOCIRCUITO A 24 VDC

Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso descritto sopra di un sensore singolo collegato con un ingresso alimentato da alimentatore esterno). È necessario adottare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat2/PLd con alta disponibilità

Sensore singolo collegato su 2 ingressi alimentati da alimentatore esterno:



Dato che il sensore è alimentato dall'esterno, si applica la seguente diagnostica del cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	No	-
Cortocircuito a 0 V verso terra	No	
Cortocircuito a 24 Vdc ¹	No	
Circuiti incrociati tra due canali	No	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare circuiti incrociati tra due canali (nel caso di un singolo sensore collegato a due ingressi, alimentati da un alimentatore esterno, come illustrato sopra). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

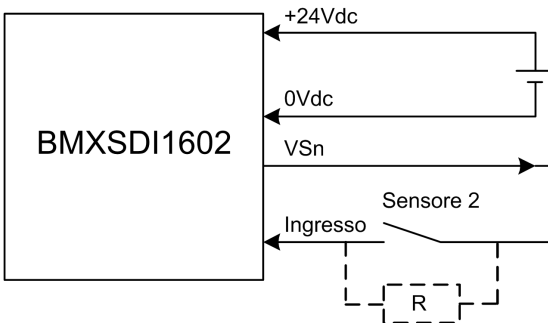
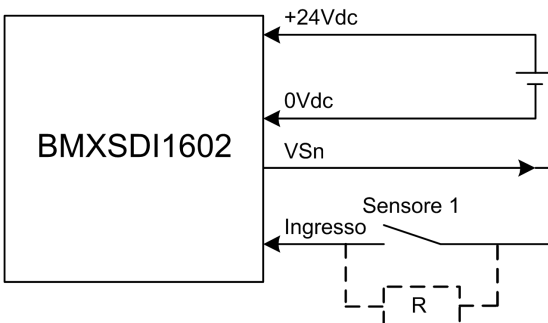
RISCHIO DI CORTOCIRCUITO A 24 VDC

Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso descritto sopra di un sensore singolo collegato con due ingressi alimentati da alimentatore esterno). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

2 sensori ridondanti collegati ai singoli ingressi di 2 moduli che utilizzano VS:

L'esempio seguente presenta due sensori ridondanti (che possono essere accoppiati meccanicamente o meno) che vengono utilizzati per acquisire la stessa variabile di processo. Ogni sensore è cablato a un singolo punto di ingresso su un modulo di ingresso diverso, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione S_DIHA per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Dato che il sensore è alimentato internamente tramite un contatto VS, vale la seguente diagnostica di cablaggio per il canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS. È necessario applicare un'altra misura di sicurezza per rilevare ed escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

2 sensori ridondanti collegati ai singoli ingressi di 2 moduli che utilizzano l'alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vdc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Dato che il sensore è alimentato internamente tramite un contatto VS, vale la seguente diagnostica di cablaggio per il canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc	No	–

Condizione	Rilevabile?	Tempo di rilevamento tipico
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

▲ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare circuiti incrociati tra due canali (nel caso di due sensori ridondanti collegati su ingressi singoli di due moduli con alimentazione esterna). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

▲ AVVERTIMENTO

RISCHIO DI CORTOCIRCUITO A 24 VDC

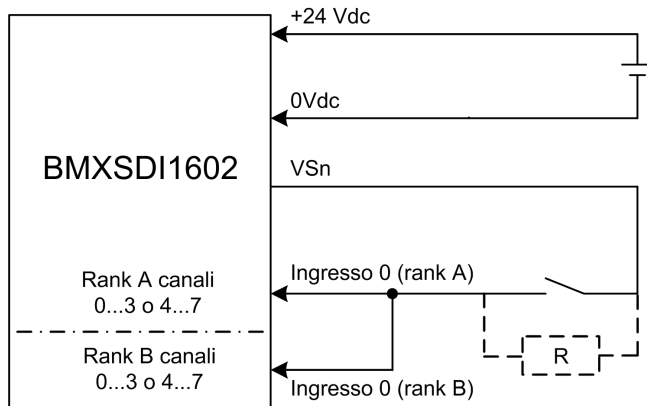
Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso di due sensori ridondanti collegati su ingressi singoli di due moduli con alimentazione esterna). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Cat4/PLe

Sensore singolo collegato su 2 ingressi dello stesso modulo con uso del modulo Vs:

L'esempio seguente presenta un sensore singolo cablato a due punti di ingresso sullo stesso modulo di ingresso, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_EQUIVALENT` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS. È necessario applicare un'altra misura di sicurezza per rilevare ed escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore singolo collegato su 2 ingressi dello stesso modulo con uso di alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vdc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	No	-
Circuiti incrociati tra due canali	No	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare circuiti incrociati tra due canali (nel caso di un singolo sensore collegato a due ingressi dello stesso modulo alimentati da un alimentatore esterno). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

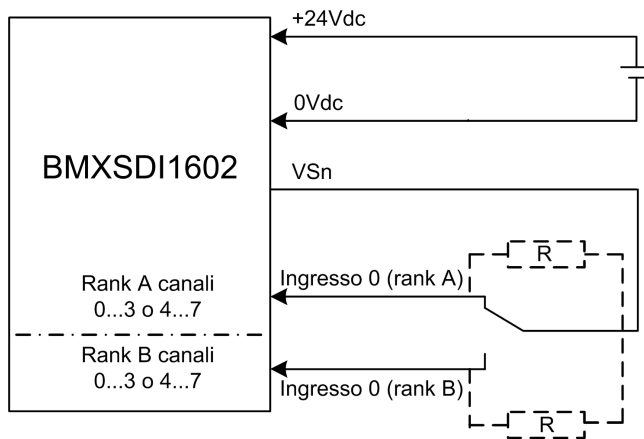
RISCHIO DI CORTOCIRCUITO A 24 VDC

Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso di un singolo sensore collegato a due ingressi dello stesso modulo alimentati da un alimentatore esterno). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore non equivalente collegato su 2 ingressi non equivalenti dello stesso modulo con uso del modulo Vs:

L'esempio seguente presenta un sensore singolo non equivalente cablato a due punti di ingresso sullo stesso modulo di ingresso, con alimentazione fornita da un alimentatore VS monitorato. Il modulo esegue una valutazione 1oo2D:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_ANTIIVALENT` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensori singoli non equivalenti collegati su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

Sensore non equivalente collegato su 2 ingressi non equivalenti dello stesso modulo con uso di alimentazione esterna:

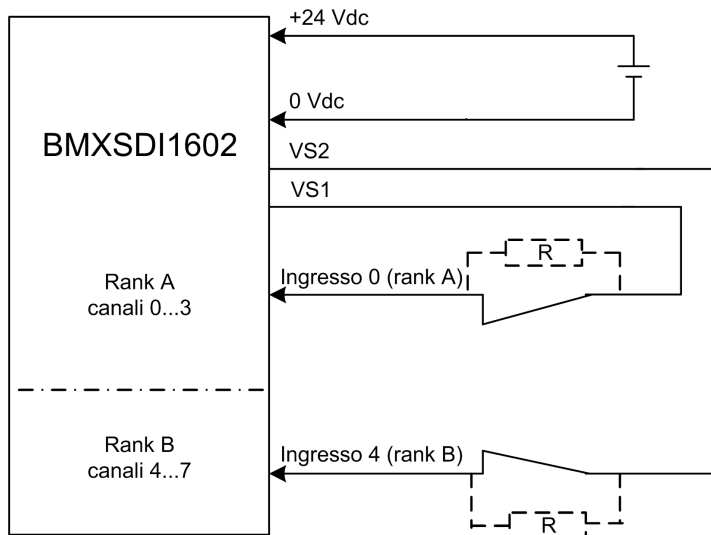
NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vdc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensori singoli non equivalenti collegati su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	No	-
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con modulo VS:

L'esempio seguente presenta due sensori ridondanti (che possono essere accoppiati meccanicamente o meno) che vengono utilizzati per acquisire la stessa variabile di processo. Ogni sensore è cablato a un singolo punto di ingresso sullo stesso modulo di ingresso, con alimentazione fornita dall'alimentatore VS monitorato:



NOTA:

- Gli ingressi 0...3 dal rank A vengono utilizzati con gli ingressi 4...7 dal rank B.
- Gli ingressi 0...3 dal rank B vengono utilizzati con gli ingressi 4...7 dal rank A.

⚠ AVVERTIMENTO

RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare sensori qualificati idonei.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione S_EQUIVALENT per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

Il modulo non è in grado di rilevare circuiti incrociati tra due canali nello stesso gruppo VS (nel caso dell'acquisizione della stessa variabile di processo tramite due sensori separati con alimentazione fornita dal modulo VS). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CORTOCIRCUITO A 24 VDC

Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso dell'acquisizione della stessa variabile di processo che utilizza due sensori separati con alimentazione fornita dall'alimentatore VS). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vdc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	No	-
Circuiti incrociati tra due canali	No	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare circuiti incrociati tra due canali (nel caso dell'acquisizione della stessa variabile di processo tramite due sensori separati con alimentazione esterna). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI FUNZIONAMENTO ANOMALO

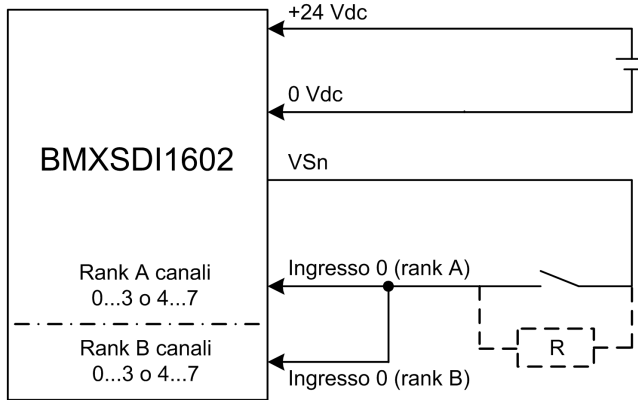
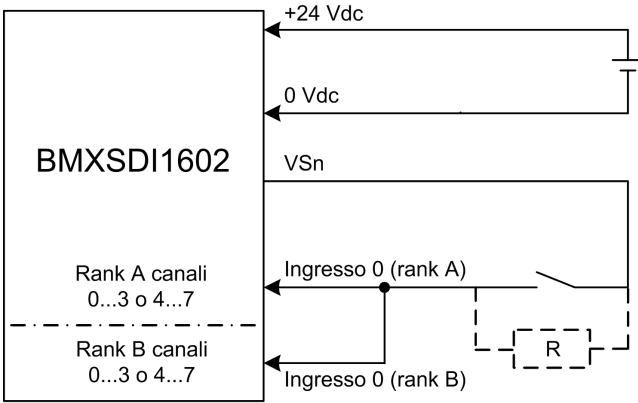
Per raggiungere il livello SIL3/Cat4/PLe tramite questo cablaggio, occorre utilizzare un sensore qualificato idoneo.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Cat4/PLe con alta disponibilità

Schema di cablaggio con collegamento a canale singolo di due sensori a canale singolo ridondanti con uso del modulo Vs:

L'esempio seguente presenta due sensori a canale singolo ridondanti (che possono essere accoppiati meccanicamente o meno), ognuno dei quali è cablato a due punti di ingresso su due moduli di ingresso diversi, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si possono utilizzare i blocchi funzione S_EQUIVALENT e S_DIHA per gestire i quattro segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Schema di cablaggio con collegamento a canale singolo di due sensori a canale singolo ridondanti con uso di alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vdc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	No	-
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.		

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare circuiti incrociati tra due canali (nel caso di un collegamento a canale singolo di due sensori a canale singolo ridondanti con alimentazione esterna). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

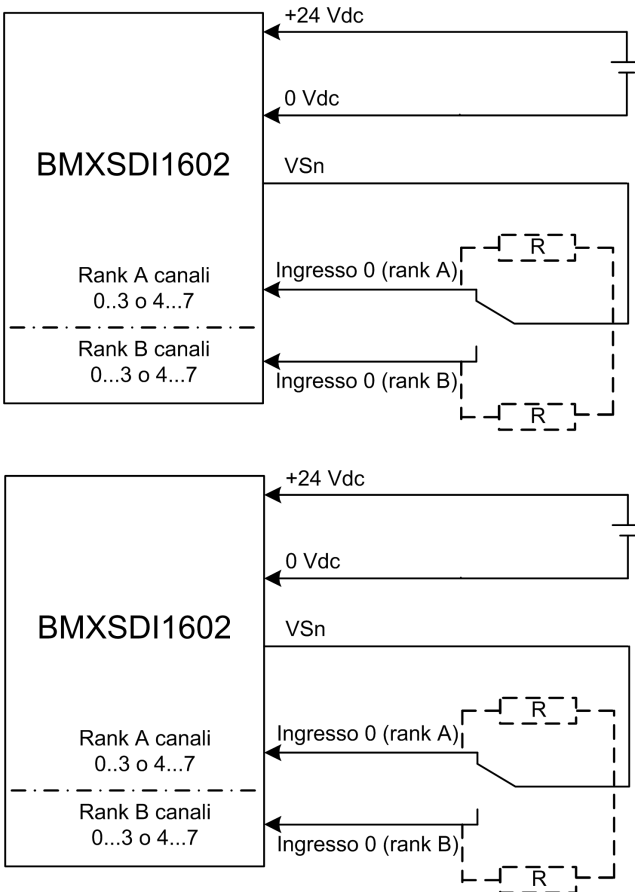
RISCHIO DI CORTOCIRCUITO A 24 VDC

Il modulo non è in grado di rilevare una condizione di cortocircuito 24 Vdc (nel caso descritto sopra di un sensore singolo collegato con due ingressi alimentati da alimentatore esterno). È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore non equivalente (accoppiato meccanicamente o meno) collegato su 2 ingressi non equivalenti di due moduli diversi con uso di modulo VS:

L'esempio seguente presenta due coppie di sensori non equivalenti ridondanti (che possono essere accoppiati meccanicamente o meno), ognuno dei quali è cablato a un singolo punto di ingresso su due moduli di ingresso diversi, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione occorre utilizzare i blocchi funzione S_ANTIVALENT e S_DIHA per gestire i quattro segnali di ingresso.
 - S_ANTIVALENT per eseguire la valutazione 1oo2 di due coppie di valori provenienti dai due sensori collegati allo stesso modulo.
 - S_DIHA per gestire la funzione di alta disponibilità.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito 24 Vdc su un canale possa causare la stessa condizione su un canale contiguo.

Dato che il sensore è alimentato internamente tramite un contatto VS, vale la seguente diagnostica di cablaggio per il canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto) ¹	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc ¹	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

▲ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI NELLO STESSO GRUPPO

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali nello stesso gruppo VS. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore non equivalente (accoppiato meccanicamente o meno) collegato su 2 ingressi non equivalenti di due moduli diversi con uso di alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno (nel caso di un sensore non equivalente collegato su due ingressi non equivalenti di due moduli diversi con alimentazione esterna). In questo caso una condizione di circuiti incrociati tra due canali non sarebbe rilevabile.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI TRA I CANALI

Il modulo non è in grado di rilevare i circuiti incrociati tra due canali. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI FUNZIONAMENTO ANOMALO

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio, occorre utilizzare sensori qualificati idonei.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

BMXSDI1602 Struttura dei dati

Introduzione

Il tipo di dati derivati `T_U_DIS_SIS_IN_16` del dispositivo (DDDT) è l'interfaccia tra il modulo di ingresso digitale BMXSDI1602 e l'applicazione eseguita nella CPU. Il DDDT `T_U_DIS_SIS_IN_16` include i tipi di dati `T_SAFE_COM_DBG_IN` e `T_U_DIS_SIS_CH_IN`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT `T_U_DIS_SIS_IN_16`

La struttura DDDT `T_U_DIS_SIS_IN_16` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH ¹	BOOL	<ul style="list-style-type: none"> • 1: il modulo funziona correttamente. • 0: il modulo non funziona correttamente. 	RO
SAFE_COM_STS ¹	BOOL	<ul style="list-style-type: none"> • 1: comunicazione del modulo valida. 	RO

Elemento	Tipo di dati	Descrizione	Accesso
		<ul style="list-style-type: none"> 0: comunicazione del modulo non valida. 	
PP_STS	BOOL	<ul style="list-style-type: none"> 1: l'alimentatore di processo è funzionante. 0: l'alimentatore di processo non è funzionante. 	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> 1: configurazione del modulo bloccata. 0: configurazione del modulo non bloccata. 	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Struttura di debug comunicazione sicura.	RO
CH_IN_A	ARRAY[0...7] di T_U_DIS_SIS_CH_IN	Array di struttura del canale dal rank A.	-
CH_IN_B	ARRAY[0...7] di T_U_DIS_SIS_CH_IN	Array di struttura del canale dal rank B.	-
MUID ²	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED	ARRAY[0...9] di INT	-	-
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.</p> <p>2. Questo valore autogenerato può essere modificato eseguendo il comando Crea > Rinnova ID & Ricrea tutto nel menu principale di Control Expert.</p>			

Struttura T_SAFE_COM_DBG_IN

La struttura T_SAFE_COM_DBG_IN include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
S_COM_EST	BOOL	<ul style="list-style-type: none"> 1: comunicazione con il modulo stabilita. 0: la comunicazione con il modulo non è stabilita o è disturbata. 	RO
M_NTP_SYNC	BOOL	<p>Con firmware della CPU 3.10 o precedente:</p> <ul style="list-style-type: none"> 1: il modulo è sincronizzato con il server NTP. 0: il modulo non è sincronizzato con il server NTP. <p>NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.</p>	RO

Elemento	Tipo di dati	Descrizione	Accesso
CPU_NTP_SYNC	BOOL	Con firmware della CPU 3.10 o precedente: <ul style="list-style-type: none"> 1: la CPU è sincronizzata con il server NTP. 0: la CPU non è sincronizzata con il server NTP. NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: <ul style="list-style-type: none"> 1...65534: il tempo, in ms, trascorso dalla ricezione da parte della CPU dell'ultima comunicazione del modulo. 65535: la CPU non ha ricevuto una comunicazione dal modulo. 	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	R/W
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO

Struttura T_U_DIS_SIS_CH_IN

La struttura T_U_DIS_SIS_CH_IN include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il canale è funzionante. 0: è stato rilevato un errore sul canale che non è operativo. <p>Formula: CH_HEALTH = non (OC o IC o SC) e SAFE_COM_STS</p>	RO
VALUE ²	EBOOL	<ul style="list-style-type: none"> 1: l'ingresso è alimentato. 0: l'ingresso non è alimentato. <p>Formula: VALUE = if (SAFE_COM_STS and not (IC)) then READ_VALUE else 0</p>	RO
OC	BOOL	<ul style="list-style-type: none"> 1: il canale è aperto o cortocircuitato verso terra. 0: il canale è collegato e non cortocircuitato verso terra. 	RO
SC	BOOL	<ul style="list-style-type: none"> 1: il canale è cortocircuitato con una sorgente 24 V oppure i due canali sono incrociati. 0: il canale non è cortocircuitato con una sorgente 24 V oppure i due canali sono incrociati. 	RO
IC	BOOL	<ul style="list-style-type: none"> 1: canale non valido rilevato dal modulo. 0: il canale è dichiarato internamente operativo dal modulo. 	RO
V_OC	BOOL	<p>Stato di configurazione del test circuito aperto o cortocircuito verso terra:</p> <ul style="list-style-type: none"> 1: attivato. 0: disattivato. 	RO
V_SC	BOOL	<p>Stato di configurazione del test cortocircuito a 24 V:</p> <ul style="list-style-type: none"> 1: attivato. 0: disattivato. 	RO
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.</p> <p>2. L'elemento VALUE può avere un'indicazione oraria fornita dal BMX CRA o BME CRA.</p>			

Modulo di uscita digitale BMXSDO0802

Introduzione

Questa sezione descrive il modulo di uscita digitale di sicurezza BMXSDO0802 M580.

Modulo di uscita digitale di sicurezza BMXSDO0802

Introduzione

Il modulo di uscita digitale di sicurezza BMXSDO0802 presenta le seguenti caratteristiche:

- 8 uscite da 0,5 A non elettricamente isolate.
- Tensione di uscita nominale 24 Vcc.
- Si ottiene quanto segue:
 - SIL3 IEC61508, SILCL3 IEC62061.
 - SIL4 EN5012x.
 - Categoria 4 (Cat4) / Performance Level e (PLe) ISO13849.
- Monitoraggio dell'alimentazione esterna dei preattuatori.
- Visualizzazione diagnostica mediante LED, pagina 243 fornita per il modulo e per ogni canale di uscita.
- Diagnostica del cablaggio del canale fornita automaticamente, in grado di rilevare le seguenti condizioni quando l'uscita è *alimentata*:
 - Corrente di sovraccarico
 - Cortocircuito a 0 Vcc verso terra
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva), pagina 103 in grado di rilevare le seguenti condizioni:
 - Conduttore aperto (o interrotto).
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva) in grado di rilevare le seguenti condizioni quando l'uscita *non è alimentata*:
 - Cortocircuito a 0 V verso terra.
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva) in grado di rilevare le seguenti condizioni quando l'uscita è *alimentata o non alimentata*:
 - Cortocircuito a 24 Vcc.
 - Circuiti incrociati tra i due canali (se l'alimentazione al sensore è fornita internamente).

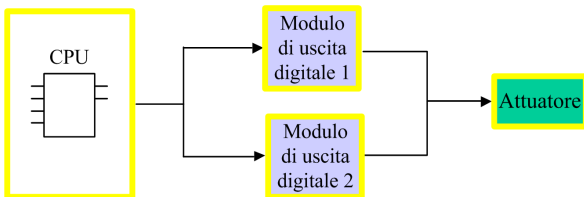
- Impostazioni di posizionamento di sicurezza configurabili per ogni canale, che vengono applicate in caso di perdita della comunicazione tra la CPU e il modulo di uscita.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 258. (La funzione CCOTF non è supportata in modalità di sicurezza), pagina 257.

NOTA: Viene avviato un autotest su ciascuna uscita per verificarne la capacità di essere non alimentata e di raggiungere lo stato sicuro senza alcun impatto sul carico (impulso di spegnimento < 1ms). L'autotest viene eseguito alternativamente, un'uscita per volta, su ciascuna uscita alimentata per meno di 1 secondo. Se l'uscita viene collegata ad un ingresso statico di un prodotto, l'ingresso statico collegato può individuare questo impulso. Per evitare un potenziale impatto dell'impulso sull'uscita potrebbe essere utile l'impiego di un filtro.

Alta disponibilità

È possibile collegare la CPU a due moduli di uscita tramite un black channel, quindi collegare ogni modulo di uscita a un singolo attuatore. Non sono necessari blocchi funzione, dato che il segnale della CPU è collegato ad entrambi i canali di uscita.

La seguente figura illustra la configurazione dell'uscita digitale ridondante per l'alta disponibilità:



Lo stato di ogni modulo di uscita può essere letto dagli elementi della rispettiva struttura `DDDT_T_U_DIS_SIS_OUT_8`, pagina 109 DDDT. Questi dati possono essere utilizzati per determinare se è necessario sostituire un modulo. Se un modulo non è più operativo e deve essere sostituito, il sistema continua a funzionare con una configurazione conforme a SIL3 mentre avviene la sostituzione del modulo.

Per maggiori dettagli su questa struttura, vedere esempio di cablaggio delle uscite ad alta disponibilità, pagina 106.

Connettore di cablaggio BMXSDO0802

Introduzione

Il modulo di uscita digitale BMXSDO0802 dispone di un singolo gruppo di 8 uscite.

- Entrambi i contatti di alimentazione a +24 Vcc (18 e 20) sono collegati internamente.
- Tutti i contatti comuni a 0 V (1, 3, 5, 7, 9, 11, 13, 15, 17 e 19) sono collegati internamente.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera tipo Cage Clamp BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario un alimentatore di processo a tensione ultra bassa protetta (SELV/PELV) di categoria di sovratensione II da 24 Vcc. Schneider Electric raccomanda di impiegare un alimentatore che non esegua il ripristino automatico dell'alimentazione dopo un'interruzione di corrente.

Fusibile

Per proteggere l'alimentatore esterno dai cortocircuiti e da eventuali condizioni di sovratensione, è necessario un fusibile rapido, max. 6 A.

⚠ ATTENZIONE

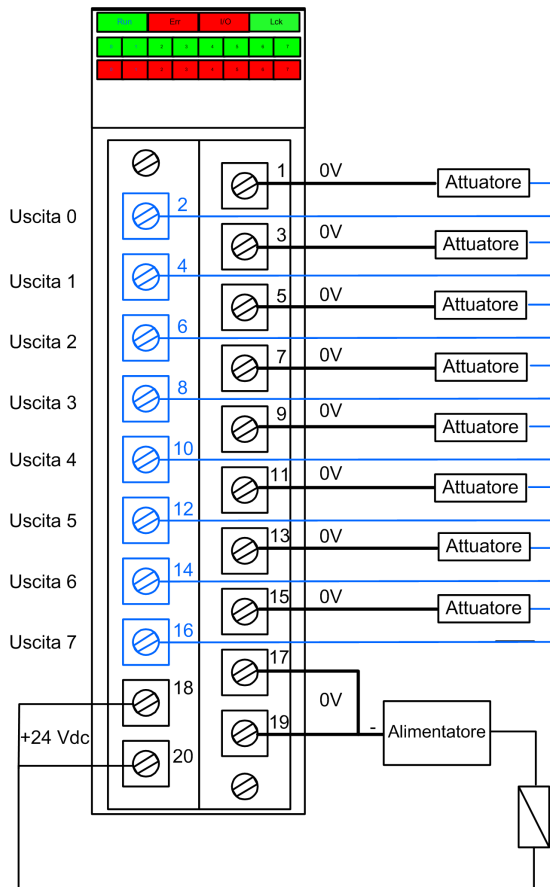
SCELTA ERRATA DEL FUSIBILE

Utilizzare fusibili rapidi per proteggere i componenti elettronici del modulo di uscita digitale da una condizione di sovracorrente. La scelta di un fusibile errato può causare danni al modulo.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Contatti del connettore di cablaggio

Il seguente schema di cablaggio presenta un singolo modulo di uscita collegato a 8 attuatori:



Mappatura delle uscite ai contatti del connettore

La seguente tabella fornisce una descrizione di ogni contatto del modulo di uscita BMXSDO0802:

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Uscita 0	2	1	Comune 0 V
Uscita 1	4	3	Comune 0 V
Uscita 2	6	5	Comune 0 V
Uscita 3	8	7	Comune 0 V
Uscita 4	10	9	Comune 0 V
Uscita 5	12	11	Comune 0 V
Uscita 6	14	13	Comune 0 V
Uscita 7	16	15	Comune 0 V
Alimentazione di processo 24 Vcc	18	17	Comune 0 V
Alimentazione di processo 24 Vcc	20	19	Comune 0 V

BMXSDO0802 Esempi di cablaggio dell'applicazione di uscita

Introduzione

È possibile cablare il modulo di uscita digitale di sicurezza BMXSDO0802 a degli attuatori per raggiungere la conformità SIL3 Categoria 4 (Cat4) / Performance Level e (PLe) in diversi modi, a seconda delle esigenze di alta disponibilità.

⚠ ATTENZIONE

RISCHIO DI FUNZIONAMENTO ANOMALO

Il livello di integrità di sicurezza (SIL) massimo è determinato dalla qualità dell'attuatore e la lunghezza dell'intervallo dei test per IEC 61508. Se si utilizzano attuatori non conformi alla qualità dello standard SIL previsto, cablare sempre questi attuatori in modo ridondante a due canali.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di uscita digitale SIL3 Cat4/PLe:

- Cat4/PLe:
 - un unico canale del modulo di uscita che comanda una variabile di processo. Questa struttura utilizza un singolo attuatore.
- Cat4/PLe con alta disponibilità:
 - due moduli di uscita ridondanti, ognuno con un canale collegato a un attuatore separato, ma che comandano la stessa variabile di processo.

⚠ ATTENZIONE

RISCHIO DI FUNZIONAMENTO ANOMALO

Quando l'apparecchiatura è impiegata in un'applicazione con fiamma o gas o quando lo stato dell'uscita deve essere sotto tensione:

- La procedura di test deve comprendere un test specifico che attesti l'efficacia del rilevamento di cavo interrotto mediante rimozione della morsettiera e verifica che i corrispondenti bit di errore siano impostati.
- Verificare l'efficacia del rilevamento di cortocircuito verso terra attivando la funzione di diagnostica **Test impulso con alimentazione** nella scheda **Configurazione** del modulo o adottando un'altra procedura (ad esempio impostando l'uscita a 1 e verificando la diagnostica, ecc.).
- Evitare l'uso di attuatori a spia in quanto la loro impedenza è molto bassa quando sono accesi, il che può comportare il rischio di rilevamento di una condizione errata di cortocircuito o sovraccarico.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Diagnostica di ingresso configurabile in Control Expert

Per il modulo di uscita digitale di sicurezza BMXSDO0802, usare la relativa pagina **Configurazione** in Control Expert per:

- Attivare **Rilevamento cortocircuito a 24V** per ogni canale alimentato. Questo test esegue le seguenti operazioni di diagnostica del cablaggio degli attuatori per un canale:
 - Rilevamento cortocircuito a 24V
 - Rilevamento circuiti incrociati tra due canali di uscita

- Attivare **Rilevamento filo aperto** per ognuno degli otto canali, che esegue la seguente diagnostica di cablaggio per quel canale:
 - Rilevamento di conduttore aperto (o interrotto) (ovvero il canale di uscita non è collegato all'attuatore)
 - Rilevamento cortocircuito a 0 V verso terra
- Attivare il **Test impulso con alimentazione** per ogni canale di uscita. Questo test viene eseguito periodicamente quando l'uscita è nello stato non alimentato e applica un impulso (della durata inferiore a 1 ms) all'uscita per determinare se può passare allo stato alimentato. Se la corrente supera una soglia di 0,7 A, l'uscita viene considerata come in condizione di cortocircuito verso terra a 0 Vdc. Il periodo di test è inferiore a 1 s.

⚠ AVVERTIMENTO

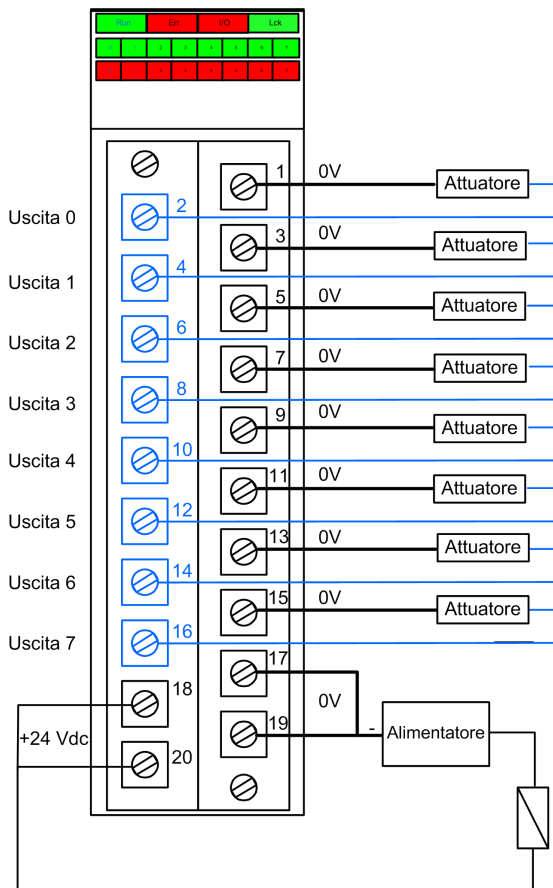
RISCHIO DI FUNZIONAMENTO ANOMALO

Schneider Electric raccomanda di attivare la diagnostica disponibile fornita in Control Expert per rilevare e reagire alle condizioni descritte sopra. Se un test di diagnostica non è attivato o non è disponibile in Control Expert, sarà necessario applicare un'altra misura di sicurezza per rilevare o escludere queste condizioni.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

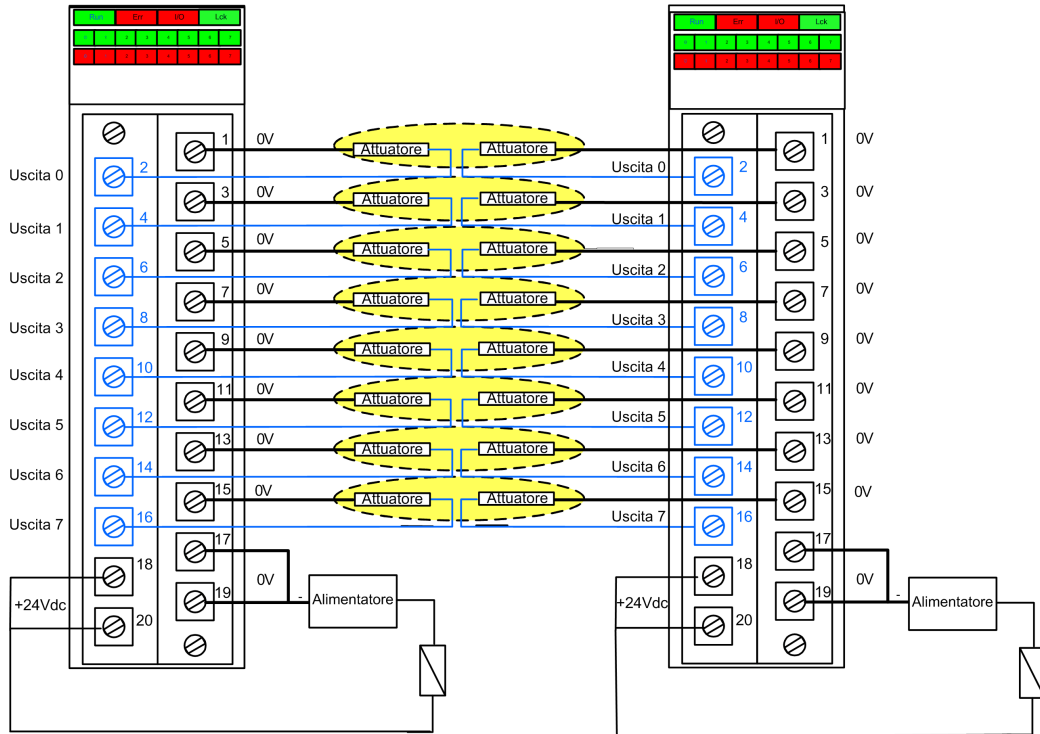
SIL 3 Cat4/PLe - Esempio di modulo di uscita digitale singolo

L'esempio seguente presenta un attuatore esclusivo cablato a ogni uscita su un singolo modulo di uscita. Ogni loop è SIL 3 Cat4/PLe:



Esempio SIL 3 Cat4/PLe - Alta disponibilità:

Nel seguente schema di cablaggio, due uscite ridondanti comandano la stessa variabile di processo. Come illustrato di seguito, ogni uscita è collegata ad attuatori separati, per cui ogni attuatore esegue lo stesso comando inviato su canali diversi. In alternativa, si possono collegare tra di loro le due uscite ridondanti per comandare lo stesso attuatore.



Riepilogo della diagnostica del cablaggio delle uscite

Le due strutture forniscono le seguenti diagnostiche di cablaggio:

Condizione	Diagnostica fornita nello stato di uscita?	
	Alimentato	Non alimentato
Conduttore aperto (o interrotto) ¹	Sì. Diagnostica per ogni ciclo.	Sì. Diagnostica per ogni ciclo.
Uscita in sovraccarico ²	Sì. Diagnostica per ogni ciclo.	No
Cortocircuito a 0 V verso terra	Sì. Diagnostica per ogni ciclo.	Sì. Periodo di diagnostica < 1 s.
Cortocircuito a 24 Vdc ¹	Sì. Periodo di diagnostica < 1 s.	Sì. Diagnostica per ogni ciclo.

Condizione	Diagnostica fornita nello stato di uscita?	
	Alimentato	Non alimentato
Circuiti incrociati tra due canali	Si. Periodo di diagnostica < 1 s.	Si. Diagnostica per ogni ciclo.
<p>1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda Configurazione del modulo in Control Expert.</p> <p>2. Dopo che la condizione è risolta, riarmare l'uscita interrompendo l'alimentazione elettrica.</p>		

⚠ AVVERTIMENTO

RISCHIO DI CORTOCIRCUITO VERSO TERRA 0 VDC

Per la condizione di cortocircuito verso terra 0 V con lo stato di uscita non alimentato, si consiglia di attivare l'opzione **Rilevamento filo aperto** nella scheda **Configurazione** del modulo. In alternativa, sarà necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CORTOCIRCUITO A 24 VDC

Per la condizione di cortocircuito a 24 Vdc con lo stato di uscita alimentato o non alimentato, si consiglia di attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo. In alternativa, sarà necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI

Il modulo non è in grado di rilevare i circuiti incrociati tra due condizioni di canali con lo stato di uscita non alimentato e l'altro canale non alimentato. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione se si verifica quando lo stato di uscita diventa alimentato.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI

Per la condizione di circuiti incrociati tra due condizioni di canali con lo stato di uscita non alimentato e l'altro canale alimentato, si consiglia di attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo. In alternativa è necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione quando lo stato di uscita diventa alimentato.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI

Il modulo non è in grado di rilevare i circuiti incrociati tra due condizioni di canali con lo stato di uscita alimentato e l'altro canale non alimentato. È necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI CIRCUITI INCROCIATI

Per la condizione di circuiti incrociati tra due condizioni di canali con lo stato di uscita alimentato e l'altro canale alimentato, si consiglia di attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo. In alternativa, sarà necessario applicare un'altra misura di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

BMXSDO0802 Struttura dei dati

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_DIS_SIS_OUT_8` è l'interfaccia tra il modulo di uscita digitale BMXSDO0802 e l'applicazione eseguita nella CPU. Il DDDT `T_U_DIS_SIS_OUT_8` include i tipi di dati `T_SAFE_COM_DBG_OUT` e `T_U_DIS_SIS_CH_OUT`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT T_U_DIS_SIS_OUT_8

La struttura DDDT T_U_DIS_SIS_OUT_8 include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il modulo funziona correttamente. 0: il modulo non funziona correttamente. 	RO
SAFE_COM_STS ¹	BOOL	<ul style="list-style-type: none"> 1: comunicazione del modulo valida. 0: comunicazione del modulo non valida. 	RO
PP_STS	BOOL	<ul style="list-style-type: none"> 1: l'alimentatore di processo è funzionante. 0: l'alimentatore di processo non è funzionante. 	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> 1: configurazione del modulo bloccata. 0: configurazione del modulo non bloccata. 	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Struttura di debug comunicazione sicura.	RO
CH_OUT	ARRAY[0...7] di T_U_DIS_SIS_CH_OUT	Array di struttura del canale.	RO
S_TO	UINT	Timeout di sicurezza prima che il modulo entri nello stato di posizionamento di sicurezza.	RO
MUID ²	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED_1	ARRAY[0...8] di INT	-	-
RESERVED_2	ARRAY[0...6] di INT	-	-
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.</p> <p>2. Questo valore autogenerato può essere modificato eseguendo il comando Crea > Rinnova ID & Ricrea tutto nel menu principale di Control Expert.</p>			

Struttura T_SAFE_COM_DBG_OUT

La struttura T_SAFE_COM_DBG_OUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
S_COM_EST	BOOL	<ul style="list-style-type: none"> 1: comunicazione con il modulo stabilita. 0: la comunicazione con il modulo non è stabilita o è disturbata. 	RO
M_NTP_SYNC	BOOL	Con firmware della CPU 3.10 o precedente: <ul style="list-style-type: none"> 1: il modulo è sincronizzato con il server NTP. 0: il modulo non è sincronizzato con il server NTP. NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.	RO
CPU_NTP_SYNC	BOOL	Con firmware della CPU 3.10 o precedente: <ul style="list-style-type: none"> 1: la CPU è sincronizzata con il server NTP. 0: la CPU non è sincronizzata con il server NTP. NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: <ul style="list-style-type: none"> 1...65534: il tempo, in ms, trascorso dalla ricezione da parte della CPU dell'ultima comunicazione del modulo. 65535: la CPU non ha ricevuto una comunicazione dal modulo. 	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	R/W
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO

Elemento	Tipo di dati	Descrizione	Accesso
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO
STS_MS_OUT	UINT	Valore di timestamp sicuro della frazione di secondo, arrotondato al millisecondo più vicino, dei dati da inviare al modulo.	RO
STS_S_OUT	UDINT	Valore di timestamp sicuro in secondi dei dati da inviare al modulo.	RO
CRC_OUT	UDINT	Valore CRC per i dati da inviare al modulo.	RO

Struttura T_U_DIS_SIS_CH_OUT

La struttura T_U_DIS_SIS_CH_OUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il canale è funzionante. 0: è stato rilevato un errore sul canale che non è operativo. <p>Formula:</p> <p>CH_HEALTH = non (SC o OL o IC o OC) e SAFE_COM_STS e non (modulo in stato di posizionamento di sicurezza)</p>	RO
VALUE	EBOOL	<p>Comando di sicurezza del canale di uscita:</p> <ul style="list-style-type: none"> 1: Comanda la chiusura dell'uscita (alimentata). 0: Comanda l'apertura dell'uscita (non alimentata). 	R/W
TRUE_VALUE ²	BOOL	<p>Valore di restituzione del canale di uscita relè:</p> <ul style="list-style-type: none"> 1: L'uscita è chiusa (alimentata). 0: L'uscita è aperta (non alimentata). 	RO
OC	BOOL	<ul style="list-style-type: none"> 1: il canale è aperto o cortocircuitato verso terra. 0: il canale è collegato e non cortocircuitato verso terra. 	RO
SC	BOOL	<ul style="list-style-type: none"> 1: Il canale non è cortocircuitato con una sorgente 24 V oppure è incrociato con un altro canale. 0: Il canale non è cortocircuitato con una sorgente 24 V oppure il circuito è incrociato. 	RO

Elemento	Tipo di dati	Descrizione	Accesso
OL	BOOL	<ul style="list-style-type: none"> 1: Il canale è sovraccarico o cortocircuitato a 0V. 0: Il canale non è sovraccarico o cortocircuitato a 0V. 	RO
IC	BOOL	<ul style="list-style-type: none"> 1: canale non valido rilevato dal modulo. 0: il canale è dichiarato internamente operativo dal modulo. 	RO
V_OC	BOOL	Stato configurazione del test circuito aperto: <ul style="list-style-type: none"> 1: attivato. 0: disattivato. 	RO
V_SC	BOOL	Stato di configurazione del test cortocircuito a 24 V: <ul style="list-style-type: none"> 1: attivato. 0: disattivato. 	RO
V_PULSE_ON	BOOL	Stato di configurazione del test impulsi sotto tensione: <ul style="list-style-type: none"> 1: attivato. 0: disattivato. 	RO
CH_FBC	BOOL	Configurazione dell'impostazione di posizionamento di sicurezza del canale: <ul style="list-style-type: none"> 1: valore definito dall'utente. 0: mantieni ultimo valore. 	RO
CH_FBST	BOOL	Configurazione dello stato di posizionamento di sicurezza del canale quando è selezionato definito da utente: <ul style="list-style-type: none"> 1: Alimentato. 0: Non alimentato. 	RO
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.</p> <p>2. L'elemento TRUE_VALUE può avere un'indicazione oraria fornita da BMX CRA o BME CRA.</p>			

Modulo di uscita relè digitale BMXSRA0405

Introduzione

Questa sezione descrive il modulo di uscita relè digitale di sicurezza BMXSRA0405 M580.

Modulo di uscita relè digitale di sicurezza BMXSRA0405

Introduzione

Il modulo di uscita relè digitale di sicurezza BMXSRA0405 presenta la seguenti caratteristiche:

- 4 uscite relè con corrente 5 A.
- Tensione di uscita nominale di 24 Vcc e 24...230 Vca (categoria di sovratensione II).
- Conformità fino a SIL4 (EN5012x) / SIL3 (IEC61508) Categoria 4 (Cat4) / Performance Level e (PLe).
- Supporta 8 opzioni di configurazione di cablaggio dell'applicazione predefinite.
- Monitoraggio mediante autotest automatico configurabile della capacità del relè di eseguire lo stato comandato delle uscite (a seconda della configurazione di cablaggio dell'applicazione selezionata).
- Impostazioni del modulo configurabili per la modalità di posizionamento di sicurezza e il timeout di posizionamento di sicurezza (in ms).
- Visualizzazione diagnostica mediante LED, pagina 248 fornita per il modulo e per ogni canale di uscita.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 258. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 257).

Connettore di cablaggio BMXSRA0405

Introduzione

Il modulo di uscita relè digitale BMXSRA0405 include 4 relè e supporta fino a 4 uscite. Il modulo dispone di una coppia di contatti *a* e *b* per ogni relè. Notare che per ogni relè:

- i due contatti *a* sono collegati internamente e

- anche i due contatti *b* sono collegati internamente.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera tipo Cage Clamp BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario installare l'alimentatore di processo a 24 Vdc o 24 Vac ... 230 Vac.

Fusibile

È necessario un fusibile rapido, max. 6 A, adatto per l'applicazione selezionata e la struttura relè selezionata. Installare sempre un fusibile esterno in serie con l'alimentatore esterno, il relè e il carico.

⚠ AVVERTIMENTO

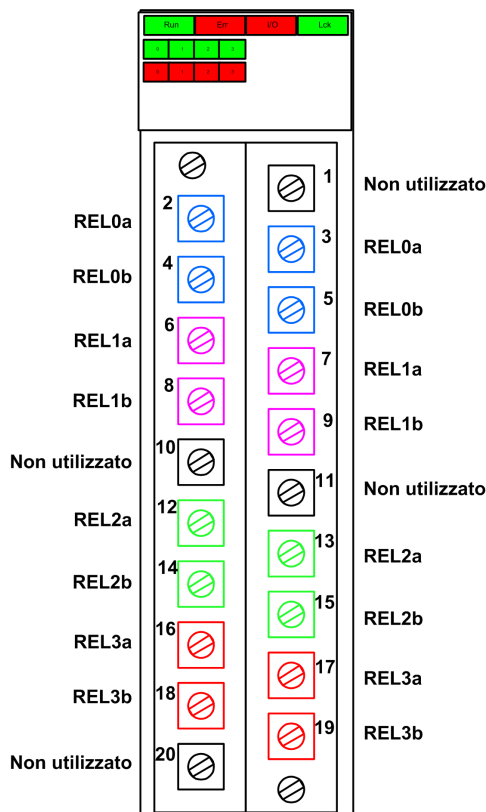
RISCHIO DI FUNZIONAMENTO ANOMALO

È responsabilità dell'utente implementare la diagnostica del cablaggio appropriata per rilevare e impedire il verificarsi di guasti pericolosi sul cablaggio esterno.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Connettore di cablaggio

Il seguente esempio illustra i contatti del modulo relè:



Mappatura degli ingressi ai contatti del connettore

La seguente tabella fornisce una descrizione di ogni contatto del modulo di uscita relè digitale BMXSRA0405:

Descrizione del contatto	Numero del contatto sulla morsetteria		Descrizione del contatto
Contatto NO, relè 0a	2	1	Non usato
Contatto NO, relè 0b	4	3	Contatto NO, relè 0a
Contatto NO, relè 1a	6	5	Contatto NO, relè 0b
Contatto NO, relè 1b	8	7	Contatto NO, relè 1a
Non usato	10	9	Contatto NO, relè 1b

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Contatto NO, relè 2a	12	11	Non usato
Contatto NO, relè 2b	14	13	Contatto NO, relè 2a
Contatto NO, relè 3a	16	15	Contatto NO, relè 2b
Contatto NO, relè 3b	18	17	Contatto NO, relè 3a
Non usato	20	19	Contatto NO, relè 3b

NOTA: Dato che i due contatti *a* per ogni relè sono collegati internamente, si deve usare solo un contatto *a* per ogni relè. Analogamente, dato che i due contatti *b* per ogni relè sono collegati internamente, si deve usare solo un contatto *b* per ogni relè.

BMXSRA0405 Esempi di cablaggio dell'applicazione di uscita

Introduzione

È possibile cablare il modulo relè di uscita digitale di sicurezza BMXSRA0405 per raggiungere la conformità SIL2 Categoria 2 (Cat2) / Performance Level c (PLc) o SIL3 Cat4 / PLe in diversi modi, a seconda dei fattori seguenti:

- il numero di uscite che il modulo supporterà e
- il modo in cui si intende verificare la capacità del modulo di commutare l'attuatore nello stato di domanda previsto, ovvero:
 - automaticamente da parte del modulo (in questo caso non vi è alcuna transizione di stato per l'attuatore) oppure
 - tramite una procedura che effettua e verifica una transizione giornaliera del segnale dal modulo all'attuatore (in questo caso la transizione influenza lo stato dell'attuatore).

Realizzare questa configurazione selezionando un numero di applicazione (riportato nelle tabelle seguenti) nell'elenco **Funzione** della scheda **Configurazione** del modulo in Control Expert.

Applicazioni della configurazione di cablaggio SIL2 Cat2 / PLc:

Funzione	Stato richiesto	Relè	Uscite	Test del segnale?		Schema di cablaggio (vedi oltre)
				Test automatico del segnale? ¹	Transizione di segnale giornaliera?	
Applicazione_1	Non alimentato	1	4	No	Sì	A
Applicazione_2	Non alimentato	2	2	Sì	No	B
Applicazione_3	Alimentato	1	4	No	Sì	A
Applicazione_4	Alimentato	2	2	Sì	No	C

1. Il test automatico del segnale non influenza lo stato dell'attuatore.

Applicazioni della configurazione di cablaggio SIL3 Cat4 / PLc:

Funzione	Stato richiesto	Relè	Uscite	Test del segnale?		Schema di cablaggio (vedi oltre)
				Test automatico del segnale? ¹	Transizione di segnale giornaliera?	
Applicazione_5	Non alimentato	2	2	No	Sì	C
Applicazione_6	Non alimentato	4	1	Sì	No	D
Applicazione_7	Alimentato	2	2	No	Sì	C
Applicazione_8	Alimentato	2	2	Sì	No	C

1. Il test automatico del segnale non influenza lo stato dell'attuatore.

Ognuna di queste otto applicazioni è descritta negli esempi di cablaggio seguenti.

Applicazione_1: 4 uscite, SIL2 / Cat2 / PLc, stato non alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Se il modulo rileva un errore interno per un'uscita, interrompe l'alimentazione per quell'uscita.

▲ ATTENZIONE

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Per raggiungere il livello SIL2 secondo IEC61508 e Category 2 / Performance Level c secondo ISO 13849 tramite questa configurazione di cablaggio, occorre effettuare una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Per una raffigurazione della configurazione di cablaggio per Applicazione_1, vedere lo schema di cablaggio A, pagina 122 di seguito.

Applicazione_2: 2 uscite, SIL2 / Cat2 / PLc, stato non alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici automatico su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_2, vedere lo schema di cablaggio B, pagina 123 di seguito.

Applicazione_3: 4 uscite, SIL2 / Cat2 / PLc, stato alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Se il modulo rileva un errore interno per un'uscita, interrompe l'alimentazione per quell'uscita ovvero la commuta in stato sicuro.

⚠ ATTENZIONE

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Per raggiungere il livello SIL2 secondo IEC61508 e Category 2 / Performance Level c secondo ISO 13849 tramite questa configurazione di cablaggio, occorre effettuare una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Per una raffigurazione della configurazione di cablaggio per Applicazione_3, vedere lo schema di cablaggio A, pagina 122 di seguito.

Applicazione_4: 2 uscite, SIL2 / Cat2 / PLc, stato alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_4, vedere lo schema di cablaggio C, pagina 124 di seguito.

Applicazione_5: 2 uscite, SIL3 / Cat4 / PLe, stato non alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

▲ ATTENZIONE

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4 / Performance Level e secondo ISO 13849 tramite questa configurazione di cablaggio, occorre effettuare una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Per una raffigurazione della configurazione di cablaggio per Applicazione_5, vedere lo schema di cablaggio C, pagina 124 di seguito.

Applicazione_6: 1 uscita, SIL3 / Cat4 / PLe, stato non alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di tutti i relè (relè 0, relè 1, relè 2 e relè 3) per il modulo.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei quattro relè utilizzati (2 coppie di relè in serie impostati in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_6, vedere lo schema di cablaggio D, pagina 125 di seguito.

Applicazione_7: 2 uscite, SIL3 / Cat4 / PLe, stato alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

⚠ ATTENZIONE

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Per raggiungere il livello SIL3 secondo IEC61508 e Category 4 / Performance Level e secondo ISO 13849 tramite questa configurazione di cablaggio, occorre effettuare una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Per una raffigurazione della configurazione di cablaggio per Applicazione_7, vedere lo schema di cablaggio C, pagina 124 di seguito.

Applicazione_8: 2 uscite, SIL3 / Cat4 / PLe, stato alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Se il modulo rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

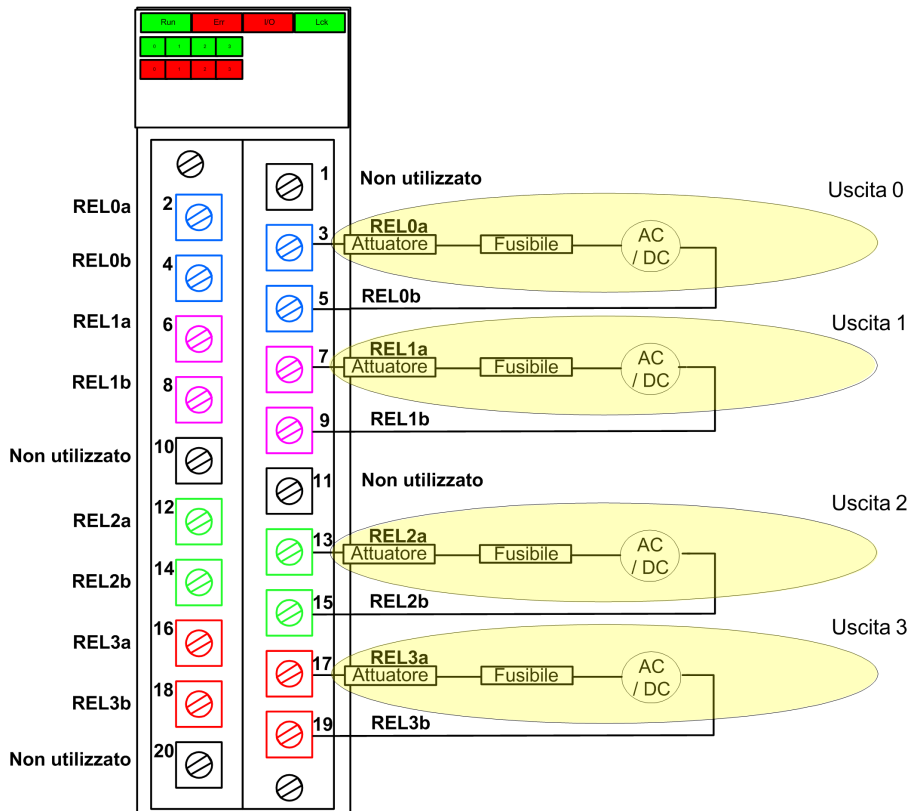
Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in serie), il test non ha alcuna influenza sul carico di uscita (normalmente *non alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_8, vedere lo schema di cablaggio C, pagina 124 di seguito.

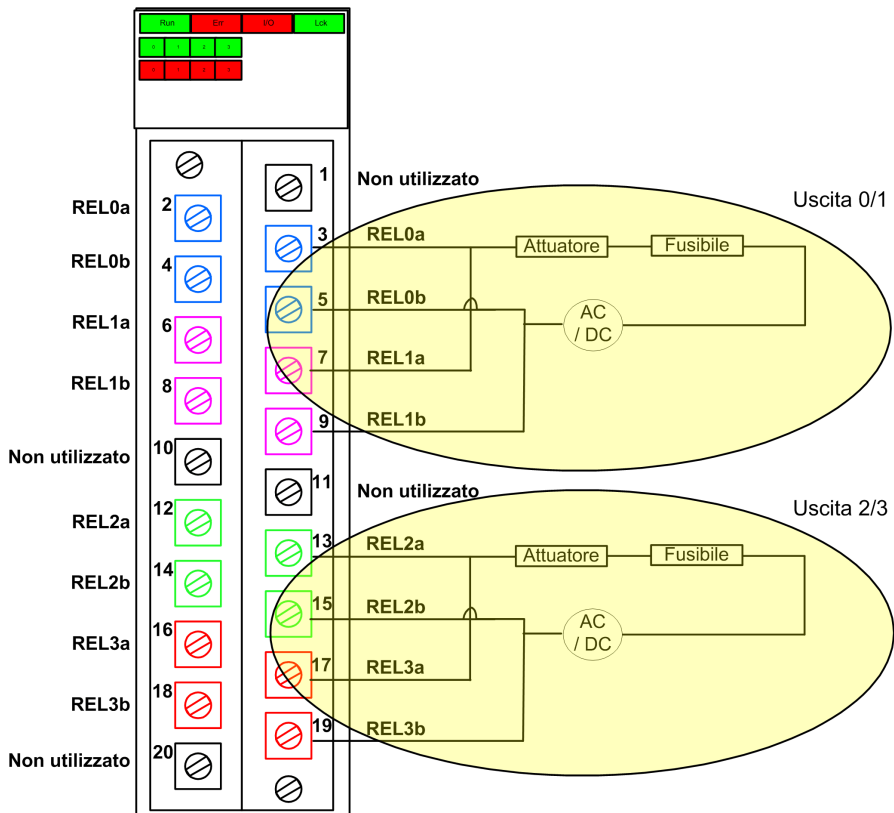
Schema di cablaggio A

Questo schema di cablaggio si applica a Applicazione_1 e Applicazione_3:



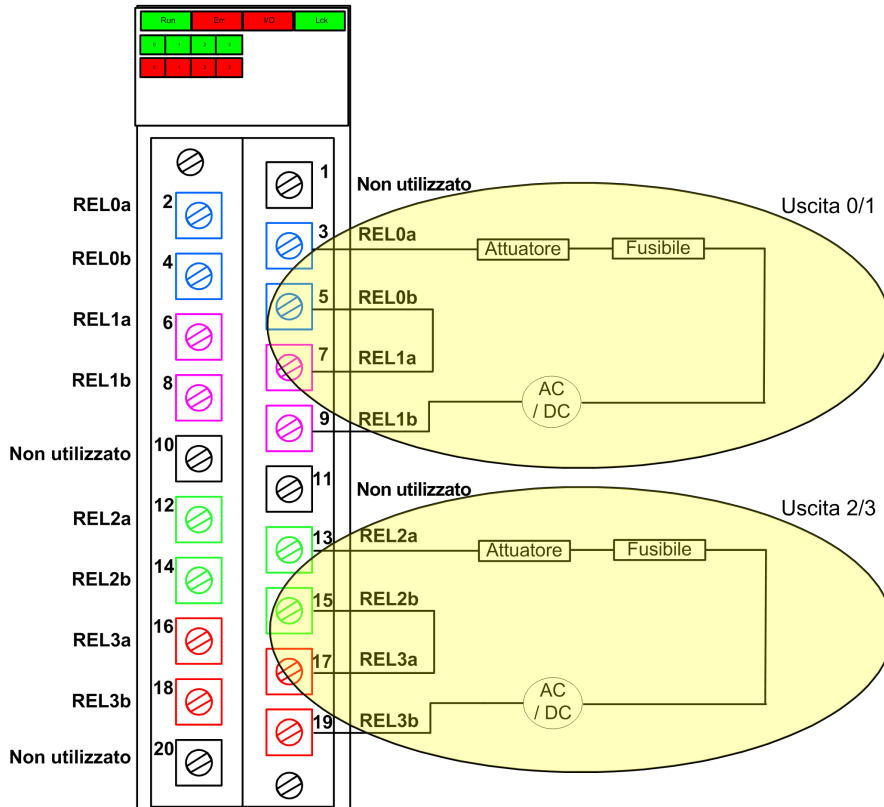
Schema di cablaggio B

Questo schema di cablaggio si applica a Applicazione_2:



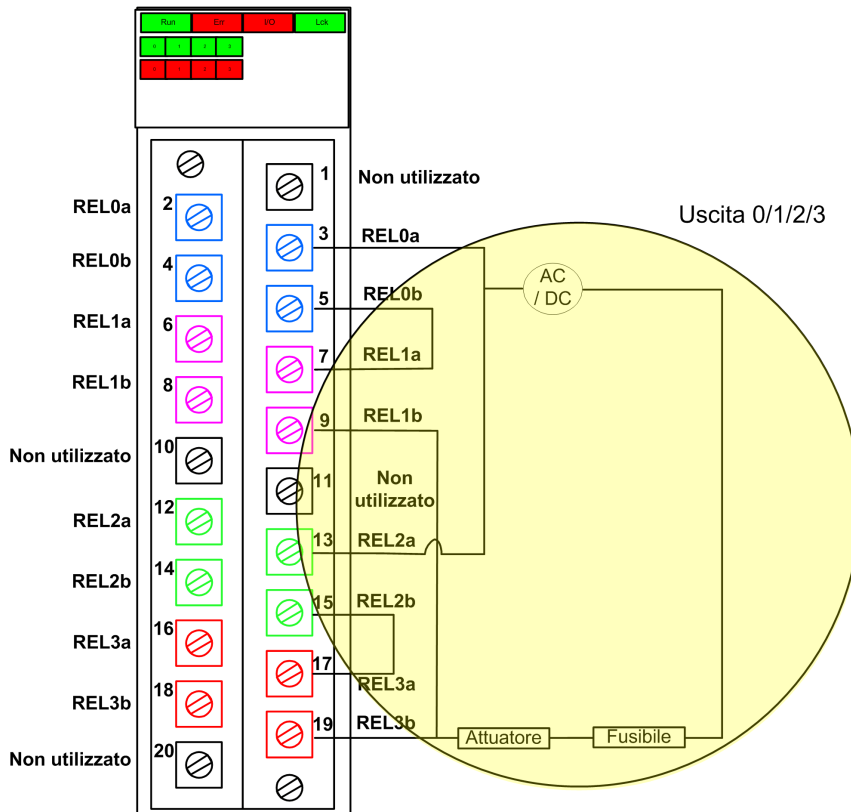
Schema di cablaggio C

Questo schema di cablaggio si applica a Applicazione_4, Applicazione_5, Applicazione_7 e Applicazione_8:



Schema di cablaggio D

Questo schema di cablaggio si applica a Applicazione_6:



BMXSRA0405 Struttura dei dati

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_DIS_SIS_OUT_4` è l'interfaccia tra il modulo relè di uscita BMXSRA0405 e l'applicazione eseguita nella CPU. Il DDDT `T_U_DIS_SIS_OUT_4` include i tipi di dati `T_SAFE_COM_DBG_OUT` e `T_U_DIS_SIS_CH_ROUT`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT T_U_DIS_SIS_OUT_4

La struttura DDDT T_U_DIS_SIS_OUT_4 include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il modulo funziona correttamente. 0: il modulo non funziona correttamente. 	RO
SAFE_COM_STS ¹	BOOL	<ul style="list-style-type: none"> 1: comunicazione del modulo valida. 0: comunicazione del modulo non valida. 	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> 1: configurazione del modulo bloccata. 0: configurazione del modulo non bloccata. 	RO
APPLI	UINT	Configurazione applicazione relè: 1, 2, 3, 4, 5, 6, 7 o.	RO
TIME_PERIOD	UINT	Periodo di tempo per il monitoraggio automatico dei relè (in minuti).	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Struttura di debug comunicazione sicura.	RO
CH_OUT	ARRAY[0...3] di T_U_DIS_SIS_CH_ROUT	Array di struttura del canale.	–
S_TO	UINT	Timeout di sicurezza prima che il modulo entri nello stato di posizionamento di sicurezza.	RO
MUID ²	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED_1	ARRAY[0...7] di INT	-	–
RESERVED_2	ARRAY[0...6] di INT	-	–
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.</p> <p>2. Questo valore autogenerato può essere modificato eseguendo il comando Crea > Rinnova ID & Ricrea tutto nel menu principale di Control Expert.</p>			

Struttura T_SAFE_COM_DBG_OUT

La struttura T_SAFE_COM_DBG_OUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
S_COM_EST	BOOL	<ul style="list-style-type: none"> 1: comunicazione con il modulo stabilita. 0: la comunicazione con il modulo non è stabilita o è disturbata. 	RO
M_NTP_SYNC	BOOL	<p>Con firmware della CPU 3.10 o precedente:</p> <ul style="list-style-type: none"> 1: il modulo è sincronizzato con il server NTP. 0: il modulo non è sincronizzato con il server NTP. <p>NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con firmware della CPU 3.10 o precedente:</p> <ul style="list-style-type: none"> 1: la CPU è sincronizzata con il server NTP. 0: la CPU non è sincronizzata con il server NTP. <p>NOTA: Con firmware della CPU 3.20 o successivo, il valore è sempre 1.</p>	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	<p>Ritardo di comunicazione tra due valori ricevuti dal modulo:</p> <ul style="list-style-type: none"> 1...65534: il tempo, in ms, trascorso dalla ricezione da parte della CPU dell'ultima comunicazione del modulo. 65535: la CPU non ha ricevuto una comunicazione dal modulo. 	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	R/W
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO
STS_MS_OUT	UINT	Valore di timestamp sicuro della frazione di secondo, arrotondato al millisecondo più vicino, dei dati da inviare al modulo.	RO

Elemento	Tipo di dati	Descrizione	Accesso
STS_S_OUT	UDINT	Valore di timestamp sicuro in secondi dei dati da inviare al modulo.	RO
CRC_OUT	UDINT	Valore CRC per i dati da inviare al modulo.	RO

Struttura T_U_DIS_SIS_CH_ROUT

La struttura T_U_DIS_SIS_CH_ROUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH ¹	BOOL	<ul style="list-style-type: none"> 1: il canale è funzionante. 0: è stato rilevato un errore sul canale che non è operativo. <p>Formula:</p> <p>CH_HEALTH = non (IC) e SAFE_COM_STS e non (modulo in stato di posizionamento di sicurezza)</p>	RO
VALUE	EBOOL	<p>Comando di sicurezza del canale di uscita:</p> <ul style="list-style-type: none"> 1: Comanda la chiusura dell'uscita (alimentata). 0: Comanda l'apertura dell'uscita (non alimentata). 	R/W
TRUE_VALUE ²	BOOL	<p>Valore di restituzione del canale di uscita relè:</p> <ul style="list-style-type: none"> 1: L'uscita è chiusa (alimentata). 0: L'uscita è aperta (non alimentata). 	RO
IC	BOOL	<ul style="list-style-type: none"> 1: canale non valido rilevato dal modulo. 0: il canale è dichiarato internamente operativo dal modulo. 	RO
CH_FBC	BOOL	<p>Configurazione dell'impostazione di posizionamento di sicurezza del canale:</p> <ul style="list-style-type: none"> 1: valore definito dall'utente. 0: mantieni ultimo valore. 	RO

Elemento	Tipo di dati	Descrizione	Accesso
CH_FBST	BOOL	Configurazione dello stato di posizionamento di sicurezza del canale quando è selezionato definito da utente: <ul style="list-style-type: none">• 1: Alimentato.• 0: Non alimentato.	RO
<p>1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.</p> <p>2. L'elemento TRUE_VALUE può avere un'indicazione oraria fornita da BMX CRA o BME CRA.</p>			

Alimentatori di sicurezza M580

Contenuto del capitolo

Alimentatori di sicurezza M580	131
Diagnostica del modulo di alimentazione di sicurezza M580	134
DDT di sicurezza M580	136

Introduzione

Questo capitolo descrive i moduli alimentatore di sicurezza M580.

Alimentatori di sicurezza M580

Introduzione

Con il PAC di sicurezza M580 possono essere usati i seguenti alimentatori:

- Alimentatore di sicurezza 100-240 Vca ridondante BMXCPS4002S
- alimentatore di sicurezza ad alta potenza 24/48 Vdc ridondante BMXCPS4022S
- alimentatore di sicurezza ad alta potenza 125 Vdc ridondante BMXCPS3522S

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Usare solo un alimentatore BMXCPS4002S, BMXCPS4022S o BMXCPS3522S in un rack che contiene un modulo di sicurezza M580. Verificare sia l'installazione fisica sia il proprio progetto in Control Expert per confermare che siano utilizzati solo alimentatori di sicurezza M580.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Funzionalità degli alimentatori

Ogni modulo di alimentazione di sicurezza M580 converte l'energia Vdc o Vac in due tensioni di uscita, 24 Vdc e 3,3 Vdc, come descritto di seguito:

Caratteristiche	Alimentazione		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Rete di alimentazione di ingresso principale	100...240 Vca, 50...60 Hz	24...48 Vcc	100...150 Vcc
Uscita limite di potenza verso backplane	40 Vcc	40 Vcc	40 Vcc

Caratteristiche	Alimentazione		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Temperatura ambiente per limite di potenza	-25° C...+60° C	-25° C...+60° C	-25° C...+60° C
Cablaggio con	<ul style="list-style-type: none"> rete AC con neutro cablato a terra OPPURE rete AC con neutro isolato e impedente verso terra, con neutro AC protetto tramite fusibile dall'utente. 	Una rete DC 24...48 Vdc	Una rete DC 125 Vdc

Ogni alimentatore rileva le condizioni di sovratensione, sovraccarico e cortocircuito su entrambe le linee del backplane, 3,3 Vdc e 24 Vdc.

Se viene rilevata la soglia superiore 40 Vdc, il modulo esegue le seguenti azioni di risposta:

- Viene eseguito un reset, che causa la reinizializzazione dei moduli alimentati dall'alimentatore.
- Se la soglia di tensione superiore è stata rilevata sulla linea:
 - 24 Vdc del backplane: il PAC viene spento.
 - 3,3 Vdc del backplane: il PAC smette di funzionare, ma continua a ricevere alimentazione.

Per maggiori informazioni su come reagire a queste condizioni vedere la sezione *Diagnostica per le tensioni del backplane 24 Vdc e 3,3 Vdc*, pagina 134.

Moduli di alimentazione ridondanti

I moduli BMXCPS4002S, BMXCPS4022S e BMXCPS3522S sono moduli di alimentazione ridondanti. Due di questi moduli di alimentazione possono essere installati (uno come master e uno come slave) in un rack Ethernet ridondante. Le configurazioni possibili sono le seguenti:

Configurazione	Caratteristiche		
	Gestione della ridondanza (alimentazione di controllo e segnali dei LED)	Invio di dati all'applicazione	Monitoraggio e salvataggio dei dati di alimentazione
2 alimentatori nel rack principale	✓	✓	✓
2 alimentatori nel rack di estensione	✓	X	✓

Configurazione	Caratteristiche		
	Gestione della ridondanza (alimentazione di controllo e segnali dei LED)	Invio di dati all'applicazione	Monitoraggio e salvataggio dei dati di alimentazione
1 alimentatore in un rack esistente	X	X	✓
✓ = supportata. X = non supportata.			

Per ulteriori informazioni sugli alimentatori ridondanti, consultare il capitolo *Descrizione dei moduli di alimentazione Modicon X80* (vedi Modicon X80, Alimentatori e rack , Manuale di riferimento hardware).

Diagnostica del modulo di alimentazione di sicurezza M580

Diagnostica per le tensioni del backplane 24 Vdc e 3,3 Vdc

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S e BMXCPS3522S effettuano automaticamente il rilevamento di una condizione di sovratensione, sovraccarico o cortocircuito sulle tensioni del backplane 24 VDC e 3,3 VDC.

Se l'alimentatore rileva una delle seguenti condizioni sulla tensione 24 Vdc, si verifica quanto segue:

- La funzione di conversione dell'alimentazione viene disattivata per l'intero backplane.
- Viene emesso un comando RESET per tutti i moduli del rack.
- Il LED **OK** dell'alimentatore è OFF.
- L'intero PAC è disinserito.

Se l'alimentatore rileva una di queste condizioni sulla tensione 3,3 Vdc, si verifica quanto segue:

- La funzione di conversione dell'alimentazione viene disinserita per la tensione del backplane 3,3 Vdc.
- Viene emesso un comando RESET per tutti i moduli del rack.
- Il LED **OK** dell'alimentatore è OFF.
- Il funzionamento dell'intero programma PAC viene interrotto, sebbene alcuni circuiti PAC possano continuare a ricevere energia.

In ogni caso, per correggere queste condizioni procedere nel seguente modo:

1. Disinserire la linea di alimentazione principale.
2. Verificare la compatibilità tra l'assorbimento di potenza stimato del PAC rispetto alla capacità del modulo di alimentazione di sicurezza M580 sulle linee del backplane 24 Vdc e 3,3 Vdc.
3. Eliminare la causa della condizione esistente.
4. Attendere 1 minuto dopo la disinserizione del sistema.
5. Applicare potenza sulla linea principale per riavviare il modulo di alimentazione di sicurezza M580.

Diagnostica dei contatti relè di allarme

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S dispongono di un contatto relè di allarme a due pin che permette di ottenere le seguenti informazioni:

- Se il relè è attivato (ossia chiuso):
 - Entrambe le tensioni del backplane 24 Vdc e 3,3 Vdc sono corrette e
 - RESET non è attivo.; e
 - Se l'alimentatore è collocato nel rack locale principale:
 - la CPU è operativa, e
 - la CPU è in modalità RUN.
- Se il relè è disattivato (ossia aperto):
 - Una delle due tensioni del backplane 24 Vdc o 3,3 Vdc o entrambe non sono corrette, oppure
 - RESET è attivo, oppure
 - Se l'alimentatore è collocato nel rack locale principale:
 - la CPU non è operativa, oppure
 - la CPU è in modalità STOP.

DDT di sicurezza M580

Introduzione

I moduli di alimentazione di sicurezza M580 presentano due set di tipi di dati derivati (DDT):

- PWS_DIAG_DDT_V2 per diagnostica
- PWS_CMD_DDT per i comandi

PWS_DIAG_DDT_V2

Offset byte	Nome	Tipo	Commento
0	Riservato	BYTE	–
1	Riservato	BYTE	–
2	PwsMajorVersion	BYTE	Versione firmware maggiore alimentatore
3	PwsMinorVersion	BYTE	Versione firmware minore alimentatore
4	Modello	BYTE	Identificativo modello Identificativo modello: <ul style="list-style-type: none"> • BMXCPS4002S = 01 • BMXCPS4022S = 02 • BMXCPS3522S = 03
5	Stato	BYTE	Stato alimentatore
6	I33BacPos	UINT	Misura corrente sulla linea backplane 3,3V nel ruolo nominale (produttore)
8	V33Buck	UINT	Misura tensione 3,3V Buck
10	I24Bac	UINT	Misura corrente della linea backplane 24V
12	V24Int	UINT	Misura tensione 24V Int
14	Temperatura	INT	Misura della temperatura ambiente
16	OperTimeMasterSincePO	UDINT	Tempo operativo come master dall'ultima accensione
20	OperTimeSlaveSincePO	UDINT	Tempo operativo come slave dall'ultima accensione
24	OperTimeMaster	UDINT	Tempo operativo come master dal momento della produzione
28	OperTimeSlave	UDINT	Tempo operativo come slave dal momento della produzione

Offset byte	Nome	Tipo	Commento
32	Work	UDINT	Lavoro fornito dal momento della produzione
36	RemainingLTPC	UINT	Durata di vita residua in percentuale
38	NbPowerOn	UINT	Numero di accensioni dal momento della produzione
40	NbVoltageLowFail	UINT	Numero errori rilevati sulla tensione del primario dalla soglia inferiore
42	NbVoltageHighFail	UINT	Numero errori rilevati sulla tensione del primario dalla soglia superiore
44	Riservato	UDINT	–
48	Riservato	UDINT	–
52	RemainingLTMO	UINT	Durata di vita residua in mesi
54	Riservato	BYTE	–
63	Riservato	BYTE	–

PWS_CMD_DDT

Offset byte	Nome	Tipo	Commento
0	Riservato	BYTE	–
1	Codice	BYTE	Codice di comando: <ul style="list-style-type: none"> • 1 = scambia • 3 = azzera
2	PwsTarget	BYTE	Alimentatore di destinazione: 1 per sinistro, 2 per destro, 3 per entrambi Alimentatore di destinazione: <ul style="list-style-type: none"> • 1 = sinistro • 2 = destro
3	Riservato	BYTE	–
15	Riservato	BYTE	–

Convalida di un sistema di sicurezza M580

Contenuto del capitolo

Architetture del modulo di sicurezza M580	139
Valori SIL e MTTF del modulo di sicurezza M580.....	147
Calcolo delle prestazioni e dei tempi per il sistema di sicurezza M580	154

Introduzione

Questo capitolo spiega come eseguire i calcoli per la convalida del sistema di sicurezza M580 utilizzato.

Architetture del modulo di sicurezza M580

Introduzione

Questa sezione descrive le architetture interne dei moduli di sicurezza.

Architettura di sicurezza della CPU e del coprocessore di sicurezza M580

Introduzione

Le CPU BME•58•040S e il coprocessore BMEP58CPROS3 (Copro), con funzionalità di coppia di processori, sono certificati da TÜV Rheinland Group per l'uso in soluzioni di sicurezza conformi a Safety Integrity Level 3 (SIL3) M580.

Lavorando insieme, la CPU e il coprocessore forniscono le seguenti funzioni di sicurezza SIL3:

- Doppia esecuzione indipendente del codice del task di sicurezza.
- Confronto dei risultati della doppia esecuzione del codice.
- Autotest periodici.
- Supporto per un'architettura 1oo2D ("uno su due") con diagnostica.

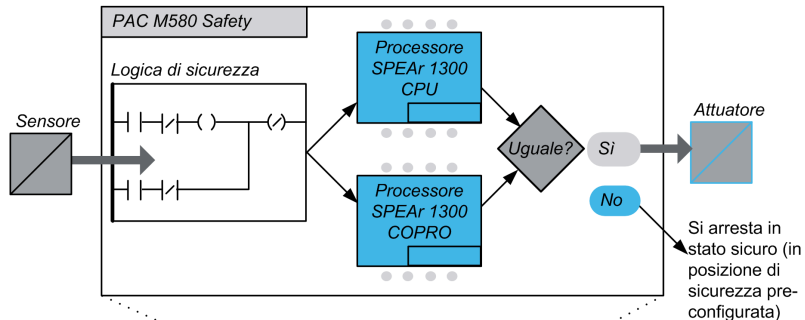
NOTA: Oltre alla funzionalità di sicurezza, le CPU BMEP58•040S forniscono funzionalità comparabili alle CPU M580 standalone non di sicurezza equivalenti e le CPU BMEH58•040S forniscono funzionalità comparabili alle CPU Hot Standby M580 non di sicurezza equivalenti. Per informazioni sulle funzionalità non di sicurezza di queste CPU di sicurezza, consultare *Modicon M580, Hardware, Manuale di riferimento* e *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente*.

Descrizione dell'architettura interna della CPU e del coprocessore

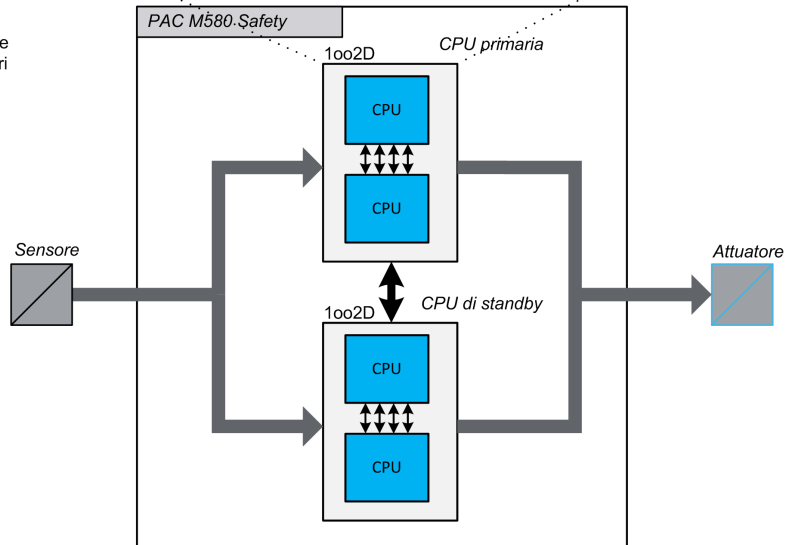
La CPU di sicurezza e il coprocessore M580 contengono un processore SPEAr 1300. Ogni processore esegue la logica di sicurezza nella propria area di memoria e confronta i risultati dell'esecuzione alla fine del task di sicurezza.

La illustrazioni seguenti mostrano l'architettura interna della CPU M580 Safety in configurazioni singola e ridondante:

Architettura singola
basata su 2 processori



Architettura ridondante
basata su 4 processori



Generazione ed esecuzione del doppio codice

I due processori presenti all'interno del PAC di sicurezza M580 provvedono alla generazione e all'esecuzione del doppio codice. La presenza di due processori diversi consente i seguenti vantaggi nel rilevamento degli errori:

- Vengono generati in modo indipendente due codici di programma eseguibili. Viene facilitato il rilevamento degli errori di sistema durante la generazione del codice grazie all'uso di due compilatori indipendenti.

- I due codici di programma generati vengono eseguiti da due processori separati. In questo modo, la CPU può rilevare sia gli errori di sistema nell'esecuzione del codice e gli errori casuali nel PAC.
- Ogni processore utilizza la propria area di memoria indipendente. Gli errori casuali nella RAM possono quindi essere rilevati dal PAC, per cui non è necessario eseguire un test della RAM completo ad ogni scansione.

Architettura 1oo2D

L'architettura 1oo2D (“uno su due con Diagnostica”) significa che due canali indipendenti eseguono la logica di sicurezza e, se viene rilevato un errore su uno dei canali, il sistema passa allo stato sicuro.

Architettura singola

L'architettura PAC M580 Safety singola si basa su 1oo2D composta da processori doppi che garantiscono la compatibilità a SIL3 (safety integrated level) anche in un'architettura non ridondante.

Architettura ridondante

Il PAC M580 Safety nell'architettura ridondante fornisce la massima disponibilità del sistema e attività del processo tramite aggiunta di piena ridondanza (Quadrupla struttura, ad esempio quattro CPU) su controllo, alimentazione e comunicazione.

Una delle CPU (coppia di processori) funge da Primario, esegue l'applicazione tramite esecuzione della logica di programma e attuazione degli IO. La CPU primaria (coppia di processori) aggiorna la CPU secondaria (coppia di processori) in modo che sia pronta per assumere il controllo degli IO.

Il sistema esegue continuamente l'automonitoraggio. In caso di guasto di controllo della CPU primaria, il sistema passa il controllo alla CPU secondaria. In questa modalità degradata, il sistema rimane SIL3. In caso di guasto delle CPU primaria e secondaria, il sistema passa in uno stato fail safe.

Il PAC M580 Safety ridondante, basato su architettura quadrupla (4 processori) consente di aumentare la disponibilità del sistema e garantisce compatibilità SIL3 (safety integrated level).

Watchdog

Un watchdog hardware e un watchdog firmware controllano l'attività del PAC e il tempo necessario per eseguire la logica del programma di sicurezza.

NOTA: Configurare il watchdog software (nella finestra di dialogo **Proprietà di SAFE**) per consentire:

- il tempo di esecuzione dell'applicazione
- il filtraggio degli errori di comunicazione degli I/O rilevati
- il tempo di sicurezza del processo.

Per maggiori informazioni, vedere la sezione *Tempo di sicurezza del processo*, pagina 154.

Controllo della memoria

L'integrità del contenuto della memoria statica viene testata mediante il controllo ciclico della ridondanza (CRC) e l'esecuzione del doppio codice. L'integrità del contenuto della memoria dinamica viene testata mediante l'esecuzione del doppio codice e l'uso di un sistema di codice correzione errore (ECC) che individua e corregge le istanze più comuni di dati interni corrotti. Durante l'avvio a freddo, questi test vengono reinizializzati ed eseguiti completamente prima che la CPU passi in modalità Stop o Run.

Monitoraggio della sovratensione

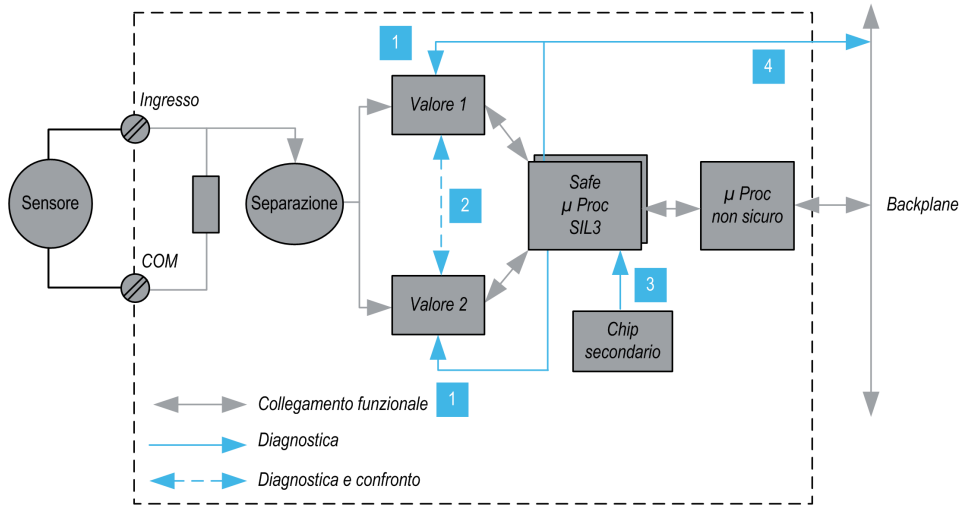
La CPU riceve l'alimentazione dal modulo di alimentazione di sicurezza dedicato M580 sulla linea del backplane. Il modulo di alimentazione di sicurezza fornisce 24V regolati con una tensione max. assoluta compresa nel campo 0...36V.

La CPU contiene una funzione integrata che controlla gli alimentatori interni. Se viene rilevata una condizione di sovratensione o sottotensione, il PAC si spegne.

Architettura di sicurezza del modulo di ingresso analogico BMXSAI0410

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSAI0410 esegue la funzione di sicurezza nel seguente modo:



1 Viene costantemente monitorata la capacità dei dispositivi di misura di misurare, senza errori rilevati, 10 valori analogici compresi tra 4 e 20 mA. Contemporaneamente viene misurata la linearità delle fasi della misura.

2 Ogni valore di ingresso è acquisito da 2 circuiti identici. I valori misurati vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido. Tra i due valori è tollerata una discrepanza massima pari allo 0,35% della scala completa fino a 20 mA.

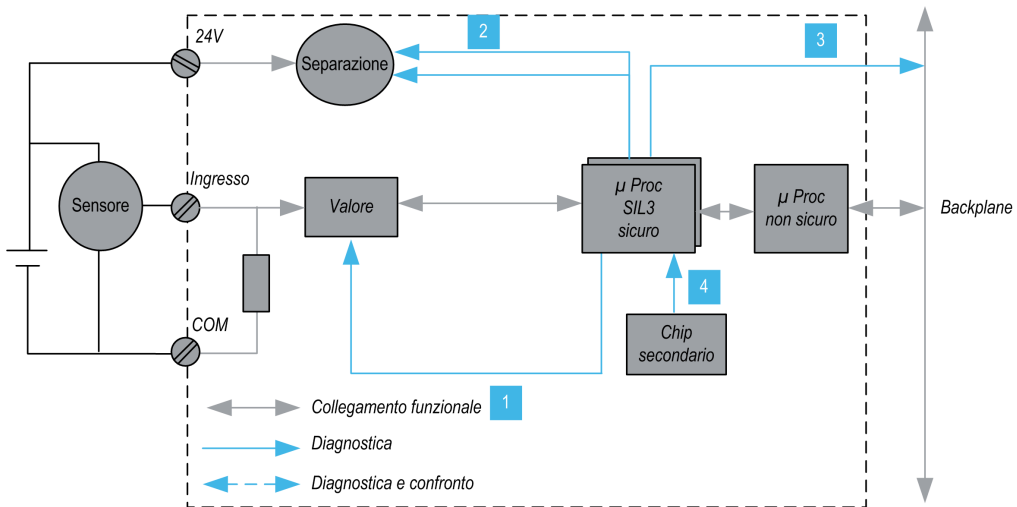
3 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

4 La tensione di alimentazione dal backplane viene monitorata per rilevare un'eventuale condizione di sovratensione o di sottotensione.

Architettura di sicurezza del modulo di ingresso digitale BMXSDI1602

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSDI1602 esegue la funzione di sicurezza nel seguente modo:



1 Viene costantemente monitorata la capacità dei dispositivi di misura di misurare un valore "1" e un valore "0".

2 L'alimentazione esterna 24 Vdc è monitorata costantemente dal processore di sicurezza. Ogni valore di ingresso è acquisito da due circuiti identici. I valori acquisiti vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido.

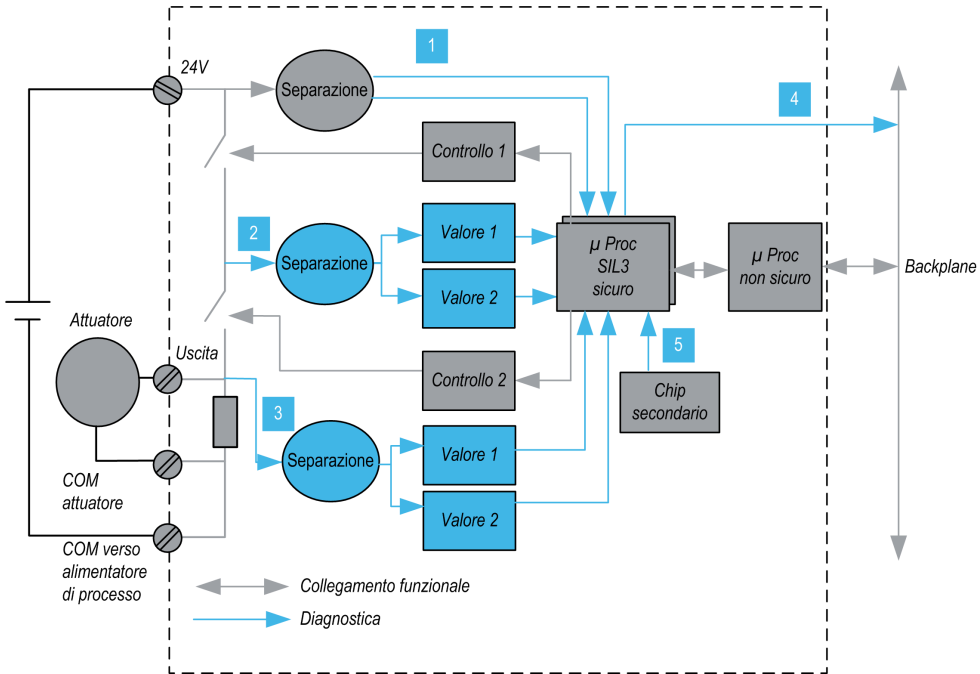
3 La tensione di alimentazione dal backplane viene monitorata per rilevare un'eventuale condizione di sovratensione o di sottotensione.

4 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Architettura di sicurezza del modulo di uscita digitale BMXSDO0802

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSDO0802 esegue la funzione di sicurezza nel seguente modo:

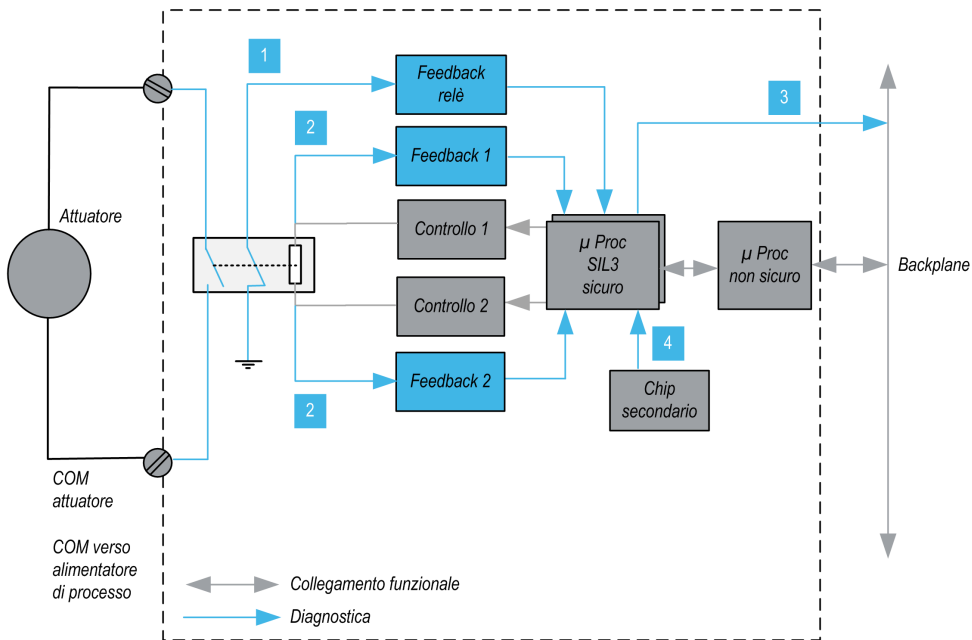


- 1 L'alimentazione esterna 24 Vdc è monitorata costantemente dal processore di sicurezza.
- 2 Ogni uscita consiste di 2 interruttori in serie tra l'alimentazione esterna +24 Vdc e la terra. Il valore del punto medio (2) viene letto in modo ridondante e inviato al processore di sicurezza. I valori misurati dei punti medi vengono confrontati dal processore di sicurezza. Se i valori non corrispondono a quelli previsti, il canale viene dichiarato non valido.
- 3 Anche il valore del punto inferiore (3) viene monitorato per la diagnostica del cablaggio esterno.
- 4 La tensione di alimentazione dal backplane viene monitorata per determinare se sussiste una condizione di sovratensione o di sottotensione.
- 5 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Architettura di sicurezza del modulo di uscita relè digitale BMXSRA0405

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSRA0405 esegue la funzione di sicurezza nel seguente modo:



1 Lo stato del relè è monitorato costantemente dal processore di sicurezza, che legge lo stato di un contatto NC collegato meccanicamente al contatto NO, a sua volta collegato all'attuatore.

2 Lo stato del comando relè è monitorato costantemente. Ogni valore di ingresso è acquisito da 2 circuiti identici. I valori misurati vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido.

3 La tensione di alimentazione dal backplane viene monitorata per determinare se sussiste una condizione di sovratensione o di sottotensione.

4 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Valori SIL e MTTF del modulo di sicurezza M580

Introduzione

Questa sezione descrive i valori SIL e MTTF che si possono utilizzare per i calcoli relativi al modulo di sicurezza M580.

Calcoli del livello di integrità della sicurezza

Classificazione dei prodotti Schneider Electric

Il PAC di sicurezza M580 può comprendere:

- Moduli di sicurezza, che possono eseguire funzioni di sicurezza, tra cui:
 - CPU e coprocessore
 - moduli di I/O
 - alimentazione
- Moduli non interferenti, pagina 29, che non eseguono funzioni di sicurezza, ma consentono di aggiungere elementi non di sicurezza al progetto di sicurezza.

NOTA:

- Dato che i moduli non interferenti non fanno parte del loop di sicurezza, non rientrano nei calcoli del livello di integrità della sicurezza.
- Un errore rilevato in un modulo non interferente non influisce negativamente sull'esecuzione delle funzioni di sicurezza.
- Gli alimentatori BMXCPS4002S, BMXCPS4022S e BMXCPS3522S sono certificati. Dato che presenta un tasso di errore pericoloso trascurabile (<1% del SIL3 desiderato), l'alimentatore non è incluso nei calcoli del livello di integrità di sicurezza per il loop di sicurezza. Di conseguenza, per i moduli di alimentazione non vengono forniti né PFH né PFD.

Valori PFD/PFH per moduli di sicurezza M580

Schneider Electric propone i seguenti moduli di sicurezza certificati per l'uso in applicazioni di sicurezza. I moduli di sicurezza sono elencati con i valori corrispondenti di probabilità di errore, pagina 150 (PFD/PFH) per diversi intervalli dei test di prova, pagina 153 (PTI). Le probabilità PFD/PFH sono espresse come valori che contribuiscono alla probabilità PFD/PFH totale dell'intero loop di sicurezza, pagina 17.

Le tabelle che seguono elencano i moduli di sicurezza e i rispettivi valori PFD/PFH per le applicazioni SIL2 e SIL3, laddove applicabili:

Tipo prodotto	Codice prodotto	SIL	PTI = 1 anno	
			PFD _G	PFH _G
CPU con coprocessore	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.38E-07	1.00E-10
Ingresso analogico	BMXSAI0410	SIL3 ²	5.76E-06	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3 ²	6.81E-06	1.56E-09
Uscita digitale	BMXSDO0802	SIL3 ¹	5.75E-06	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 ³	5.85E-06	1.68E-09
		SIL3 ⁴	5.84E-06	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentatore	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Tipo prodotto	Codice prodotto	SIL	PTI = 5 anni	
			PFD _G	PFH _G
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3 ¹	2.20E-06	1.01E-10
Ingresso analogico	BMXSAI0410	SIL3 ²	2.88E-05	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3 ²	3.41E-05	1.56E-09
Uscita digitale	BMXSDO0802	SIL3 ¹	2.88E-05	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 ³	2.92E-05	1.68E-09
		SIL3 ⁴	2.92E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09

Tipo prodotto	Codice prodotto	SIL	PTI = 5 anni	
			PFD _G	PFH _G
Alimentatore	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Tipo prodotto	Codice prodotto	SIL	PTI = 10 anni	
			PFD _G	PFH _G
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.44E-06	1.02E-10
Ingresso analogico	BMXSAI0410	SIL3 ²	5.76E-05	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3 ²	6.81E-05	1.56E-09
Uscita digitale	BMXSDO0802	SIL3 ¹	5.75E-05	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 ³	5.84E-05	1.68E-09
		SIL3 ⁴	5.84E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentatore	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Tipo prodotto	Codice prodotto	SIL	PTI = 20 anni	
			PFD _G	PFH _G
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3 ¹	9.00E-06	1.04E-10
Ingresso analogico	BMXSAI0410	SIL3 ²	1.15E-04	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3 ²	1.36E-04	1.56E-09
Uscita digitale	BMXSDO0802	SIL3 ¹	1.15E-04	1.31E-09

Tipo prodotto	Codice prodotto	SIL	PTI = 20 anni	
			PFD _G	PFH _G
Uscita relè digitale	BMXSRA0405	SIL2 ³	1.17E-04	1.68E-09
		SIL3 ⁴	1.17E-04	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentatore	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Probabilità di guasto per applicazioni SIL3

Per le applicazioni SIL3, IEC 61508 definisce le seguenti probabilità di guasto su richiesta (PFD) e probabilità di guasto all'ora (PFH) per ogni loop di sicurezza, in base alla modalità di funzionamento:

- $PFD \geq 10^{-4}$ - $< 10^{-3}$ per modalità di domanda di funzionamento bassa
- $PFH \geq 10^{-8}$ - $< 10^{-7}$ per modalità di domanda di funzionamento alta

Il PAC di sicurezza M580 è certificato per un utilizzo in sistemi a bassa domanda e ad alta domanda di funzionamento.

Esempio di calcolo del livello di integrità della sicurezza

Questo esempio di calcolo mostra come determinare:

- Il contributo di rischio dei moduli Schneider Electric all'applicazione di sicurezza; e
- Il restante contributo di rischio che altri dispositivi nel loop di sicurezza (ad esempio, sensori e attuatori) possono aggiungere all'applicazione di sicurezza per un determinato livello di integrità della sicurezza e un modo di funzionamento.

NOTA: Quando si calcola il contributo di rischio di sensori e attuatori all'applicazione di sicurezza, contattare i costruttori di questi dispositivi per ottenere i valori PFD/PFH per l'intervallo del test di prova appropriato.

Questo esempio comprende i seguenti moduli di sicurezza Schneider Electric:

- 1: CPU BMPEP584040S

- 1: Coprocessore BMEP58CPROS3
- 1: Ingresso analogico BMXSAI0410
- 1: Uscita digitale BMXSDO0802
- 1: Alimentatore BMXCPS4002S

Il calcolo seguente utilizza i valori PFH_G per una modalità di funzionamento ad alta domanda per un loop di sicurezza SIL3 con un PTI di 20 anni. Il valore PFH massimo consentito per questa applicazione di sicurezza è 10^{-7} (o $1.0E-7$):

Modulo di sicurezza		Contributo (notazione scientifica)	Contributo residuo per sensori e attuatori
CPU con coprocessore		7.01E-10	-
Ingresso analogico		1.31E-09	
Uscita digitale		1.31E-09	
Alimentatore		-	
Totale	numerico	2.72E-09	97.28E-09
	% max	2,72%	97,28%
Nota 1: l'uscita relè utilizza quattro relè per supportare un'uscita.			

Valori per moduli di sicurezza M580 per macchinari

Schneider Electric propone i seguenti moduli di sicurezza certificati per l'uso in applicazioni di sicurezza per macchinari secondo la norma ISO13849-1. La tabella che segue elenca i moduli di sicurezza e i rispettivi valori, la categoria e il livello, laddove applicabili:

Tipo prodotto	Codice prodotto	Configurazione	Categoria	Performance Level	MTTF (anni)	DCav
CPU con coprocessore	BME•58•040S & BMEP58CPROS3	NA	4	e	235	Alto (>99%)
Ingresso analogico	BMXSAI0410	uso di 1 canale	2	d	255	99,66%
		uso di 2 canali	4	e	255	99,66%
Ingresso digitale	BMXSDI1602	uso di 1 canale	2	d	231	99,69%
		uso di 2 canali	4	e	231	99,69%
Uscita digitale	BMXSDO0802	NA	4	e	253	99,63%
Uscita relè digitale	BMXSRA0405	uso di 1 canale	2	c	156	99,77%

Tipo prodotto	Codice prodotto	Configurazione	Categoria	Performance Level	MTTF (anni)	DCav
		uso di 2 canali	4	e	156	99,77%

Valori per i moduli M580 Safety per il settore ferroviario

Schneider Electric offre i seguenti moduli di sicurezza certificati per il settore ferroviario in base alle norme Cenelec EN50126, EN50128, EN50129. Nella tabella seguente sono elencati i moduli di sicurezza e i relativi valori di affidabilità:

Tipo prodotto	Codice prodotto	SIL	TFFR (PTI = 20 anni)
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL4	1.04E-10
Ingresso analogico	BMXSAI0410	SIL4	1.31E-09
Ingresso digitale	BMXSDI1602	SIL4	1.56E-09
Uscita digitale	BMXSDO0802	SIL4	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL3 ¹	1.68E-09
		SIL4 ²	1.34E-09
		SIL4 ³	1.35E-09
Alimentatore	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL4	–

NOTA: I valori SIL sono a 80° C

1. 1 relè per uscita a 80° C
2. 2 relè per uscita a 80° C
3. 4 relè per uscita a 80° C

La somma di TFFR di un modulo di ingresso, della CPU e del coprocessore, dell'alimentatore e di un modulo di uscita è sempre inferiore a 3.5E-09/h, che è inferiore al budget allocato massimo del 40%, visto come tasso di guasto residuo massimo per una funzione di sicurezza SIL4 che consente di integrare altri prodotti nel loop di sicurezza.

TFFR all'ora e per funzione	Attributo SIL
$10^{-9} \leq \text{TFFR} \leq 10^{-8}$	4
$10^{-8} \leq \text{TFFR} \leq 10^{-7}$	3
$10^{-7} \leq \text{TFFR} \leq 10^{-6}$	2
$10^{-60} \leq \text{TFFR} \leq 10^{-5}$	1

Descrizione dei tempi di sicurezza

Il PAC di sicurezza M580 dispone di un tempo di ciclo minimo del PAC di 10 ms, necessario per elaborare il segnale dai moduli di I/O, eseguire la logica utente e impostare le uscite. Per calcolare il tempo di reazione massimo del PAC, occorre conoscere il tempo di reazione massimo dei sensori e attuatori utilizzati. Inoltre, il tempo di reazione massimo del PAC dipende dal tempo di sicurezza del processo (PST), pagina 154 richiesto dal processo specifico.

Intervallo del test di prova

Il test di prova è un test periodico che va effettuato per rilevare eventuali guasti in un sistema correlato alla sicurezza in modo da poter ripristinare il sistema, se necessario, a una nuova condizione o a quella più vicina possibile a questa condizione. Il periodo di tempo tra questi test è chiamato intervallo del test di prova.

L'intervallo del test di prova dipende dal livello di integrità di sicurezza mirato, dai sensori, dagli attuatori e dall'applicazione del PAC. Il sistema di sicurezza M580 è adatto per essere utilizzato in un'applicazione SIL3 riguardante IEC 61508 e un intervallo di test di tenuta di 20 anni.

Calcolo delle prestazioni e dei tempi per il sistema di sicurezza M580

Introduzione

Questa sezione spiega come calcolare il tempo di reazione PAC, il tempo di reazione del sistema e il tempo di sicurezza del processo per il proprio sistema di sicurezza M580.

Tempo di sicurezza del processo

Descrizione del tempo di sicurezza del processo

Il tempo di sicurezza del processo (process safety time, PST) è una misura essenziale di un processo eseguito da un loop di sicurezza. Viene definito come il periodo di tempo che intercorre tra il verificarsi di un guasto nell'apparecchiatura sotto controllo (EUC, Equipment Under Control) e il verificarsi di un evento pericoloso se la funzione di sicurezza non viene eseguita (ovvero se lo stato sicuro non viene raggiunto).

NOTA: Il tempo di sicurezza del processo è determinato dal processo di sicurezza specifico. È necessario verificare che il sistema relativo alla sicurezza possa eseguire le funzioni di sicurezza entro il tempo di sicurezza del sistema.

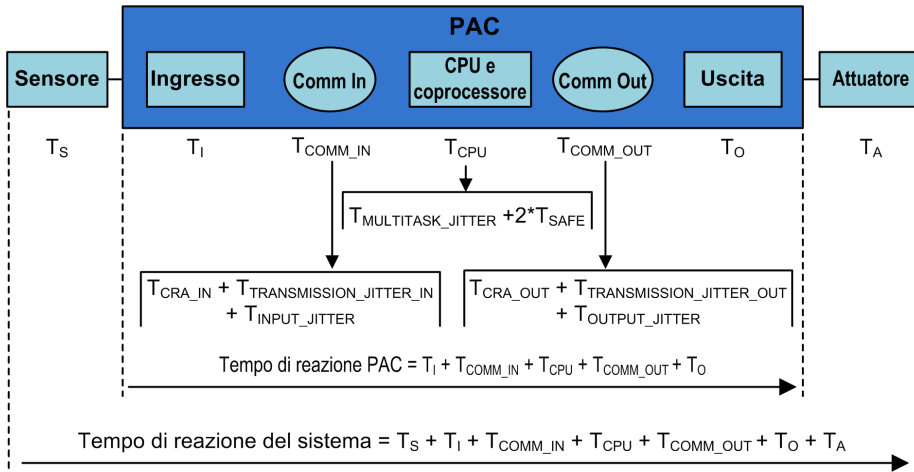
Descrizione del tempo di reazione del sistema

Il tempo di reazione del sistema è la somma del tempo di reazione del PAC e dei tempi di reazione del sensore selezionato (T_S) e dell'attuatore selezionato (T_A).

NOTA: T_S e T_A sono specifici del dispositivo.

Per ogni loop di sicurezza verificare che il tempo di reazione del sistema sia minore del tempo di sicurezza del processo.

Il tempo di reazione del sistema è illustrato di seguito:



I componenti del tempo di reazione del sistema possono includere:

Componente	Descrizione	Valore worst case stimato
T_s	Tempo di reazione richiesto dal sensore selezionato per reagire a un evento di processo.	Specifico del dispositivo.
T_i	Tempo massimo richiesto dal modulo di ingresso per campionare e confermare un evento di sensore. Comprende: <ul style="list-style-type: none"> Un periodo di campionamento del modulo di ingresso. Periodi di campionamento multipli del modulo di ingresso per filtraggio. 	6 ms
T_{COMM_IN}	Ritardo di comunicazione ingressi. I relativi componenti sono descritti nell'argomento <i>Tempo di risposta dell'applicazione nella Modicon M580 Indipendente, Guida di pianificazione del sistema per architetture di utilizzo frequente</i> e comprendono quanto indicato di seguito (i numeri si riferiscono al calcolo ART nell'argomento di riferimento): <ul style="list-style-type: none"> T_{CRA_IN}: CRA_Drop_Process (2) + CRA Input RPI (3) T_{JITTER_IN}: Network_In_Time (4) + Network_In_Jitter (5) + CPU_In_Jitter (6) 	–
T_{CPU}	Il tempo di reazione di CPU e coprocessore, pari alla somma del ritardo causato dai task in sospenso di maggiore priorità (il task FAST) più due tempi di scansione del task SAFE – dove il primo è una scansione mancata e il secondo una scansione riuscita: $T_{MULTITASK_JITTER} + 2 * T_{SAFE}$.	
$T_{MULTITASK_JITTER}$	Il ritardo massimo provocato dall'esecuzione di task in sospenso con priorità più alta. In questo caso, il task FAST. $T_{MULTITASK_JITTER} = T_{FAST}$.	–

Componente	Descrizione	Valore worst case stimato
T _{SAFE}	Periodo del task SAFE configurato.	–
T _{FAST}	Questo valore viene incluso perché l'esecuzione del task FAST è prioritaria rispetto al task SAFE. NOTA: Per semplificare la formula, si presume che nessun task del sistema si trovi in condizione di overrun. Pertanto questo valore equivale al periodo del task FAST configurato, o a 0 se il task FAST non è configurato.	–
T _{COMM_OUT}	Ritardo di comunicazione uscite. I relativi componenti sono descritti nell'argomento <i>Tempo di risposta dell'applicazione</i> nella <i>Modicon M580 Indipendente, Guida di pianificazione del sistema per architetture di utilizzo frequente</i> e comprendono quanto indicato di seguito (i numeri si riferiscono al calcolo ART nell'argomento di riferimento): <ul style="list-style-type: none"> • T_{CRA_OUT}: CRA_Drop_Process (12) • T_{JITTER_IN}: CPU_Out_Jitter (9) + Network_Out_Time (10) + Network_Out_Jitter (11) 	–
T _O	Equivale alla somma dei seguenti tempi: <ul style="list-style-type: none"> • Tempo di ritardo tra la lettura e l'applicazione del valore di uscita della CPU (0...3 ms). • Tempo richiesto dal modulo di uscita di sicurezza per modificare l'uscita fisica, ossia per propagare lo scambio dalla RAM X all'uscita fisica (tra 0...3 ms). 	6 ms
T _A	Tempo di reazione dell'attuatore selezionato.	Specifico del dispositivo.

Descrizione del tempo di reazione del PAC

Per gli I/O situati nel rack principale locale (con la CPU), il tempo di reazione del PAC è la somma dei tempi di reazione correlati per il modulo di ingresso selezionato (T_I) e il modulo di uscita selezionato (T_O), più il tempo di reazione della CPU e del coprocessore (T_{CPU}):

Tempo di reazione PAC (locale) = T_{CPU} + T_{COMM_IN} + T_I + T_{COMM_OUT} + T_O

Se gli I/O si trovano su un rack remoto, il tempo di reazione del PAC include anche il tempo di ritardo di comunicazione degli ingressi (T_{COMM_IN}) e il tempo di ritardo di comunicazione delle uscite (T_{COMM_OUT}):

Tempo di reazione PAC (remoto) = T_{CPU} + T_{COMM_IN} + T_I + T_{COMM_OUT} + T_O

Descrizione del tempo di reazione della CPU e del coprocessore

Il tempo di reazione della CPU e del coprocessore è influenzato direttamente dal periodo del task SAFE e dal periodo del task FAST. Verificare che la logica di sicurezza sarà eseguita entro il periodo del task SAFE.

Poiché può comparire un segnale all'inizio del ciclo di esecuzione quando i segnali sono già stati elaborati, possono essere necessari due cicli del task SAFE per reagire al segnale.

Poiché il task FAST ha la priorità sul task SAFE, quando si stima il tempo di reazione di CPU e coprocessore occorre anche considerare il tempo necessario per l'esecuzione del task FAST quando si valuta il jitter.

Ne consegue la seguente equazione per il tempo di reazione massimo (caso peggiore):

Tempo di reazione della CPU e del coprocessore = $2 \times T_{SAFE} + T_{FAST}$

NOTA: Se si usa la comunicazione peer-to-peer sicura, pagina 183 per eseguire la funzione di sicurezza, la stima del tempo di reazione della CPU è diversa.

Descrizione del tempo per moduli di ingresso

I tempi massimi (worst case) per il modulo di ingresso digitale di sicurezza e per il modulo di ingresso analogico di sicurezza T_I sono pari a 6 ms.

Descrizione del tempo per moduli di uscita

Il tempo massimo T_O per il modulo di uscita digitale di sicurezza è stimato a 6 ms.

Occorre configurare un timeout di posizionamento di sicurezza S_TO per il modulo di uscita digitale, pagina 109 e il modulo di uscita relé digitale, pagina 126. In base al periodo del task SAFE configurato (T_{SAFE}), il valore per S_TO deve essere configurato come indicato di seguito:

- Se $(2,5 * T_{SAFE}) \leq 40$ ms, impostare S_TO a un minimo di 40 ms.
- Se $(2,5 * T_{SAFE}) > 40$ ms, impostare S_TO a un minimo di $(2,5 * T_{SAFE})$ ms.

AVVISO

RISCHIO DI FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Impostare il timeout di posizionamento di sicurezza (S_TO) per un modulo di uscita di sicurezza ad almeno un valore maggiore del più grande tra 40 ms o $(2,5 * T_{SAFE})$, dove T_{SAFE} è pari al periodo del task SAFE configurato.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Per applicazioni Hot Standby, considerare l'impatto sul parametro del timeout del posizionamento di sicurezza (S_TO) di tempo aggiuntivo (T_{SWAP}) richiesto da uno scambio, pagina 158 e di un tempo aggiuntivo T_{SWITCH} richiesto da uno switchover, pagina 160.

Calcolo del tempo di reazione del sistema

Conoscendo il tempo di sicurezza del processo (PST) e il tempo di reazione massimo di sensori e attuatori, si può calcolare il tempo di reazione del sistema (SRT) massimo ammissibile nel processo.

Il tempo di reazione max. (worst case) del sistema può essere calcolato come segue:

Per sistemi con I/O in derivazioni remote:

$$\text{Max SRT} = T_S + T_I + 2 \times T_{\text{CRA}} + T_{\text{RPI}} + 2 \times T_{\text{SAFE}} + T_{\text{FAST}} + T_O + T_A.$$

oppure

$$\text{Max SRT} = 16 \text{ ms} + T_S + 2,5 \times T_{\text{SAFE}} + T_{\text{FAST}} + T_A.$$

Per sistemi con I/O locali:

$$\text{Max SRT} = T_S + T_I + 2,5 \times T_{\text{SAFE}} + T_{\text{FAST}} + T_O + T_A.$$

oppure

$$\text{Max SRT} = 15 \text{ ms} + T_S + 2,5 \times T_{\text{SAFE}} + T_{\text{FAST}} + T_A.$$

NOTA: Per i PAC Hot Standby, per il calcolo del tempo di reazione di sicurezza massimo, prendere in considerazione i componenti aggiuntivi ai calcoli precedenti:

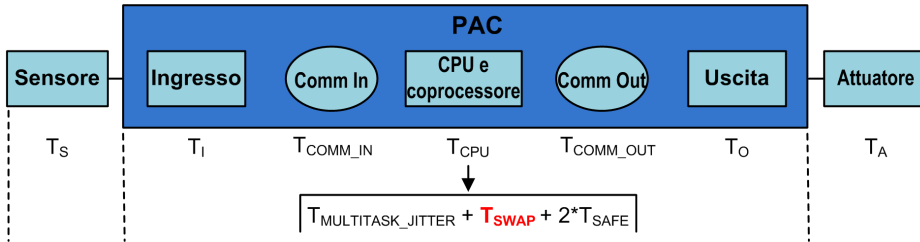
- Mentre si verifica un evento imprevisto e uno switchover, il tempo di reazione massimo potrebbe aumentare aggiungendo il componente, pagina 160 T_{SWITCH} ai calcoli precedenti.
- Mentre l'operatore del sistema esegue uno scambio, il tempo di reazione massimo potrebbe aumentare con un componente aggiuntivo, pagina 158 T_{SWAP} ai calcoli precedenti.

Tempo di reazione del sistema durante uno scambio

Uno scambio è un'azione avviata dall'operatore su un sistema Hot Standby, che provoca lo scambio dei ruoli dei PAC primario e di standby. Lo scambio consuma tempo aggiuntivo, perché durante lo scambio non si possono perdere informazioni e tutte le uscite del sistema devono aver timeout sicuri.

Il componente di tempo dello scambio viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER} , come indicato di seguito:

Il componente di tempo T_{SWAP} viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER} . La sequenza è mostrata di seguito. Tranne per l'inclusione del componente di scambio, la descrizione del tempo di reazione del sistema è uguale a quella descritta in precedenza, pagina 154:



Il componente del tempo T_{SWAP} è la somma di:

$$T_{ADDITIONAL_JITTER} + T_{TRANSFER}$$

I componenti specifici dello scambio sono descritti di seguito:

Componente	Descrizione	Valore worst case stimato
$T_{ADDITIONAL_JITTER}$	Jitter introdotto dal sistema multi-task per riavviare il task sul nuovo PAC. Quindi, $T_{ADDITIONAL_JITTER} = T_{SAFE}$.	–
$T_{TRANSFER}$	Durante la diagnostica del task MAST, il PAC accetta il comando Scambia e inizia a eseguire il trasferimento di tutti i dati più recenti per ogni task.	Vedere la formula seguente.

$T_{TRANSFER}$ può essere calcolato come indicato di seguito:

$$K3 \times (MAST_{KB} + 2 \times SAFE_{KB} + FAST_{KB}) + K4 \times (MAST_{DFB} + 2 \times SAFE_{DFB} + FAST_{DFB}) / 1000$$

Dove:

- $TASK_{KB}$ = Dimensione dei dati (in KB) scambiati per il TASK tra il PAC primario e il PAC di standby.
- $MAST_{DFB}$ = Il numero di DFB dichiarati nel TASK.
- K3 e K4 sono costanti, con valori determinati dal modulo CPU specifico utilizzato nell'applicazione, come indicato di seguito:

Coefficiente	BMEH582040S	BMEH584040S oppure BMEH586040S
K3	46,4 μ s/kB	14,8 μ s/kB
K4	34,5 μ s/istanza DFB	11,0 μ s/istanza DFB

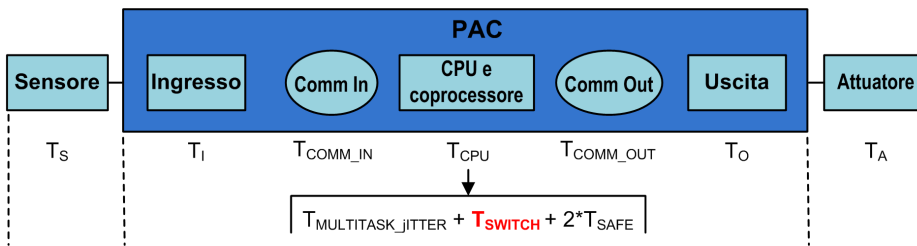
Se l'operatore di sistema vuole eseguire uno scambio senza uscite del modulo di sicurezza che vanno in stato di posizionamento di sicurezza, impostare il parametro di timeout di

posizionamento di sicurezza dei moduli di uscita di sicurezza (S_TO) ad almeno un valore maggiore di: $T_{MULTITASK_JITTER} + T_{SWAP} + T_{SAFE}$.

Tempo di reazione del sistema durante uno switchover

Lo switchover si verifica quando il PAC di standby in un sistema Hot Standby diventa il PAC primario in risposta a un evento imprevisto, ad esempio, quando l'hardware nel PAC primario diventa improvvisamente non operativo. Lo scopo dello switchover è, per il nuovo PAC primario, di sostituire senza interruzioni quello vecchio e iniziare le operazioni dal punto in cui il precedente PAC primario ha cessato di funzionare. Tuttavia, l'ultimo ciclo potrebbe dover essere rieseguito. Lo scopo del sistema è raggiungere il ripristino più rapido possibile.

Il componente di tempo T_{SWITCH} viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER} . La sequenza è mostrata di seguito. Tranne per l'inclusione del componente di switchover, la descrizione del tempo di reazione del sistema è uguale a quella descritta in precedenza, pagina 154:



Il componente del tempo T_{SWITCH} è la somma di:

$$T_{DETECT} + T_{ADDITIONAL_JITTER}$$

I componenti specifici dello switchover sono descritti di seguito:

Componente	Descrizione	Valore worst case stimato
T_{DETECT}	Tempo utilizzato dal PAC di standby per rilevare e confermare che il PAC primario è diventato non operativo.	15 ms
$T_{ADDITIONAL_JITTER}$	Jitter introdotto dal sistema multi-task per riavviare il task sul nuovo PAC. Quindi, $T_{ADDITIONAL_JITTER} = T_{SAFE}$.	–

A differenza dallo scambio, non è necessario tempo aggiuntivo per eseguire un trasferimento di dati.

Per consentire al sistema di rispondere a un evento imprevisto ed eseguire uno switchover senza uscite del modulo di sicurezza che vanno in stato di posizionamento di sicurezza, impostare il parametro di timeout di posizionamento di sicurezza dei moduli di uscita di sicurezza (S_TO) ad almeno un valore maggiore di: $T_{JITTER} + T_{SWITCH} + T_{SAFE}$.

Configurazione dei periodi massimi dei task SAFE e FAST della CPU

Il PAC di sicurezza M580 può effettuare soltanto l'esecuzione periodica dei task SAFE e FAST (l'esecuzione ciclica non è supportata per questi task).

Le impostazioni del **Periodo** del task SAFE e del **Watchdog** della CPU massimo consentito sono configurate nella scheda **Generale** della finestra di dialogo **Proprietà di SAFE**. Le impostazioni dell'uscita digitale di sicurezza **Timeout posizionamento di sicurezza** sono configurate nella scheda **Configurazione** del modulo di uscita, pagina 103.

Analogamente, le impostazioni del **Periodo** del task FAST e del **Watchdog** della CPU massimo consentito sono configurate nella scheda **Generale** della finestra di dialogo **Proprietà di FAST**.

NOTA:

- L'intervallo di valori di impostazione ammessi per il periodo del task SAFE è 10...255 ms, con un valore predefinito di 20 ms.
- L'intervallo di valori di impostazione ammessi per il periodo del task FAST è 1...255 ms, con un valore predefinito di 5 ms.
- L'intervallo di valori di impostazione ammessi per il watchdog è 10...500 ms, con un valore predefinito di 250 ms.
- L'intervallo delle impostazioni ammesse per il timeout di posizionamento di sicurezza delle uscite digitali è 0...65535 ms, con un valore predefinito di 500 ms.

Verificare che l'impostazione del watchdog sia maggiore del periodo del task SAFE.

Verificare l'impostazione del periodo del task SAFE della CPU al momento della messa in servizio del progetto. Attualmente Control Expert Safety fornisce i valori in tempo reale dal PAC.

Queste informazioni sono disponibili in Control Expert Safety nella scheda **Task** selezionando la voce di menu **Strumenti > Schermo PLC**.

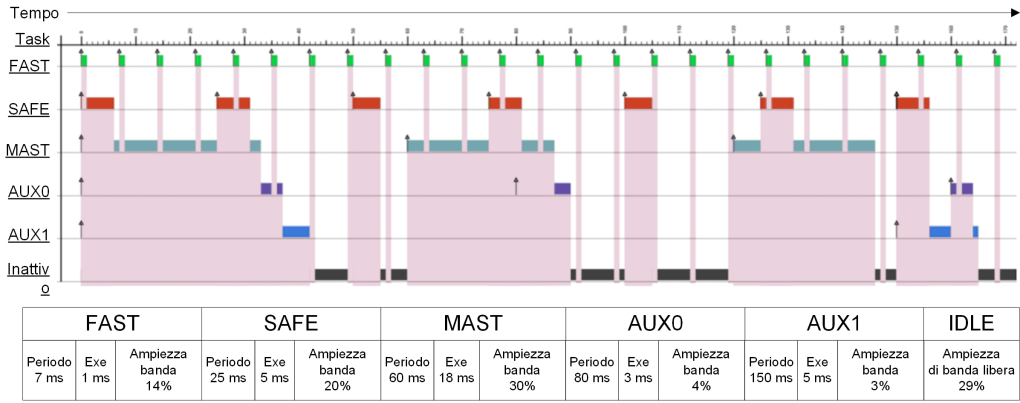
AVVERTIMENTO

RISCHIO DI SUPERAMENTO DEL TEMPO DI SICUREZZA DEL PROCESSO

Impostare il periodo massimo del task SAFE della CPU tenendo conto del tempo di sicurezza del processo. Il periodo del task SAFE della CPU deve essere minore del tempo di sicurezza del processo.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il disegno seguente illustra l'esecuzione di ogni task in un sistema multi-task e mostra la priorità delle risorse della CPU in base alla priorità dei task:



NOTA: quando il task MAST non è in modalità ciclica e per le prestazioni ottimali della CPU, Schneider Electric consiglia di lasciare inattivo il 20% di larghezza di banda della CPU.

Calcolo dell'impatto dei periodi di esecuzione dei task sulla larghezza di banda della CPU

Ogni task configurato utilizza una parte del tempo di elaborazione, o larghezza di banda, della CPU. Il valore stimato della percentuale di larghezza di banda della CPU utilizzata da un task è il risultato (o quoziente) del valore stimato del tempo di esecuzione richiesto da un task (E_{TASK}) diviso per il periodo di esecuzione configurato per tale task (T_{TASK}) e può essere descritto come segue:

$$\text{Larghezza di banda del task} = E_{TASK} / T_{TASK}.$$

Pertanto, il valore percentuale totale della larghezza di banda della CPU utilizzata da un'applicazione è la somma dei valori percentuali delle larghezze di banda della CPU utilizzate per tutti i task.

NOTA: quando il task MAST non è in modalità ciclica e per le prestazioni ottimali della CPU, Schneider Electric consiglia di consumare la percentuale totale di larghezza di banda della CPU con un'applicazione che non ecceda l'80%.

La tabella seguente presenta due applicazioni e indica l'impatto di task ad alta priorità (FAST e SAFE) sull'uso della larghezza di banda totale della CPU.

N.	FAST			SAFE			MAST			AUX0			Totale
	Per	Exe	BW %	Per	Exe	BW%	Per	Exe	BW%	Per	Exe	BW%	
1	5 ms	1 ms	20%	20 ms	5 ms	25%	50 ms	18 ms	35%	200 ms	30 ms	15%	96%
2	7 ms	1 ms	14%	25 ms	5 ms	20%	60 ms	18 ms	30%	200 ms	30 ms	15%	79%

Per = Task period (T_{TASK})
 Exe = Tempo di esecuzione richiesto per il task (E_{TASK})
 BW% = larghezza di banda del task.

Impatto delle comunicazioni CIP Safety sul tempo di reazione del sistema di sicurezza

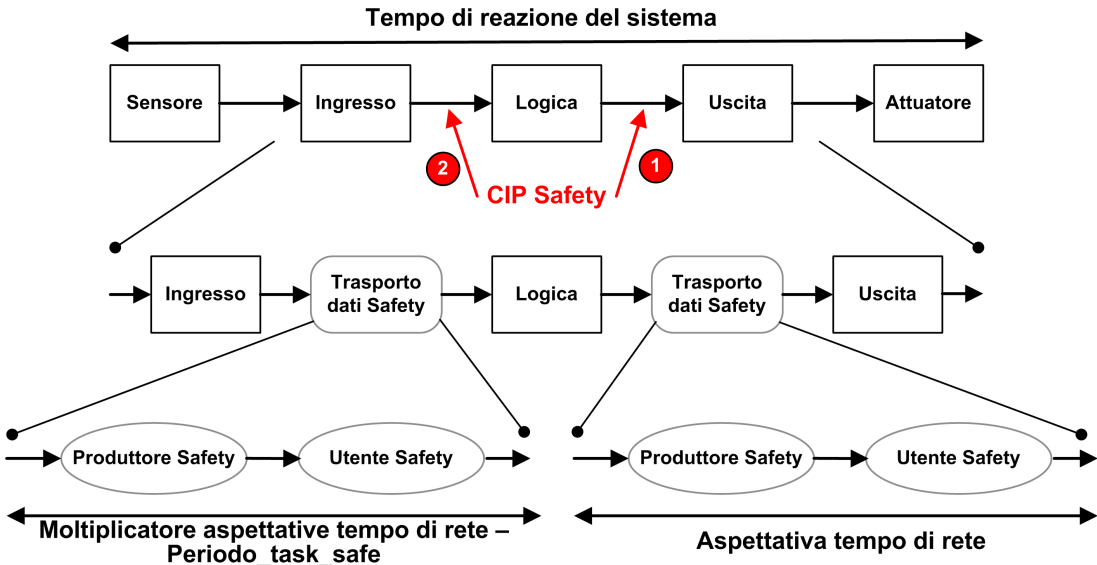
Introduzione

Il tempo impiegato dalla comunicazione CIP Safety, chiamato *aspettativa tempo di rete*, viene aggiunto al e fa parte del *tempo di reazione del sistema*, pagina 154. L'aspettativa tempo di rete rappresenta il periodo di tempo massimo, o caso peggiore, a partire dal momento in cui i dati vengono catturati dal produttore di dati di sicurezza fino a quando l'applicazione di utilizzo riconosce lo stato di sicurezza. Ciò comprende anche errori durante la produzione e l'utilizzo.

Se la comunicazione CIP Safety è compresa tra ingresso e logica, sostituire la variabile termine TCOMM_IN nel calcolo del tempo di sicurezza processo, pagina 154 con *Aspettativa tempo di rete – Periodo_task_safe* Se la comunicazione CIP Safety è compresa tra logica e uscita, sostituire la variabile termine TCOMM_OUT nel calcolo del tempo di sicurezza processo con *Aspettativa tempo di rete*.

Le misure predefinite dell'Aspettativa tempo di rete possono variare, in base al ruolo della CPU di sicurezza M580 come produttore o utilizzatore.

Gli elementi dell'aspettativa tempo di rete e il posizionamento di quest'ultima nel contesto del tempo di reazione del sistema sono indicati nel seguente diagramma:



1 CPU CIP Safety come produttore

2 CPU CIP Safety come utilizzatore

Calcolo dell'Aspettativa tempo di rete

L'aspettativa tempo di rete può essere calcolata con la formula seguente:

$$\text{Aspettativa tempo di rete} = \text{Moltiplicatore_Aspettativa_tempo_di_rete} * 128 \mu\text{Sec} > (\text{EPI} * \text{Moltiplicatore_Timeout} + \text{Ora_Messaggio_sicurezza}(\text{max}) + \text{Ora_Messaggio_Coord_Tempo}(\text{max}) + \text{Costante_Correzione_Connessione} * 128 \mu\text{Sec})$$

Dove:

- **Ora_Messaggio_sicurezza(max)** è il tempo effettivo intercorso tra il momento in cui i dati vengono catturati dal produttore dati di sicurezza e il momento in cui i dati di sicurezza vengono passati all'applicazione consumatrice per l'utilizzo.
- **Ora_Messaggio_Coord_Tempo(max)** è il tempo massimo necessario per l'invio dell'informazione di coordinamento di tempo dall'utilizzatore al produttore.
- **Moltiplicatore_Timeout** è un parametro utilizzato dall'elaboratore del protocollo CIP Safety, che determina il numero di messaggi che potrebbero andare persi prima di dichiarare un errore di connessione. Un Moltiplicatore_Timeout pari a 1 indica che nessun messaggio viene perso.

- **Costante_Correzione_Connessione** è un valore a incrementi di 128 µSec che viene sottratto dal time stamp per rappresentare il peggiore errore possibile causato da una deviazione di tempo, dalla natura asincrona degli orologi del produttore e utilizzatore e dal tempo minimo necessario al Messaggio di Coordinamento di tempo per passare dall'utilizzatore al produttore.
- **EPI** è l'intervallo di pacchetto atteso ed è basato su un periodo task SAFE configurato.
- **Moltiplicatore_Aspettativa_tempo_di_rete** e **Moltiplicatore_Timeout** sono parametri di comunicazione CIP configurati per il frame di connessione SafetyOpen di tipo 2, pagina 369.

Valori predefiniti dell'Aspettativa tempo di rete

Il calcolo predefinito del valore dell'aspettativa tempo di rete dipende dal ruolo della CPU CIP Safety come utilizzatore (caso 2 del diagramma precedente) o produttore (caso 1).

CPU come utilizzatore (caso 2):

- $Moltiplicatore_Timeout = 2$
- $EPI = \text{periodo task SAFE} / 2$
- $Ora_Messaggio_di_sicurezza(max) = \text{Periodo task Safe} + 20 \text{ ms}$ (caso peggiore)
- $Ora_Messaggio_Coord_Tempo(max) = \text{Periodo task Safe} + 20 \text{ ms}$ (caso peggiore)
- $Costante_Correzione_Connessione = 0 \text{ ms}$

Aspettativa tempo di rete = $1,5 * \text{Aspettativa_tempo_di_rete minima} = 1,5 * (3 * \text{Periodo task safe} + 40 \text{ ms}) = 4,5 * \text{Periodo task safe} + 60 \text{ ms}$

CPU come produttore (caso 1):

- $Moltiplicatore_Timeout = 2$
- $EPI = \text{periodo task SAFE}$
- $Ora_Messaggio_di_sicurezza(max) = \text{Periodo task Safe} + 20 \text{ ms}$ (caso peggiore)
- $Ora_Messaggio_Coord_Tempo(max) = \text{Periodo task Safe} + 20 \text{ ms}$ (caso peggiore)
- $Costante_Correzione_Connessione = 0 \text{ ms}$

Aspettativa tempo di rete = $1,5 * \text{Aspettativa_tempo_di_rete minima} = 1,5 * (4 * \text{Periodo task safe} + 40 \text{ ms}) = 6 * \text{Periodo task safe} + 60 \text{ ms}$

Libreria di sicurezza

Contenuto del capitolo

Libreria di sicurezza 166

Libreria di sicurezza

Presentazione della libreria di sicurezza

Quando si installa Control Expert Safety, vengono automaticamente inclusi una libreria di sicurezza di funzioni elementari (EF), blocchi funzione elementari (EFB) e blocchi funzione derivati (DFB). Questi EF, EFB e DFB sono identificati dal prefisso "S_" e sono riservati all'uso in sezioni di codice gestite dal task SAFE.

NOTA: Inoltre viene installata una raccolta aggiuntiva di EF, EFB e DFB. Si tratta della stessa raccolta di oggetti dati usata dai PC M580 non di sicurezza. Questi EF, EFB e DFB possono essere usati solo in sezioni di codice gestite dai task dello spazio dei nomi di processo (MAST, FAST, AUX0 e AUX1).

Per una descrizione dei blocchi inclusi nella libreria M580 di sicurezza, vedere il documento *Control Expert - Libreria dei blocchi di sicurezza*.

Funzioni e blocchi funzione di sicurezza certificati

⚠ AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPLICAZIONE

- Non utilizzare la V1.00 del blocco di funzioni derivate S_GUARD_LOCKING nell'applicazione.
- In Unity Pro 13.0 XLS o successiva, aggiornare il blocco funzione S_GUARD_LOCKING dell'applicazione con V1.01 o successiva e ricompilare l'applicazione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA:

Unity Pro è il nome precedente di Control Expert per versione 13.1 o precedenti.

Di seguito sono elencati gli EF e i blocchi funzione che possono essere usati nella logica di sicurezza e che sono forniti nella libreria di sicurezza.

Famiglia	Gruppo o nome	Tipo	Descrizione
Logica	S_AND_*, S_OR_*, S_XOR_*, S_NOT_*, S_SHL_*, S_SHR_*, S_ROR_*, S_ROL_*	EF	Specifico del tipo, ad esempio S_AND con 2 - 32 ingressi (codice inline)
Logica	S_RS, S_SR, S_F_TRIG, S_R_TRIG	EFB	–
Matematica	S_ADD_*, S_MUL_*, S_SUB_*, S_DIV_*, S_ABS_*, S_SIGN_*, S_NEG_*, S_MOVE, S_SQRT_REAL	EF	Gestione errori rilevati specifica del tipo (ad esempio overflow) da considerare (codice inline)
Confronto	S_GT_*, S_GE_*, S_LT_*, S_LE_*, S_NE_*, S_EQ_*	EF	Specifico del tipo (codice inline)
Statistica	S_LIMIT_*, S_MAX_*, S_MIN_*, S_MUX_*, S_SEL	EF	Specifico del tipo (codice inline)
Tipo a tipo	S_BIT_TO*, S_BOOL_TO_*, S_BYTE_TO_*, S_DINT_TO_*, S_DWORD_TO_*, S_INT_TO_*, S_REAL_TO_*, S_TIME_TO_*, S_UDINT_TO_*, S_UINT_TO_*, S_WORD_TO_*	EF	Specifico del tipo (codice inline)
Temporizzatori e contatori	S_CTU_*, S_CTD_*, S_CTUD_*	EFB	Specifico del tipo
Temporizzatori e contatori	S_TON, S_TOF, S_TP	EFB	–
Peer to peer	S_RD_ETH_MX, S_WR_ETH_MX, S_RD_ETH_MX2, S_WR_ETH_MX2	DFB	Funzioni per eseguire una comunicazione peer-to-peer di sicurezza
Connessione attuatori	S_EDM, S_ENABLE_SWITCH, S_ESPE, S_OUTCONTROL, S_GUARD_LOCKING, S_GUARD_MONITORING, S_MODE_SELECTOR	DFB	Blocchi funzione di sicurezza macchina collegati ad attuatori
Connessione sensori	S_EQUIVALENT, S_ANTIValent, S_EMERGENCYSTOP, S_TWO_HAND_CONTROL_TYPE_II, S_TWO_HAND_CONTROL_TYPE_III, S_MUTING_SEQ, S_MUTING_PAR, S_AI_COMP	DFB	Blocchi funzione di sicurezza macchina collegati a sensori
Sistema	S_SYST_STAT_MX, S_SYST_TIME_MX, S_SYST_CLOCK_MX, S_SYST_RESET_TASK_BIT_MX, S_SYST_READ_TASK_BIT_MX	EFB	Blocchi funzione di sistema

Funzioni e blocchi funzione di sicurezza non certificati

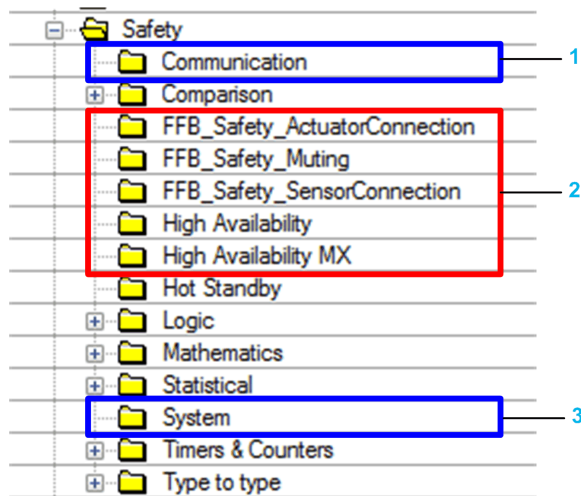
Di seguito è elencato un sottoinsieme di blocchi di funzioni derivate (DFB) che possono essere usati nella logica di sicurezza. Questi blocchi funzione non sono certificati. Il loro scopo è quello di fornire modelli di blocchi funzione di sicurezza che possono essere

facilmente riutilizzati e adattati. È possibile copiare e incollare questi blocchi funzione nella propria applicazione e modificarli per soddisfare i requisiti dell'applicazione.

Famiglia	Gruppo o nome	Tipo	Descrizione
Alta disponibilità MX	S_DIHA, S_AIHA	DFB	Funzione per moduli di ingresso digitali SIL2 o SIL3 ad alta disponibilità (codice inline)
Connessione sensori	AI_COMP	DFB	Blocchi funzione di sicurezza macchina collegati a sensori

Visualizzazione della libreria di sicurezza in Control Expert

Si può accedere alla libreria di sicurezza solo dal task SAFE. Quando si apre una libreria di sicurezza nell'**FBD Editor**, la libreria di sicurezza presenta gruppi di EF, EFB e DFB. Alcuni di questi gruppi comprendono versioni di sicurezza di funzioni e blocchi che si trovano in task non di sicurezza. Altri gruppi, riportati di seguito, contengono funzioni e blocchi specifici del task SAFE:



- 1 Blocchi per la lettura e la scrittura dei valori dei dati di sicurezza.
- 2 Blocchi per l'esecuzione di task specifici della sicurezza.
- 3 Blocchi per la lettura e la scrittura dei valori del sistema di sicurezza.

Per un esempio di come sono implementati i blocchi di sicurezza, vedere l' esempio di configurazione di comunicazione PAC-PAC, pagina 185, che comprende S_RD_ETH_MX e S_WR_ETH_MX.

Per una descrizione di ogni funzione e blocco di sicurezza vedere anche *EcoStruxure™ Control Expert - Libreria dei blocchi di sicurezza*.

Separazione dei dati in un sistema di sicurezza M580

Contenuto del capitolo

Separazione dei dati in un progetto di sicurezza M580.....	171
Come trasferire i dati tra le aree dello spazio dei nomi.....	174

Introduzione

Questo capitolo descrive la separazione dei dati in un sistema di sicurezza M580.

Separazione dei dati in un progetto di sicurezza M580

Separazione dei dati e ambito

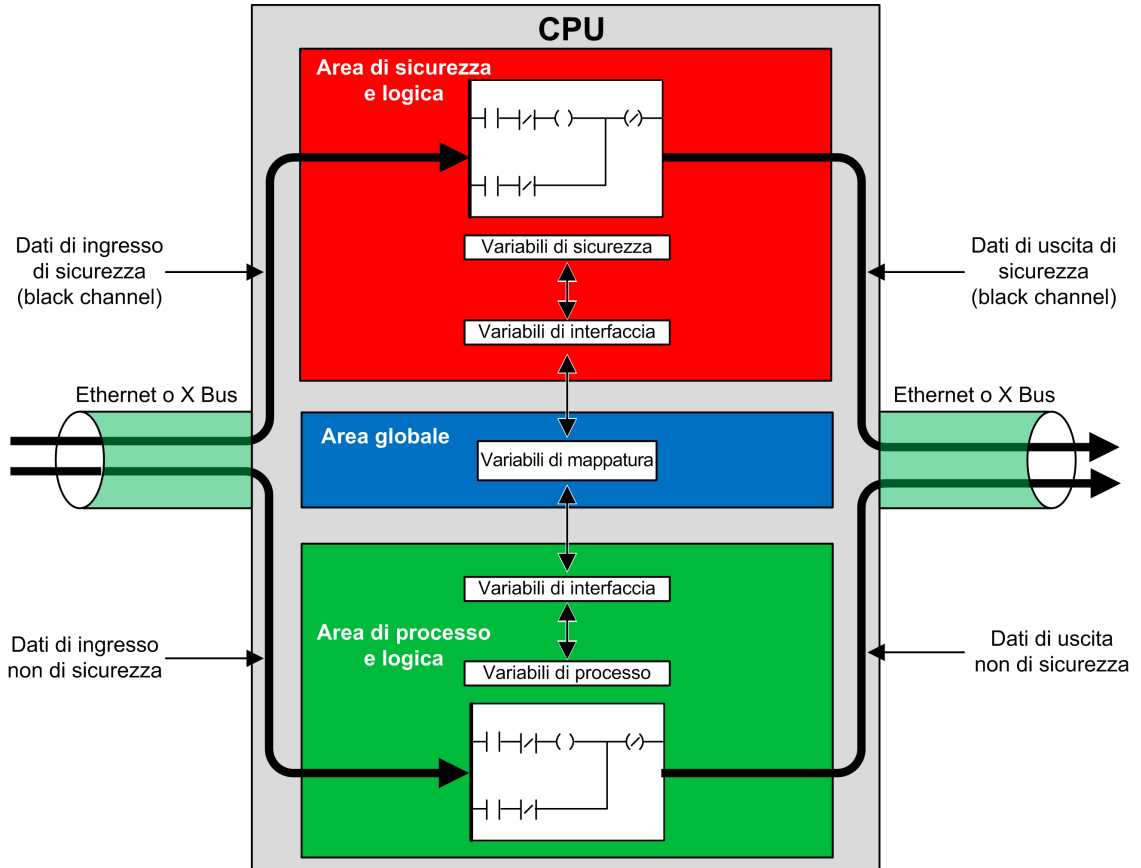
Un progetto di sicurezza M580 include sia un programma di sicurezza sia un programma di processo (non di sicurezza). Control Expert isola la logica e i dati utilizzati dal programma di sicurezza dalla logica e dai dati utilizzati dal programma di processo. Per questo, Control Expert colloca ogni parte del progetto nel proprio spazio dei nomi (detto anche area), *sicuro* o *di processo*.

A seguito di questa configurazione, l'ambito di una variabile di sicurezza è limitato all'area sicura e l'ambito di una variabile di processo è limitato all'area di processo. Questo diventa evidente quando si aggiunge la logica di programma all'applicazione:

- Quando si configura un EF o EFB nel task SAFE, sono visibili solo le variabili create nell'area sicura. Le variabili create nell'area di processo non sono visibili.
- Quando si configura un EF o EFB in un task non sicuro (MAST, FAST, AUX0 o AUX1), sono visibili solo le variabili create nell'area di processo. Le variabili create nell'area sicura non sono visibili.

Per consentire la comunicazione tra l'area sicura e l'area di processo, Control Expert fornisce anche un'area *globale*. L'area globale consente il passaggio nelle trasmissioni dati tra l'area sicura e l'area di processo. Per fare questo si dichiarano le variabili di interfaccia sia nell'area sicura che nell'area di processo, quindi si collegano queste variabili di interfaccia alle variabili di mappatura dichiarate nell'area globale.

Questa separazione dei dati nella CPU di sicurezza e nel coprocessore M580 è descritta graficamente di seguito:



Proprietà delle aree sicura, di processo e globale

Le tre aree dati di un progetto di sicurezza M580 presentano le proprietà seguenti:

Area	Tipi di variabili supportati	Ambito	Accesso esterno
Globale	Solo variabili non identificate. NOTA: Le variabili identificate non possono essere usate per la mappatura in una variabile di interfaccia sicura o di processo.	Può accedere a: <ul style="list-style-type: none"> • variabili di sicurezza, tramite indirizzamento dello spazio dei nomi, • variabili di processo, tramite indirizzamento dello spazio dei nomi, • altre variabili globali. 	Alle variabili di queste tre aree possono accedere le applicazioni HMI, SCADA o FactoryCast. (Vedere la nota sotto).
Sicura	Solo variabili non identificate.	Può accedere solo ad altre variabili di sicurezza.	
Di processo	Entrambe: <ul style="list-style-type: none"> • Variabili identificate • Variabili non identificate 	Può accedere solo ad altre variabili di processo.	

Quando un visualizzatore esterno cerca di leggere una variabile di processo, il formato di indirizzamento dipende dal fatto che sia selezionata o meno l'impostazione **Uso dello spazio dei nomi di processo** nell'area **Ambito > comune** della finestra **Strumenti > Impostazioni progetto....** Se l'impostazione **Uso dello spazio dei nomi di processo** è

- Selezionata: la schermata operatore può leggere le variabili dell'area di processo solo tramite il formato "PROCESS.<nome variabile>".
- Deselezionata: la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato "<nome variabile>" senza il prefisso PROCESS. In questo caso, verificare che il nome di ogni variabile di processo sia univoco e che non coincida con il nome di una variabile globale.

NOTA: Se l'impostazione **Uso dello spazio dei nomi di processo** è deselezionata, verificare che il nome di ogni variabile di processo sia univoco e che non coincida con il nome di una variabile globale. Se un nome di variabile è comune alle aree globale e di processo, Control Expert rileverà un errore quando si compila il progetto.

Come trasferire i dati tra le aree dello spazio dei nomi

Introduzione

Il PAC di sicurezza M580 dispone di tre diversi editor di dati:

- Un **Editor dati di sicurezza**, che permette di gestire i dati utilizzati nello spazio dei nomi di sicurezza.
- Un **Editor dati di processo**, che permette di gestire i dati utilizzati nello spazio dei nomi di processo.
- Un **Editor dati globali**, che permette di gestire le variabili globali e i tipi di dati utilizzati nell'applicazione.

Sia l'**Editor dati di sicurezza** che l'**Editor dati di processo** dispongono di una scheda **Interfaccia**. Nella scheda **Interfaccia** si possono creare variabili non identificate nello spazio dei nomi di processo specifico. La scheda **Interfaccia** presenta due gruppi di variabili non identificate:

- <ingressi>: una variabile creata in questo gruppo può essere collegata a una variabile e ricevere dati da una variabile pass-through valida a livello globale dell'**Editor dati globali** e ricevere dati da essa.
- <uscite>: una variabile di questo gruppo può essere collegata a una variabile pass-through valida a livello globale dell'**Editor dati globali** e inviarle dati.

NOTA: Una variabile creata nella scheda **Interfaccia** deve soddisfare le tre condizioni seguenti:

- Deve essere una variabile di categoria EDT o DDT.
- Deve essere una variabile dello stesso tipo della variabile alla quale è collegata.
- Non deve essere una variabile collegata a un bit estratto di una variabile identificata (ad esempio, non %MW10.1).

Le variabili non identificate create nel gruppo di schede **Interfaccia** dell'**Editor dati di sicurezza** e dell'**Editor dati di processo** possono essere collegate nel seguente modo:

Una variabile di processo di questo gruppo dell'Editor dati di processo...	può essere collegata a una variabile di sicurezza di questo gruppo dell'Editor dati di sicurezza...
<ingressi>	<uscite>
<uscite>	<ingressi>

Mediante questi tre editor dati, è possibile configurare il trasferimento di dati tra lo spazio dei nomi sicuro e lo spazio dei nomi di processo.

Trasferimento dei dati tra gli spazi dei nomi

Il processo per il passaggio dei dati dallo spazio dei nomi sicuro a quello di processo e dallo spazio dei nomi di processo a quello sicuro è l'immagine mirror di ciascuno. L'esempio seguente mostra come passare i dati dal processo all'area sicura:

Passo	Azione
1	Aprire l' Editor dati di processo , fare clic sulla scheda di programma Interfaccia e creare una nuova variabile nella parte <uscite> dell'editor dati.
2	Aprire l' Editor dei dati di sicurezza , fare clic sulla scheda di programma Interfaccia e creare una nuova variabile con lo stesso tipo di quella creata al passo 1 nella parte <ingressi> dell'editor dati. Fare quindi doppio clic sul campo Parametro effettivo . Viene visualizzata la finestra di dialogo Editor ambito dati: selezione variabili .
3	Nel menu a discesa in alto a destra nella finestra di dialogo, selezionare lo spazio dei nomi di destinazione PROCESS . Vengono visualizzate le variabili nello spazio dei nomi di PROCESSO selezionato nella parte <uscite> .
4	Selezionare la variabile di processo creata al passo 1 da collegare alla variabile di sicurezza creata al passo 2, quindi fare clic su OK . La variabile di destinazione selezionata compare nel campo Parametro effettivo .
5	Salvare le modifiche.

Dopo avere compilato, scaricato ed eseguito il programma applicativo modificato, il valore viene trasferito nel seguente modo:

- I dati della scheda **Interfaccia** creati in **<uscite>** sono pubblicati alla fine dell'esecuzione del task corrispondente.
- I dati della scheda **Interfaccia** creati in **<ingressi>** sono sottoscritti all'inizio dell'esecuzione del task corrispondente.

Comunicazioni del sistema di sicurezza M580

Contenuto del capitolo

Sincronizzazione dell'ora	177
Comunicazioni peer-to-peer.....	183
Comunicazione tra la CPU M580 e gli I/O di sicurezza	213

Introduzione

Questo capitolo descrive le comunicazioni interne al sistema di sicurezza M580.

Sincronizzazione dell'ora

Introduzione

Per PAC con firmware della CPU 3.10 o precedente:	La configurazione del servizio NTP è richiesta per consentire una comunicazione sicura. L'ora di mittenti e ricevitori deve essere sincronizzata con i servizi NTP.
Per PAC con firmware della CPU 3.20 o successivo:	<p>La sincronizzazione dell'ora sicura si basa su orologio interno e "monotonico". La comunicazione sicura non richiede la sincronizzazione dell'ora NTP:</p> <ul style="list-style-type: none"> • La CPU di sicurezza condivide l'ora sicura con tutti gli IO locali e remoti. • Il modulo di comunicazione di testa di IO remoto BM•CRA31210 richiede un firmware 2.60 o successivo. • Per una comunicazione peer to peer, le CPU condividono l'ora di sicurezza.

Configurazione della sincronizzazione dell'ora con firmware della CPU 3.10 o precedente

Introduzione

Se si installano moduli di I/O di sicurezza in una derivazione RIO, occorre configurare l'ora corrente per il PAC. Ciò è possibile in tre configurazioni con firmware della CPU 3.10 o precedente:

1. **Progettazione del server NTP remoto con la CPU come client NTP:** configurare un dispositivo nella rete di controllo come server NTP, quindi configurare la CPU di sicurezza come client NTP.
2. **Progettazione del server NTP locale:** configurare la CPU di sicurezza come server NTP per i dispositivi sulla rete RIO Ethernet.
3. **Progettazione del server NTP remoto con eNOC o eNOP:** configurare un dispositivo nella rete di controllo come server NTP, quindi configurare un modulo, moduli di comunicazione BMENOP0300 o BMENOC0301/11, nel rack principale locale e attivare la funzionalità opzionale **Aggiornamento ora della CPU > Aggiorna l'ora della CPU con questo modulo** nel DTM corrispondente. Se la derivazione RIO è stata configurata con dispositivi di sicurezza, è necessario configurare la CPU di sicurezza come server NTP, come descritto nel precedente caso 2.

Per ogni progettazione è necessario inoltre:

- Abilitare il servizio NTP.
- Impostare il periodo di interrogazione NTP a 20 s.

Se la CPU di sicurezza non è configurata come server NTP o client NTP, come descritto in precedenza, le impostazioni dell'ora di CPU e moduli di I/O di sicurezza remoti non saranno sincronizzate e la comunicazione sul black channel non funzionerà correttamente. Ingressi e uscite dei moduli di I/O di sicurezza nelle derivazioni RIO entrano nello stato di sicurezza (non alimentato) o di posizionamento di sicurezza.

▲ ATTENZIONE

RISCHIO DI FUNZIONAMENTO IMPREVISTO

Se si installano moduli di I/O di sicurezza in una derivazione RIO, occorre configurare l'ora corrente per il PAC con il firmware 3.10 o precedente. Attivare il servizio NTP per il sistema M580, quindi configurare la CPU di sicurezza come server NTP o client NTP.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Schneider Electric consiglia di configurare due sorgenti NTP, configurabili in modo ridondante, con una impostata come primaria e la seconda come server dell'ora di standby. Entrambi i server, tuttavia, devono essere sincronizzati in base all'ora. Qualsiasi regolazione dell'ora uguale o superiore a 2 s in un periodo di interrogazione NTP provoca la desincronizzazione della CPU e dei moduli IO di sicurezza e la deviazione dal server dell'ora NTP.

Modifica dell'impostazione dell'ora NTP durante il funzionamento

▲ ATTENZIONE

RISCHIO DI DISINSERZIONE DEL SISTEMA DI SICUREZZA

L'utilizzo di Control Expert V13 o V13.1 o del firmware 2.70 o precedente della CPU non determina modifiche dell'impostazione dell'ora nel server NTP o nella CPU.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

La modifica dell'ora durante il funzionamento può provocare interruzione della comunicazione e una disinserzione del sistema di sicurezza.

La modifica dell'ora durante il funzionamento può provocare una desincronizzazione con l'orologio di riferimento. Si potrebbe inoltre attivare un'interruzione della comunicazione di sicurezza provocando l'ingresso degli I/O nello stato di sicurezza o di posizionamento di sicurezza. Monitorare il sistema al fine di individuare un'eventuale desincronizzazione e nel caso si verifichi, ripristinare la sincronizzazione per evitare l'interruzione della comunicazione. Se si verifica tale desincronizzazione, utilizzare la procedura seguente, pagina 179 per risincronizzare il sistema.

Se si utilizza Control Expert V14 o versioni successive e il firmware della CPU 2.80, 2.90 o 3.10: è possibile modificare l'impostazione dell'ora nel server NTP o nella CPU durante il funzionamento senza un impatto negativo. Eseguire questa operazione seguendo la procedura indicata di seguito subito dopo una modifica dell'ora.

Vedere la sezione *Scheda NTP in Modicon M580 - Manuale di riferimento hardware* per informazioni su come configurare il servizio NTP per una CPU M580.

Procedura per sincronizzare le impostazioni dell'ora NTP

Quando l'alimentazione viene trasmessa alla CPU o la CPU subisce un reset, e inizialmente riceveva un'impostazione di tempo da un server NTP esterno, utilizzare la procedura seguente per sincronizzare l'ora della CPU.

ATTENZIONE

RISCHIO DI APPARECCHIATURA NON FUNZIONANTE

Utilizzando la funzionalità **Aggiorna ora della CPU**, opzionale per i moduli BMENOP0300 o BMENOC0301/11 per eseguire l'aggiornamento dell'ora del PAC, dal momento in cui il server NTP esterno diventa operativo (quando %SW152 passa da 0 a 1), sincronizzare l'Ora sicura con un server NTP esterno utilizzando %SW128. Seguire la procedura per la sincronizzazione dell'impostazione dell'ora NTP indicata più avanti.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

La procedura seguente è valida con il task SAFE in stato RUN, con Control Expert V14.0 o versioni successive e firmware della CPU 2.80, 2.90 o 3.10:

Pas-saggio	Azione
1	Verificare che l'ora della CPU o del server NTP sia valida, corretta e stabile.
2	Se la configurazione comprende una o più derivazioni eRIO, dopo la riattivazione del servizio NTP o dopo la modifica dell'ora (che ha portato alla desincronizzazione), attendere per 2 periodi di interrogazione NTP per consentire l'invio del nuovo valore dell'ora di riferimento a tutti i moduli CRA.
3	Sincronizzare l'ora di sistema in base all'orologio di riferimento tramite la parola di sistema %SW128: <ul style="list-style-type: none"> • impostare %SW128 a 16#1AE5 per almeno 500 ms, • impostare quindi %SW128 a #E51A per almeno 500 ms.
4	Controllare che l'ora sia sincronizzata, verificando che i valori del parametro per CPU_NTP_SYNC e M_NTP_SYNC nello IODDDT di sicurezza siano veri (1)

Ripetere questa sequenza di sincronizzazione nel caso in cui non venga eseguita correttamente.

AVVISO

RISCHIO DI SPEGNIMENTO DI SICUREZZA DEL SISTEMA

- Se si utilizza Control Expert V14.0 o versioni successive e firmware della CPU 2.80 o versioni successive per eseguire una modifica dell'ora del PAC, sarà necessario far seguire a tale modifica la procedura di sincronizzazione descritta in precedenza.
- Se non si esegue una procedura di sincronizzazione, gli I/O di sicurezza possono passare allo stato di sicurezza o di posizionamento di sicurezza dopo la deviazione dell'orologio per circa un timeout di ritardo di comunicazione.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

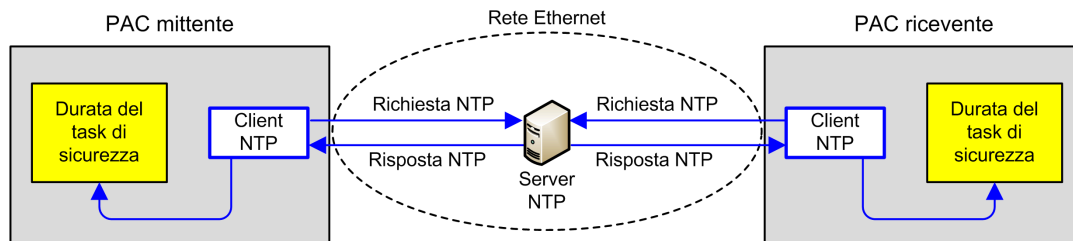
Durante le operazioni di sincronizzazione dell'ora del passo 3, alcune diagnostiche della comunicazione di sicurezza sono disattivate per una durata di 500 ms. Schneider Electric consiglia un massimo di una modifica e sincronizzazione dell'ora al giorno.

Servizio NTP per comunicazione peer-to-peer

La comunicazione PAC-PAC Ethernet sicura richiede la sincronizzazione della base tempo sia del PAC mittente che del PAC ricevente.

NOTA: Schneider Electric consiglia di configurare in ogni PAC nel ruolo di client NTP la CPU di sicurezza, un modulo di comunicazione BMENOP0300 o BMENOC0301/11, un client NTP e di configurare un altro dispositivo di rete come server NTP.

La figura seguente descrive il principio di sincronizzazione della base tempo dei PAC mittente e ricevente:



In Control Expert, configurare i parametri del servizio NTP per ogni client nel seguente modo:

- Selezionare **Client NTP**.
- Impostare l'**Indirizzo IP del server NTP primario** con l'indirizzo IP del server NTP remoto.
- Schneider Electric consiglia di impostare il valore del **Periodo di interrogazione** a 20 secondi.

Coerenza temporale e bit di sistema del server NTP

Coerenza temporale del server NTP:

- Se l'ora del server NTP corrisponde all'ora PC interna visualizzata dall'EF `S_SYST_CLOCK` con meno di 2 secondi di differenza, il valore temporale nell'EF `S_SYST_CLOCK` viene aggiornato con l'ultima ora del server NTP ricevuta, filtrata con una pendenza di 1ms/s.
- Se l'ora del server NTP ricevuta differisce dall'ora PC interna visualizzata dall'EF `S_SYST_CLOCK` di più di 2 secondi:
 - l'ultima ora del server NTP ricevuta viene ignorata dal PAC,
 - il valore temporale visualizzato dall'EF `S_SYST_CLOCK` viene aggiornato internamente,
 - il parametro `status` di `S_SYST_CLOCK` viene impostato a 0 e
 - il parametro di uscita `SYNCHRO_NTP` di `S_RD_ETH_MX` e il DFB `S_WR_ETH_MX` viene impostato a 0 per indicare questa condizione.

In questo caso si può resettare l'ora PC interna effettuando una delle operazioni seguenti:

- reinizializzare l'applicazione con un riavvio a freddo
- scaricare l'applicazione
- riavviare il PAC
- seguire la procedura per la modifica delle impostazioni dell'ora NTP, pagina 179.

NOTA: Se si perde la sincronizzazione NTP su uno dei due PAC (parametro `SYNCHRO_NTP` impostato a 0), la base tempo dei PAC mittente e ricevente può essere desincronizzata. In questo caso la comunicazione peer-to-peer sicura può cessare di essere operativa (il parametro di uscita `health` del DFB `S_RD_ETH_MX` viene impostato a 0).

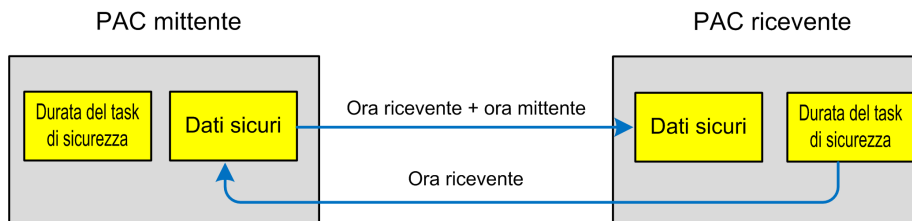
Sincronizzazione dell'ora per firmware della CPU 3.20 o successivo

Sincronizzazione dell'ora per comunicazione peer-to-peer

NOTA: Con firmware della CPU 3.20 o successivo, il servizio NTP non viene utilizzato per la sincronizzazione dell'ora.

La comunicazione sicura Ethernet PAC-to-PAC richiede che i PAC mittente e ricevente condividano un'ora sicura comune.

La figura seguente descrive il principio di condivisione dell'ora dei PAC mittente e ricevente:



In Control Expert, configurare:

- una comunicazione Da mittente a ricevente per trasmissione dati
- una comunicazione Da ricevente a mittente per trasmissione ora sicura

Coerenza dell'ora

Un'ora interna di sicurezza (indipendente da NTP) viene distribuita dalla CPU ai propri moduli IO di sicurezza locali e remoti.

Comunicazioni peer-to-peer

Introduzione

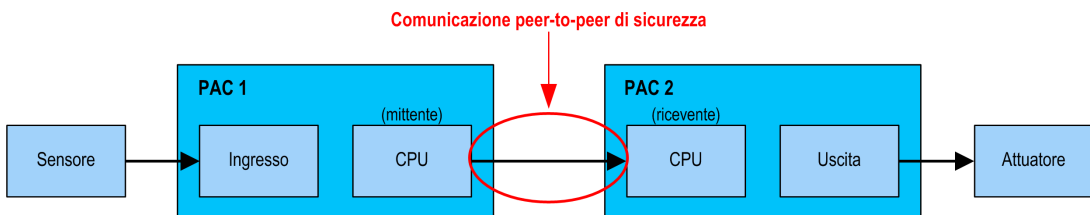
Questa sezione descrive le comunicazioni peer-to-peer tra i PAC di sicurezza M580.

Comunicazione peer-to-peer

Introduzione

È possibile configurare due PAC di sicurezza M580 in modo che eseguano comunicazioni peer-to-peer sicure tramite Ethernet. La configurazione è basata sulla comunicazione dello scanner Modbus TCP, integrato in un black channel.

Questo è lo schema funzionale della comunicazione peer-to-peer sicura:



La comunicazione viene effettuata da due blocchi di funzioni elementari della libreria dei blocchi di sicurezza M580 che gestiscono il loop di sicurezza a un livello SIL3. Il protocollo rileva gli errori di trasmissione, tra cui omissioni, inserimenti, sequenza errata, ritardi, indirizzamento impreciso e bit mascherati, e gestisce le ritrasmissioni.

Questa comunicazione peer-to-peer sicura è possibile solo tra:

- due PAC M580 Safety entrambi con firmware della CPU 3.10 o precedente,
- due PAC M580 Safety entrambi con firmware della CPU 3.20 o successivo,

NOTA: la comunicazione peer-to-peer sicura è inoltre possibile tra un PLC Modicon Quantum Safety e un PLC M580 Safety con firmware della CPU 3.10 o precedente.

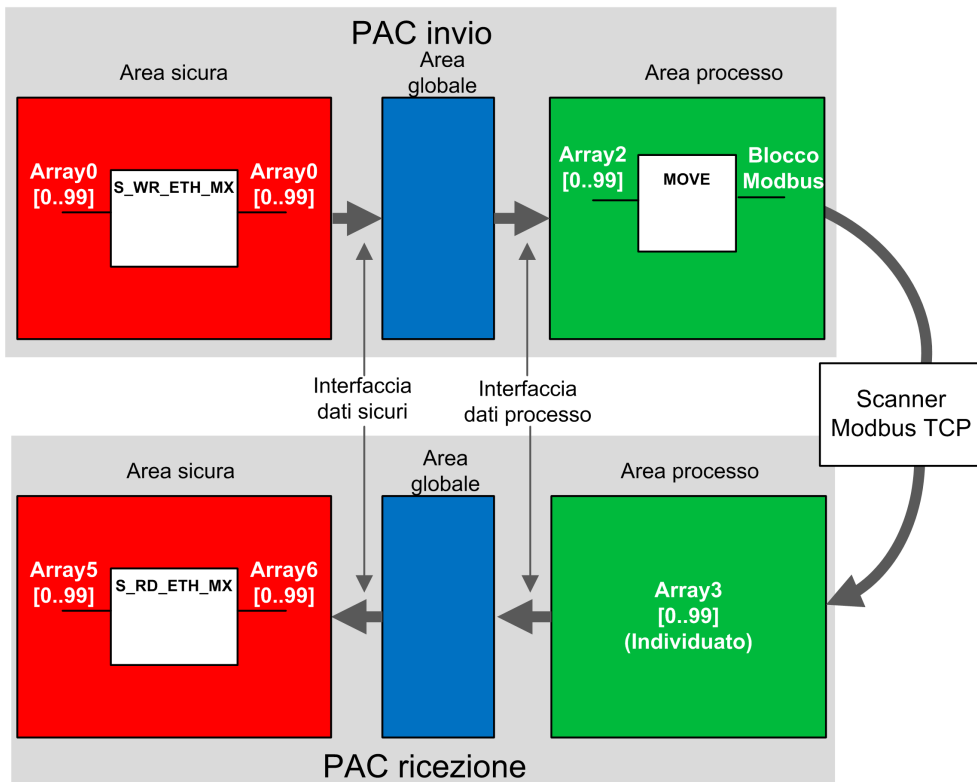
Architettura peer-to-peer con firmware della CPU 3.10 o precedente

Progettazione dell'architettura

Con firmware della CPU 3.10 o precedente, l'architettura della soluzione è basata su:

- Servizio NTP per la sincronizzazione della base tempo.
- Esecuzione di 2 DFB (S_WR_ETH_MX e MOVE nel PAC mittente e 1 DFB (S_RD_ETH_MX) nel PAC ricevente).
- Scanning tramite Modbus TCP per il trasferimento dei dati.

La seguente figura mostra una panoramica del processo richiesto per eseguire la comunicazione peer-to-peer:

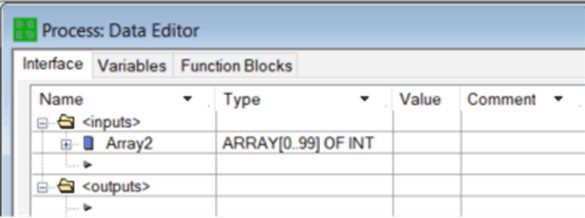
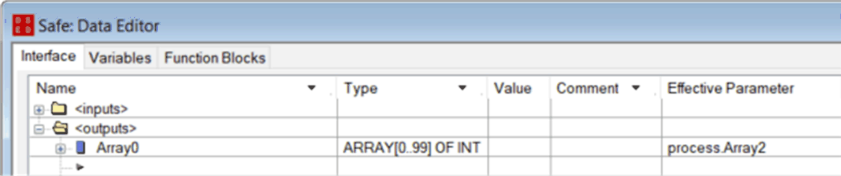


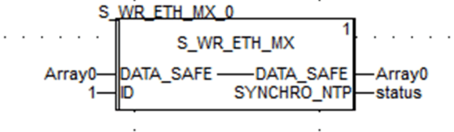
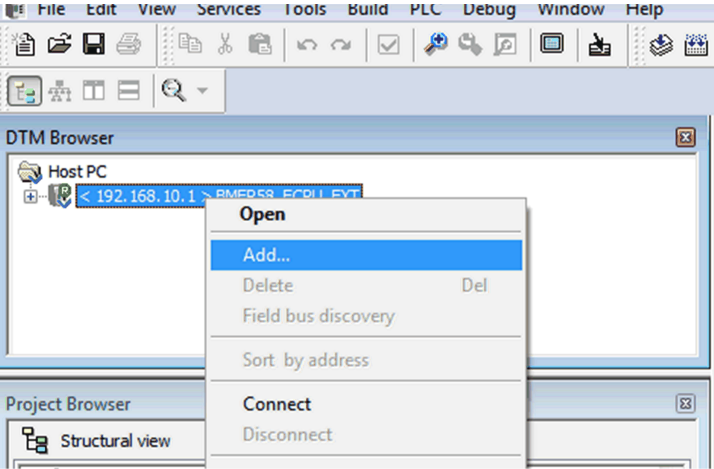
Nella figura precedente, Control Expert crea automaticamente, e nasconde dalla vista esterna, l'Array 1 e l'Array 4 nelle aree Globali dei PAC peer. Da un punto di vista utente, i collegamenti sono effettuati da Array 0 ad Array 2 e da Array 3 ad Array 5.

NOTA: Sulla rete Ethernet, si possono mischiare dati di sicurezza e dati non di sicurezza senza alcun impatto sul livello di integrità dei dati di sicurezza. Non vi sono restrizioni sulla rete Ethernet quando si utilizza la comunicazione peer-to-peer sicura.

Dettagli della configurazione del trasferimento dati Peer-to-Peer

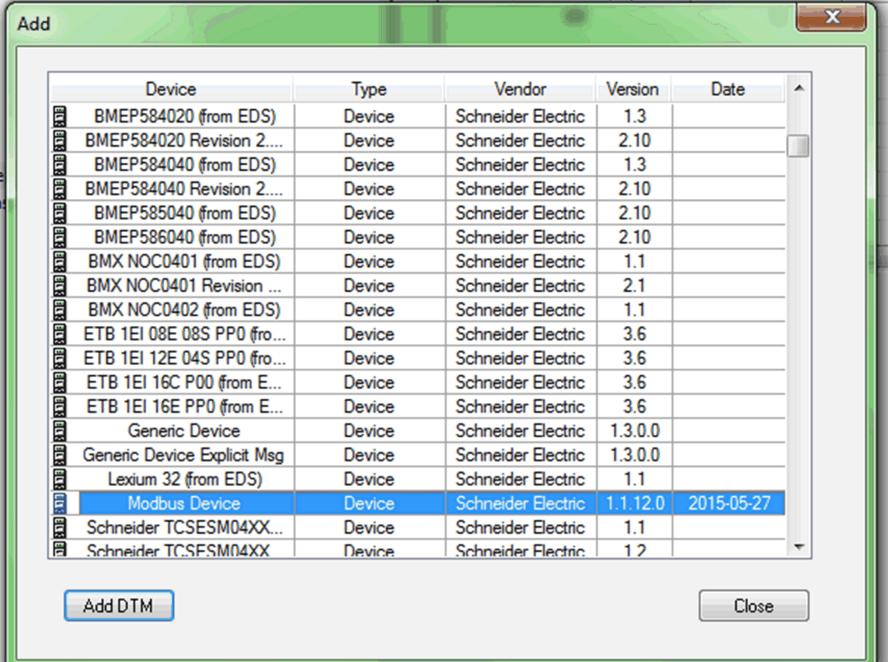
L'esempio che segue mostra come configurare un trasferimento di dati peer-to-peer tra due PAC di sicurezza con firmware della CPU 3.10 o precedente e Control Expert 14.1 o precedente:

Pas- so	Azione
1	<p>Sul PAC mittente, utilizzare l'Editor dati di processo per creare un array di 100 interi come ingresso nell'area Interfaccia. In questo esempio, il nome dell'array è Array2:</p> 
2	<p>Sul PAC mittente, creare un altro array di 100 interi come uscita nella scheda Interfaccia dell'Editor dati di sicurezza e collegarlo all'array dell'area di processo di ingresso creato al passo 1, sopra, nella colonna Parametro effettivo. In questo esempio, il nome dell'array è Array0:</p>  <p>NOTA: Le variabili di interi dall'indice 0 a 90 dell'array contengono i valori delle variabili di sicurezza da scambiare con il PAC ricevente. L'area rimanente è riservata per i dati di diagnostica autogenerati, incluso un CRC e un time stamp. Questi dati di diagnostica vengono utilizzati dal PAC ricevente per determinare se i dati trasferiti sono sicuri.</p>

Pas- so	Azione
3	<p>Sul PAC mittente, configurare il DFB S_WR_ETH_MX in una sezione dei task SAFE. Collegare il DFB ad Array0:</p> 
4	<p>Nel Browser DTM nel PAC mittente, selezionare la CPU (in questo esempio) o a un modulo di comunicazione NOC (se presente), quindi fare clic su Aggiungi... per creare uno scanner Modbus che può inviare i dati tramite Modbus TCP dal PAC mittente al PAC ricevente:</p> 

Pas-so **Azione**

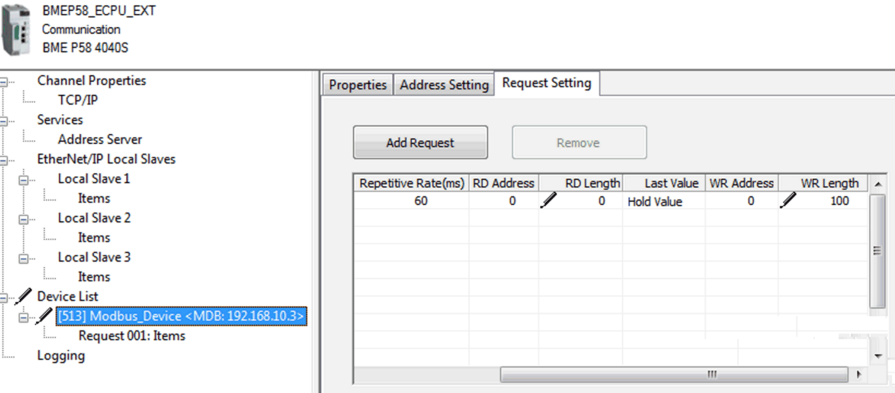
5 Selezionare **Dispositivo Modbus** e fare clic **Aggiungi DTM** per aggiungere lo scanner Modbus:



Device	Type	Vendor	Version	Date
BMEP584020 (from EDS)	Device	Schneider Electric	1.3	
BMEP584020 Revision 2...	Device	Schneider Electric	2.10	
BMEP584040 (from EDS)	Device	Schneider Electric	1.3	
BMEP584040 Revision 2...	Device	Schneider Electric	2.10	
BMEP585040 (from EDS)	Device	Schneider Electric	2.10	
BMEP586040 (from EDS)	Device	Schneider Electric	2.10	
BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1	
BMX NOC0401 Revision ...	Device	Schneider Electric	2.1	
BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1	
ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6	
ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6	
ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6	
ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6	
Generic Device	Device	Schneider Electric	1.3.0.0	
Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0	
Lexium 32 (from EDS)	Device	Schneider Electric	1.1	
Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27
Schneider TCSESM04XX...	Device	Schneider Electric	1.1	
Schneider TC.SFSM04XX	Device	Schneider Electric	1.2	

6 Aprire il dispositivo Modbus appena aggiunto, aggiungere una richiesta e nella scheda **Impostazione richiesta**:

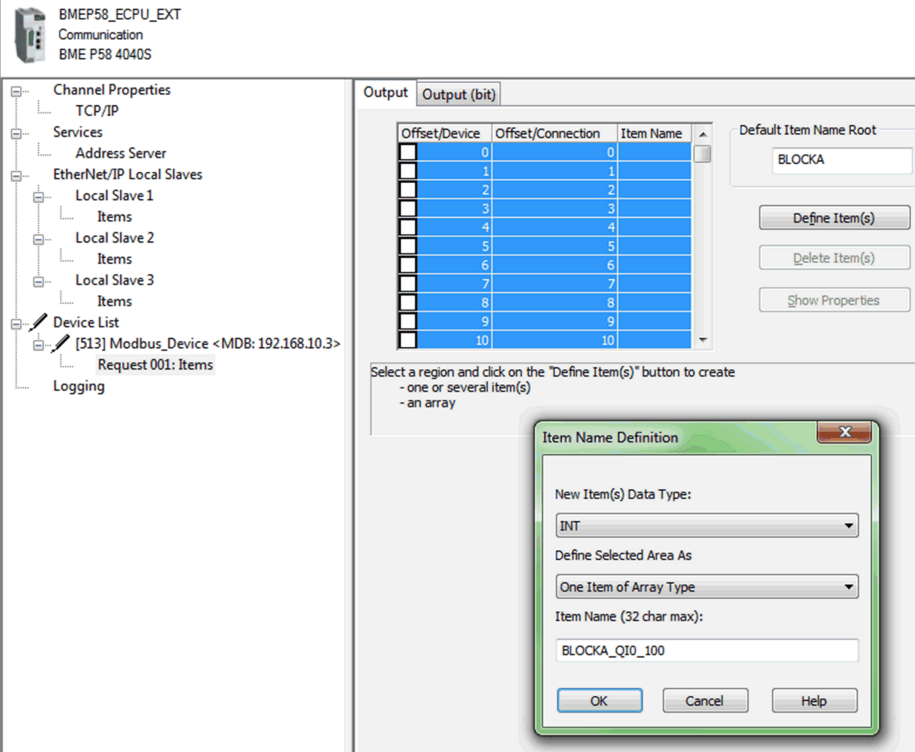
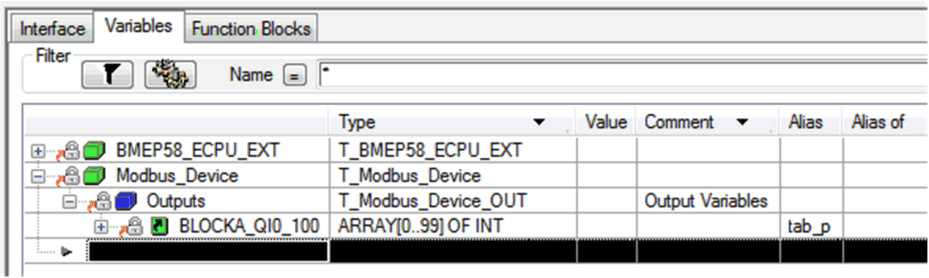
- Impostare la colonna **Lunghezza WR**, ossia la lunghezza dei dati da scrivere, al valore 100, quindi
- Impostare la colonna **Indirizzo WR**, che è l'indirizzo in cui la tabella del PAC ricevente scriverà i dati che riceve (in questo esempio: 0, ossia il PAC mittente scriverà nella tabella a partire da %MWO nel PAC ricevente).

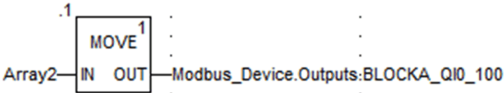
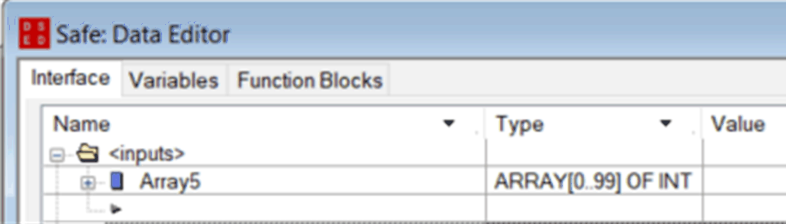
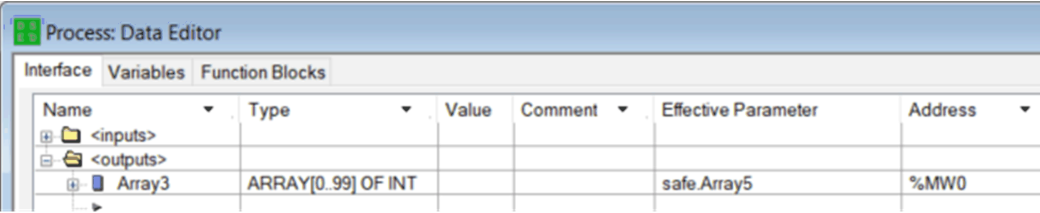


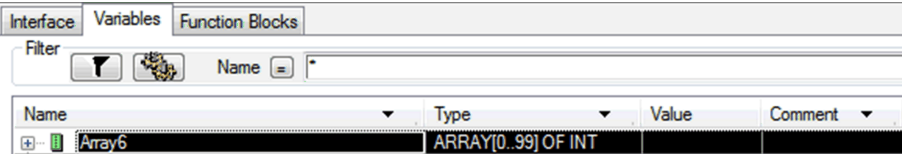
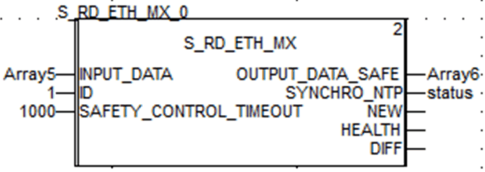
Channel Properties

- TCP/IP
- Services
 - Address Server
 - EtherNet/IP Local Slaves
 - Local Slave 1
 - Items
 - Local Slave 2
 - Items
 - Local Slave 3
 - Items
 - Device List
 - [513] Modbus_Device <MDB: 192.168.10.3>
 - Request 001: Items
 - Logging

Repetitive Rate(ms)	RD Address	RD Length	Last Value	WR Address	WR Length
60	0	0	Hold Value	0	100

Pas- so	Azione																																							
7	<p>Selezionare il nodo Request 001: Items, quindi nella scheda Uscita definire un tipo di array di INT (ossia ≥ 100 interi). Questa è la tabella del PAC mittente che verrà scritta nel PAC ricevente:</p> 																																							
8	<p>Dopo aver salvato e compilato la configurazione, il blocco (BLOCKA_QI0_100 in questo esempio) viene creato automaticamente come variabile di processo:</p>  <table border="1" data-bbox="194 1161 1122 1437"> <thead> <tr> <th>Interface</th> <th>Variables</th> <th>Function Blocks</th> </tr> </thead> <tbody> <tr> <td colspan="3">Filter</td> </tr> <tr> <td></td> <td>Name</td> <td>*</td> </tr> <tr> <th></th> <th>Type</th> <th>Value</th> <th>Comment</th> <th>Alias</th> <th>Alias of</th> </tr> <tr> <td>BMEP58_ECPU_EXT</td> <td>T_BMEP58_ECPU_EXT</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Modbus_Device</td> <td>T_Modbus_Device</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Outputs</td> <td>T_Modbus_Device_OUT</td> <td></td> <td>Output Variables</td> <td></td> <td></td> </tr> <tr> <td>BLOCKA_QI0_100</td> <td>ARRAY[0..99] OF INT</td> <td></td> <td></td> <td>tab_p</td> <td></td> </tr> </tbody> </table>	Interface	Variables	Function Blocks	Filter				Name	*		Type	Value	Comment	Alias	Alias of	BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT					Modbus_Device	T_Modbus_Device					Outputs	T_Modbus_Device_OUT		Output Variables			BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p	
Interface	Variables	Function Blocks																																						
Filter																																								
	Name	*																																						
	Type	Value	Comment	Alias	Alias of																																			
BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT																																							
Modbus_Device	T_Modbus_Device																																							
Outputs	T_Modbus_Device_OUT		Output Variables																																					
BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p																																				

Pas- so	Azione
9	<p>Sul PAC mittente, in una sezione del codice di processo, usare un DFB <code>MOVE</code> per copiare il contenuto di <code>Array2</code> nell'array definito sopra nella struttura del dispositivo Modbus:</p> 
10	<p>Sul PAC ricevente, utilizzare l'Editor dati di sicurezza per creare un array di 100 interi (<code>Array5</code>) come ingresso nell'area Interfaccia:</p> 
11	<p>Sul PAC ricevente, nell'Editor dati di processo, creare un array (<code>Array3</code>) di 100 INT nella sezione <code><uscite></code> della scheda Interfaccia. Collegare questo array all'array dell'area dati (<code>Array5</code>, creato al passo 10) nella colonna Parametro effettivo. I dati inviati dal PAC mittente verranno scritti in questo array tramite lo scanner Modbus, a condizione che questa variabile sia localizzata all'indirizzo definito nello scanner del PAC mittente (in questo esempio <code>%MW0</code>):</p> 

Pas- so	Azione
12	<p>Sul PAC ricevente, utilizzare l'Editor dati di sicurezza per creare un array di 100 interi (Array6):</p>  <p>The screenshot shows a software interface with tabs for 'Interface', 'Variables', and 'Function Blocks'. Below the tabs is a 'Filter' section with a funnel icon and a 'Name' field. A table below lists variables, with 'Array6' highlighted in the first row. The table has columns for 'Name', 'Type', 'Value', and 'Comment'. The 'Type' for 'Array6' is 'ARRAY[0..99] OF INT'.</p>
13	<p>Nel PAC ricevente, in una sezione di codice nel task SAFE, creare un'istanza del DFB S_RD_ETH_MX con l'array creato al passo 10 (Array5) quale parametro di ingresso e con l'array creato al passo 12 (Array6) quale parametro di uscita:</p>  <p>The diagram shows a block labeled 'S_RD_ETH_MX' with a '2' in the top right corner. It has several inputs and outputs: <ul style="list-style-type: none"> Input: 'Array5' connected to 'INPUT_DATA'. Input: '1' connected to 'ID'. Input: '1000' connected to 'SAFETY_CONTROL_TIMEOUT'. Output: 'Array6' connected to 'OUTPUT_DATA_SAFE'. Output: 'status' connected to 'SYNCHRO_NTP'. Output: 'NEW'. Output: 'HEALTH'. Output: 'DIFF'. </p>

Black channel peer-to-peer

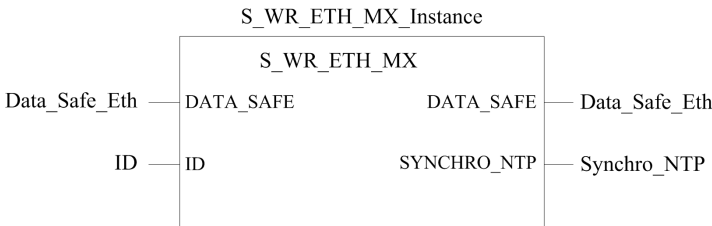
Ogni trasmissione dati peer-to-peer è costituita da *Dati di sicurezza utente*, che trasmettono il contenuto legato all'applicazione, e *Dati riservati*. I *Dati riservati* servono al PAC di sicurezza per testare l'affidabilità della trasmissione, che deve soddisfare i requisiti SIL3. I *Dati riservati* sono formati dai seguenti elementi:

- Un CRC calcolato dal PAC mittente a partire dai dati che devono essere trasmessi. Il PAC ricevente verifica il CRC prima di usare i dati trasmessi.
- Un identificativo di comunicazione, che è incluso nel calcolo del CRC per evitare bit mascherati e cyberattacchi sulla trasmissione dei dati di sicurezza.
- Un'indicazione oraria contenente la durata della trasmissione in ms. Questa indicazione oraria è basata sul valore orario fornito dal servizio NTP e permette di sincronizzare sia il PAC mittente che il PAC ricevente. Il PAC mittente aggiunge un valore temporale ai dati inviati al PAC ricevente. Il PAC ricevente confronta l'indicazione oraria con il proprio valore orario e la usa per:
 - Verificare l'età dei dati.
 - Rifiutare trasmissioni doppie.
 - determinare l'ordine cronologico delle trasmissioni ricevute
 - determinare il tempo trascorso tra le notifiche di ricezione delle trasmissioni dati.

Configurazione del DFB S_WR_ETH_MX nella logica di programma del PAC mittente

Rappresentazione

Rappresentazione del DFB:



Per una descrizione estesa di questo DFB, consultare *EcoStruxure™ Control Expert, Safety, Block Library*.

Descrizione

Il DFB S_WR_ETH_MX è per PAC con firmware della CPU 3.10 o precedente. Calcola i dati (dati riservati contenenti un CRC e un timestamp) richiesti dal ricevitore per controllare e gestire gli errori rilevati durante la comunicazione peer-to-peer.

Il blocco funzione DFB S_WR_ETH_MX deve essere richiamato in ogni ciclo nel PAC mittente. Nell'ambito del ciclo, questo blocco deve essere eseguito nella logica dopo che sono state eseguite tutte le modifiche necessarie sui dati da inviare. Questo significa che i dati da inviare non possono essere modificati nel ciclo dopo l'esecuzione del DFB, altrimenti le informazioni CRC utilizzate nell'area dati riservati non saranno corrette e la comunicazione peer-to-peer sicura non potrà avere luogo.

È necessario assegnare al parametro ID un valore univoco che identifichi la comunicazione peer-to-peer sicura tra un mittente e un ricevente.

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Il valore del parametro ID deve essere univoco e fisso nella rete per una coppia mittente/ ricevente.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Descrizione dell'array `DATA_SAFE`

Utilizzare la scheda **Interfaccia** nell'**Editor dati di sicurezza** ed **Editor dati processo** in per creare il collegamento tra le variabili di processo e le variabili di sicurezza. Control Expert

Il collegamento di processo e variabili di sicurezza in questo modo è possibile per:

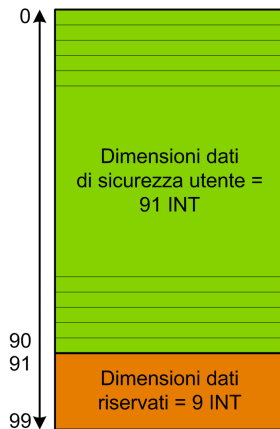
- Trasferire il valore delle variabili di sicurezza alle variabili di processo, tramite variabili globali collegate.
- Inviare valori variabili dall'area processo del PAC mittente all'area processo del PAC ricevente, tramite messaggistica esplicita su Modbus TCP.

L'array `DATA_SAFE` è composto da due aree:

- L'area **Dati sicurezza utente** contiene i dati dell'area di sicurezza del PAC. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Tali dati sono utilizzati dal PAC ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o meno. Quest'area inizia all'indice 91 e finisce all'indice 99.

NOTA: Non scrivere nell'area **Dati riservati**.

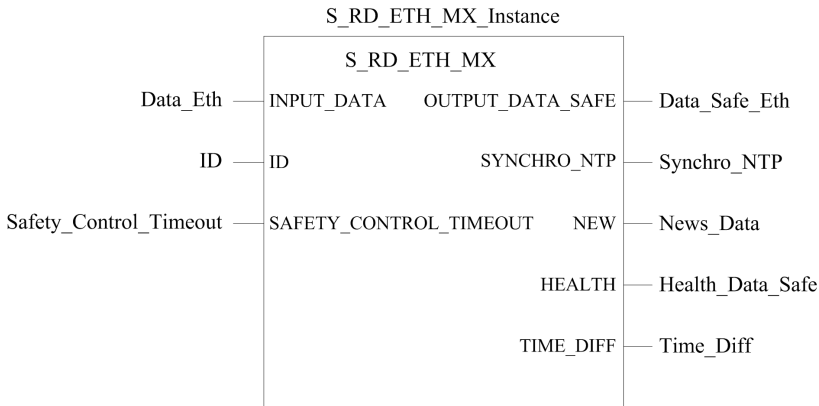
Rappresentazione della struttura dell'array `DATA_SAFE` (array[0..99] of INT):



Configurazione del DFB S_RD_ETH_MX nella logica di programma del PAC ricevente.

Rappresentazione

Rappresentazione del DFB:



Per una descrizione estesa di questo DFB, consultare *EcoStruxure™ Control Expert, Safety, Block Library*.

Descrizione

Il DFB S_RD_ETH_MX è per PAC con firmware della CPU 3.10 o precedente. Copia i dati ricevuti nell'area di processo sull'area di sicurezza e convalida la precisione dei dati ricevuti.

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Il blocco funzione DFB S_RD_ETH_MX deve essere richiamato a ogni ciclo nella logica di programma del PC ricevente e deve essere eseguito prima che i dati del ciclo vengano usati.
- Il valore del parametro ID deve essere univoco e fisso nella rete per una coppia mittente/ricevente.
- Occorre testare il valore del bit HEALTH del DFB S_RD_ETH_MX a ogni ciclo prima di usare dati sicuri per gestire la funzione di sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il blocco funzione `S_RD_ETH_MX`:

- copia i dati ricevuti nel registro `INPUT_DATA` al registro `OUTPUT_DATA_SAFE` se supera i seguenti test:
 - Il blocco funzione controlla il CRC dell'ultimo pacchetto dati ricevuto, tramite scanner degli I/O su Ethernet (Modbus TCP). Se CRC non è corretto, i dati vengono considerati non sicuri e non scritti sul registro `OUTPUT_DATA_SAFE` nell'area di sicurezza.
 - Il blocco funzione controlla gli ultimi dati ricevuti per determinare se sono più recenti di quelli già scritti nel registro `OUTPUT_DATA_SAFE` nell'area di sicurezza (confrontando i timestamp). Se gli ultimi dati ricevuti non sono più recenti, non vengono copiati nel registro `OUTPUT_DATA_SAFE` nell'area di sicurezza.
- Verifica l'età dei dati presenti nell'area di sicurezza. Se l'età è superiore a un valore massimo impostato nel registro d'ingresso `SAFETY_CONTROL_TIMEOUT`, i dati sono dichiarati non sicuri e il bit `HEALTH` è impostato a 0.

NOTA: L'età dei dati è data dalla differenza tra l'ora in cui i dati sono calcolati nel PAC di invio e l'ora in cui vengono verificati nel PAC di ricezione. Il riferimento in base tempo viene aggiornato periodicamente con l'ora ricevuta da un server NTP.

Se il bit `HEALTH` è impostato a 0, i dati disponibili nell'array `OUTPUT_DATA_SAFE` sono considerati non sicuri. In questo caso, prendere le appropriate misure.

Descrizione degli array `INPUT_DATA` e `OUTPUT_DATA_SAFE`

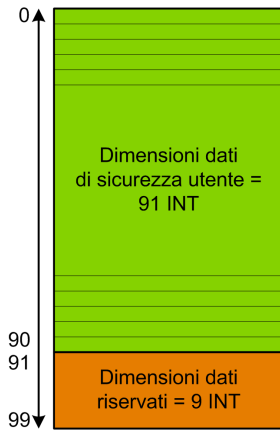
Gli array `INPUT_DATA` consistono di dati provenienti dall'area di memoria dati di processo. Gli array `OUTPUT_DATA_SAFE` consistono di variabili di sicurezza. Utilizzare le schede **Interfaccia dati di sicurezza** e **Interfaccia dati di processo** in per creare il collegamento tra le variabili di processo e le variabili di sicurezza. Control Expert

Gli array `INPUT_DATA` e `OUTPUT_DATA_SAFE` sono composti da 2 aree:

- L'area **Dati sicurezza utente** contiene i dati dell'utente. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Tali dati sono utilizzati dal PAC ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o meno. Quest'area inizia all'indice 91 e finisce all'indice 99.

NOTA: Si consiglia di non scrivere nell'area **Dati riservati**, in quanto si sovrascriverebbero i dati diagnostici generati automaticamente.

Rappresentazione della struttura degli array `INPUT_DATA` e `OUTPUT_DATA_SAFE` (array [0..99] of INT):



Calcolo di un valore `SAFETY_CONTROL_TIMEOUT`

Quando si calcola un valore `SAFETY_CONTROL_TIMEOUT`, considerare quanto segue:

- Valore minimo: $SAFETY_CONTROL_TIMEOUT > T1$
- Valore consigliato: $SAFETY_CONTROL_TIMEOUT > 2 * T1$

$T1 = \text{tempo ciclo MAST CPU}_{\text{mittente}} + \text{tempo ciclo SAFE CPU}_{\text{mittente}} + \text{Frequenza}_{\text{ripetizione}} + \text{Tempo trasmissione di rete} + \text{tempo ciclo MAST CPU}_{\text{ricevente}} + \text{tempo ciclo SAFE CPU}_{\text{ricevente}}$

Dove:

- *Tempo ciclo CPU_{mittente} MAST* è il tempo di ciclo MAST del PAC mittente.
- *Tempo ciclo CPU_{mittente} SAFE* è il tempo di ciclo SAFE del PAC mittente.
- *Frequenza_{ripetizione}* è la frequenza di tempo della query di scrittura dello scanner degli I/O dal PAC mittente al PAC ricevente.
- *Tempo trasmissione di rete* è il tempo impiegato sulla rete Ethernet per la trasmissione dei dati dal PAC mittente al PAC ricevente.
- *Tempo ciclo CPU_{ricevente} MAST* è il tempo di ciclo MAST del PAC ricevente.
- *Tempo ciclo CPU_{ricevente} SAFE* è il tempo di ciclo SAFE del PAC ricevente.

Tenere presente che il valore definito per il parametro `SAFETY_CONTROL_TIMEOUT` ha un effetto diretto sulla robustezza e disponibilità della comunicazione sicura peer-to-peer. Se il valore del parametro `SAFETY_CONTROL_TIMEOUT` supera di molto $T1$, la comunicazione tollera vari ritardi (ad esempio i ritardi di rete) o trasmissioni di dati danneggiati.

L'utente è responsabile per la configurazione della rete Ethernet in modo che il carico non provochi un ritardo eccessivo sulla rete durante la trasmissione dei dati, che provocherebbe la scadenza del timeout. Per consentire una comunicazione peer-to-peer sicura senza eccessivi ritardi dovuti ad altri dati non sicuri trasmessi sulla stessa rete, utilizzare una rete Ethernet dedicata per il protocollo peer-to-peer sicuro.

Quando si mette in servizio il progetto, occorre valutare le prestazioni della comunicazione sicura peer-to-peer verificando i valori forniti nel parametro di uscita `TIME_DIFF` e valutando il margine utilizzando il valore definito nel parametro `SAFETY_CONTROL_TIMEOUT`.

Note sul bit HEALTH

Quando il bit `HEALTH` è uguale a:

- 1: l'integrità dei dati è corretta (CRC) e l'età dei dati è inferiore al valore impostato nel registro di ingresso `SAFETY_CONTROL_TIMEOUT`.
NOTA: L'età dei dati considerati è il tempo tra:
 - l'inizio del ciclo dove i dati sono danneggiati nel PAC mittente.
 - l'inizio del ciclo dove i dati sono controllati nel PAC mittente.
- 0: i nuovi dati validi non sono ricevuti nell'intervallo di tempo richiesto (il timer scade e il bit `HEALTH` è impostato a 0).

NOTA: Se il bit `HEALTH` è impostato a 0, i dati nell'array di uscita `OUTPUT_DATA_SAFE` sono considerati non sicuri; rispondere in modo adeguato.

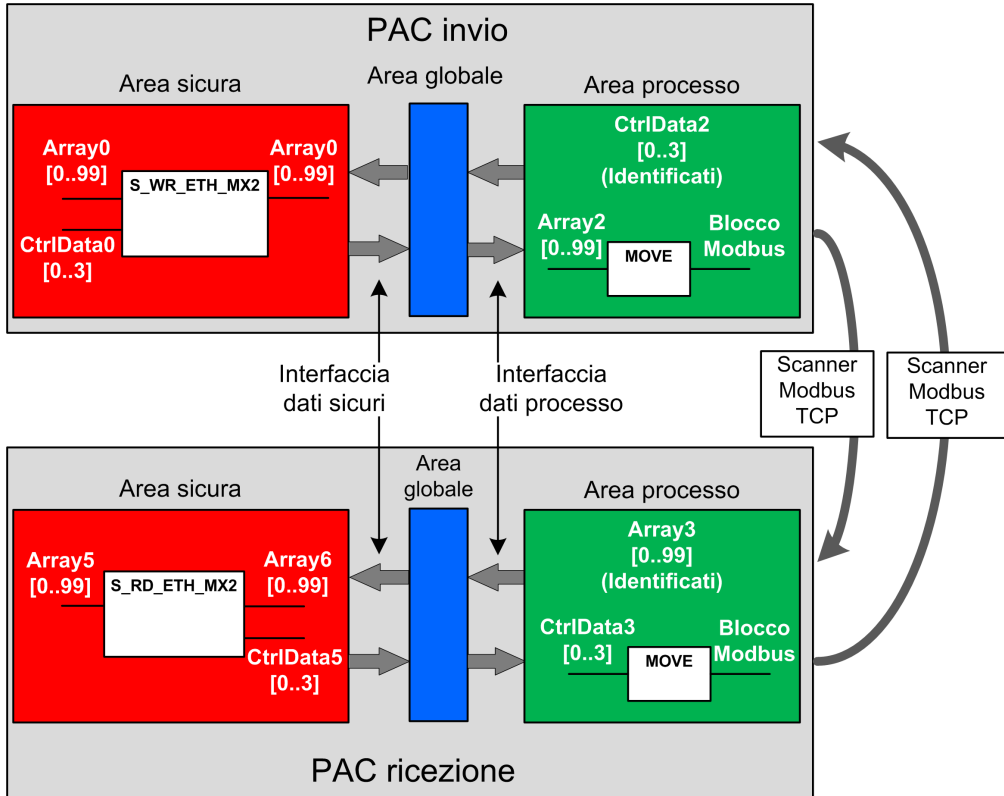
Architettura peer-to-peer con firmware della CPU 3.20 o successivo

Progettazione dell'architettura

Con firmware della CPU 3.20 o successivo, l'architettura della soluzione è basata su:

- Esecuzione di 2 DFB (`S_WR_ETH_MX2` e `MOVE` nel PAC mittente e 2 DFB (`S_RD_ETH_MX2` e `MOVE`) nel PAC ricevente.
- Scansione tramite Modbus TCP, per trasporto dati sicuro da mittente a ricevente.
- Scansione tramite Modbus TCP, per trasporto dati di controllo da ricevente a mittente.

La figura seguente mostra una panoramica del processo richiesto per eseguire la comunicazione sicura peer-to-peer:

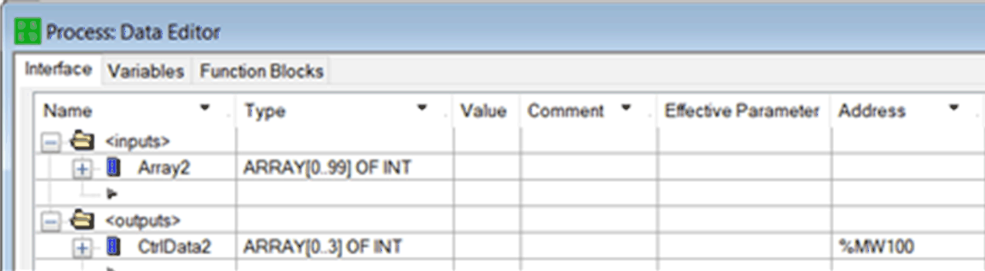
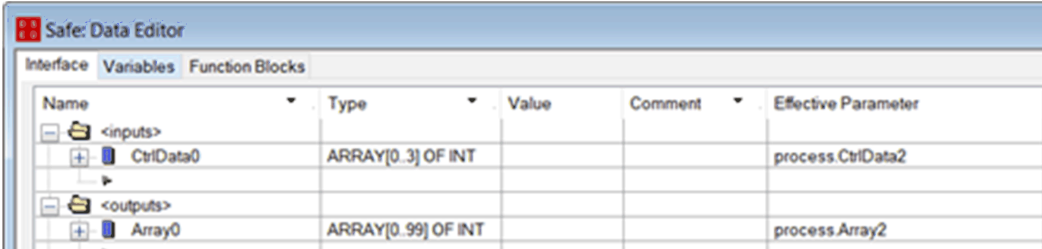
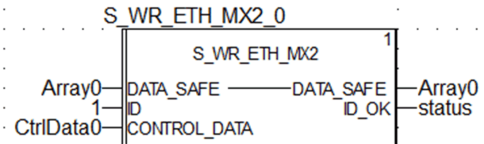


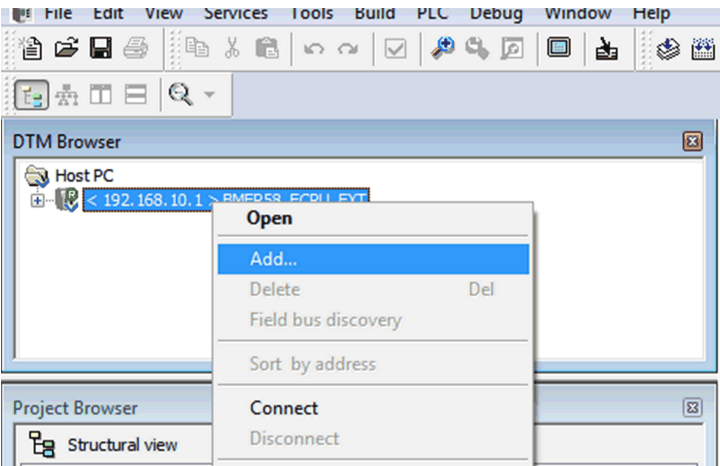
Nella figura precedente, Control Expert crea automaticamente, e nasconde dalla vista esterna, Array1 e Array4 nelle aree Globali dei PAC peer. Da un punto di vista utente, i collegamenti sono effettuati da Array0 ad Array2 e da Array3 ad Array5.

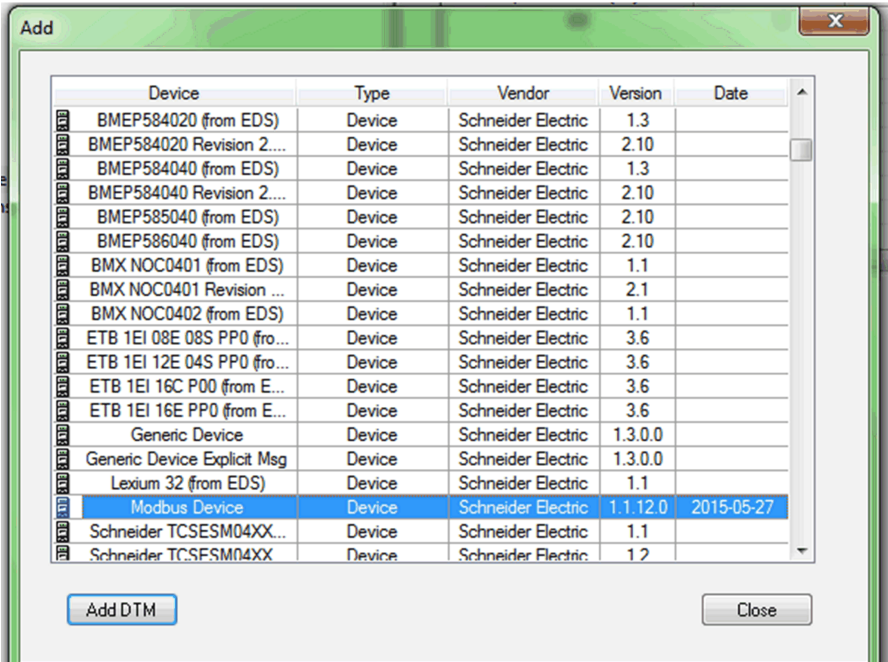
NOTA: Sulla rete Ethernet, si possono mischiare dati di sicurezza e dati non di sicurezza senza alcun impatto sul livello di integrità dei dati di sicurezza. Non vi sono restrizioni sulla rete Ethernet quando si utilizza la comunicazione peer-to-peer sicura.

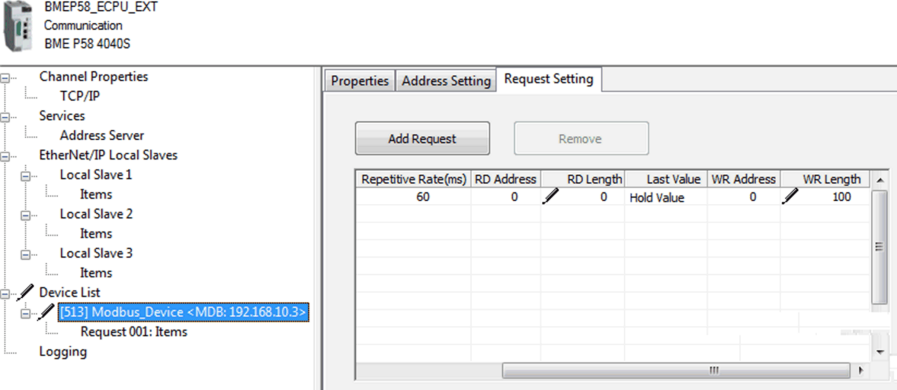
Dettagli della configurazione del trasferimento dati Peer-to-Peer

L'esempio che segue mostra come configurare un trasferimento di dati peer-to-peer tra due PAC di sicurezza con firmware della CPU 3.20 o successivo e Control Expert 15.0 o successivo:

Pas- so	Azione
1	<p>Sul PAC mittente, usare l'Editor dati di processo per creare un array di 100 interi (Array2) come ingresso nell'area Interfaccia: Creare nello stesso Editor dati di processo un array di 4 interi (CtrlData2) come uscita nell'area Interfaccia.</p> <p>I dati di controllo dal PAC ricevente verranno scritti in questo CtrlData2 tramite lo scanner Modbus, a condizione che CtrlData2 sia localizzato all'indirizzo definito nello scanner del PAC mittente (in questo esempio %MW100, vedere il passo 14):</p>  <p>The screenshot shows the 'Process: Data Editor' window with a table of variables. Under the '<inputs>' section, 'Array2' is listed with type 'ARRAY[0..99] OF INT'. Under the '<outputs>' section, 'CtrlData2' is listed with type 'ARRAY[0..3] OF INT' and address '%MW100'.</p>
2	<p>Sul PAC mittente, utilizzare l'Editor dati di sicurezza per creare un altro array di 100 interi (Array0) come uscita nell'area Interfaccia e collegarlo ai dati process.Array2 creati al passo 1 precedente, nella colonna Parametro effettivo.</p> <p>Creare nello stesso Editor dati di sicurezza un array di 4 interi (CtrlData0) come ingresso nell'area di sicurezza Interfaccia e collegarlo ai dati process.CtrlData2 creati al passo 1 precedente, nella colonna Parametro effettivo.</p>  <p>The screenshot shows the 'Safe: Data Editor' window with a table of variables. Under the '<inputs>' section, 'CtrlData0' is listed with type 'ARRAY[0..3] OF INT' and effective parameter 'process.CtrlData2'. Under the '<outputs>' section, 'Array0' is listed with type 'ARRAY[0..99] OF INT' and effective parameter 'process.Array2'.</p> <p>NOTA: Le variabili di interi degli indici 0 ... 90 dell'array contengono i valori delle variabili di sicurezza che si vogliono scambiare con il PAC ricevente. L'area rimanente è riservata per i dati di diagnostica autogenerati, incluso un CRC e un time stamp. Questi dati di diagnostica vengono utilizzati dal PAC ricevente per determinare se i dati trasferiti sono sicuri.</p>
3	<p>Sul PAC mittente, configurare il DFB S_WR_ETH_MX2 in una sezione dei task SAFE. Collegare il DFB ad Array0 e CtrlData0:</p>  <p>The diagram shows a block labeled 'S_WR_ETH_MX2_0' with two inputs on the left: 'Array0' connected to 'DATA_SAFE' and 'CtrlData0' connected to 'CONTROL_DATA'. On the right, there are two outputs: 'Array0' connected to 'DATA_SAFE' and 'status' connected to 'ID_OK'. A '1' is shown in a box next to the 'DATA_SAFE' output line.</p>

Pas-so	Azione
4	<p>Nel Browser DTM nel PAC mittente, selezionare la CPU (in questo esempio) o a un modulo di comunicazione NOC (se presente), quindi fare clic su Aggiungi... per creare uno scanner Modbus che può inviare i dati tramite Modbus TCP dal PAC mittente al PAC ricevente:</p> 

5	<p>Selezionare Dispositivo Modbus e fare clic Aggiungi DTM per aggiungere lo scanner Modbus:</p>  <table border="1" data-bbox="235 933 1001 1421"> <thead> <tr> <th>Device</th> <th>Type</th> <th>Vendor</th> <th>Version</th> <th>Date</th> </tr> </thead> <tbody> <tr><td>BMEP584020 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584020 Revision 2...</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP584040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584040 Revision 2...</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP585040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP586040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMX NOC0401 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>BMX NOC0401 Revision ...</td><td>Device</td><td>Schneider Electric</td><td>2.1</td><td></td></tr> <tr><td>BMX NOC0402 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>ETB 1EI 08E 08S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 12E 04S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16C P00 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16E PP0 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>Generic Device</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Generic Device Explicit Msg</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Lexium 32 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>Modbus Device</td><td>Device</td><td>Schneider Electric</td><td>1.1.12.0</td><td>2015-05-27</td></tr> <tr><td>Schneider TCSESM04XX...</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>Schneider TCSESM04XX</td><td>Device</td><td>Schneider Electric</td><td>1.2</td><td></td></tr> </tbody> </table>	Device	Type	Vendor	Version	Date	BMEP584020 (from EDS)	Device	Schneider Electric	1.3		BMEP584020 Revision 2...	Device	Schneider Electric	2.10		BMEP584040 (from EDS)	Device	Schneider Electric	1.3		BMEP584040 Revision 2...	Device	Schneider Electric	2.10		BMEP585040 (from EDS)	Device	Schneider Electric	2.10		BMEP586040 (from EDS)	Device	Schneider Electric	2.10		BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1		BMX NOC0401 Revision ...	Device	Schneider Electric	2.1		BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1		ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6		ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6		Generic Device	Device	Schneider Electric	1.3.0.0		Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0		Lexium 32 (from EDS)	Device	Schneider Electric	1.1		Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27	Schneider TCSESM04XX...	Device	Schneider Electric	1.1		Schneider TCSESM04XX	Device	Schneider Electric	1.2	
Device	Type	Vendor	Version	Date																																																																																																	
BMEP584020 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584020 Revision 2...	Device	Schneider Electric	2.10																																																																																																		
BMEP584040 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584040 Revision 2...	Device	Schneider Electric	2.10																																																																																																		
BMEP585040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMEP586040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
BMX NOC0401 Revision ...	Device	Schneider Electric	2.1																																																																																																		
BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6																																																																																																		
Generic Device	Device	Schneider Electric	1.3.0.0																																																																																																		
Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0																																																																																																		
Lexium 32 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27																																																																																																	
Schneider TCSESM04XX...	Device	Schneider Electric	1.1																																																																																																		
Schneider TCSESM04XX	Device	Schneider Electric	1.2																																																																																																		

Pas- so	Azione
6	<p>Aprire il dispositivo Modbus appena aggiunto e nella scheda Impostazione richiesta:</p> <ul style="list-style-type: none"> Impostare la colonna Lunghezza WR, ossia la lunghezza dei dati da scrivere, al valore 100, quindi Impostare la colonna Indirizzo WR, che è l'indirizzo in cui la tabella del PAC ricevente scriverà i dati che riceve (in questo esempio: 0, ossia il PAC mittente scriverà nella tabella a partire da %MW0 nel PAC ricevente). 
7	<p>Selezionare il nodo Request 001: Items, quindi nella scheda Uscita definire un tipo di array di INT (ossia ≥ 100 interi). Questa è la tabella del PAC mittente che verrà scritta nel PAC ricevente:</p>

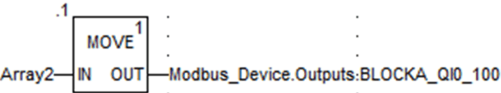
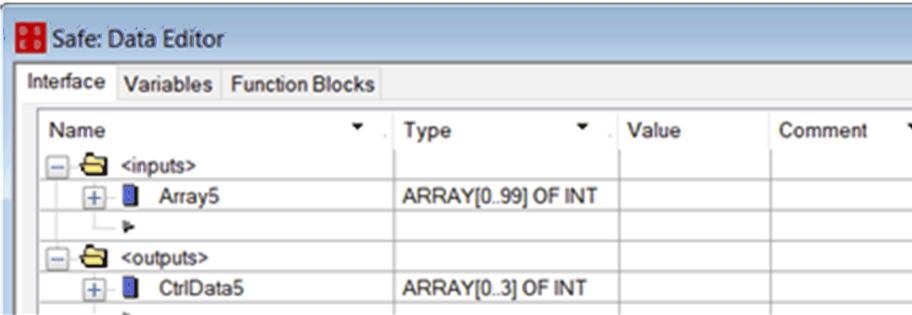
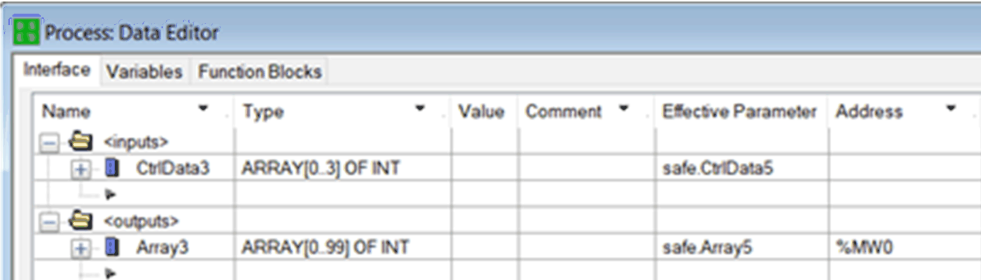
Pas-so	Azione
	<p>The screenshot displays the configuration environment for a BMEP58_ECPU_EXT communication module. The left sidebar shows a hierarchical tree structure including Channel Properties, Services, Address Server, EtherNet/IP Local Slaves, Local Slave 1-3, Device List, and Logging. The main workspace shows the 'Output' configuration for a selected device, with a table listing offsets and item names. A dialog box for defining item names is active, showing the configuration for 'BLOCKA_QI0_100' as an array of integers.</p>

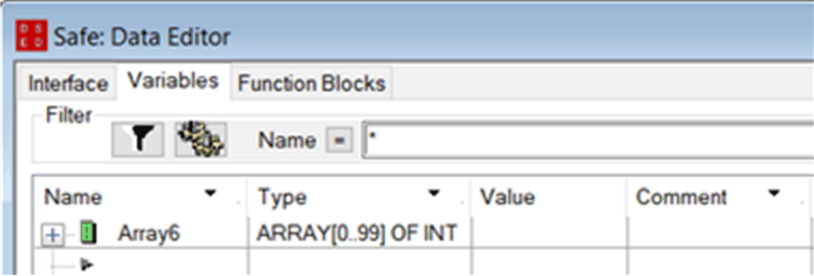
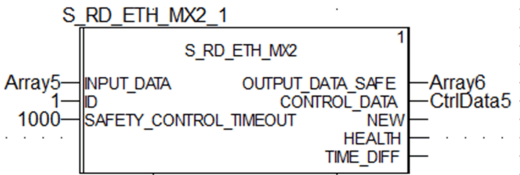
8

Dopo che la configurazione è stata salvata e compilata, il blocco (BLOCKA_QI0_100 in questo esempio) viene creato automaticamente come variabile di processo:

The screenshot shows the 'Variables' tab of the software interface. It contains a table with columns for Name, Type, Value, Comment, Alias, and Alias of. The variable 'BLOCKA_QI0_100' is listed with the type 'ARRAY[0..99] OF INT' and the alias 'tab_p'.

Name	Type	Value	Comment	Alias	Alias of
BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT				
Modbus_Device	T_Modbus_Device				
Outputs	T_Modbus_Device_OUT		Output Variables		
BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p	

Pas- so	Azione
9	<p>Sul PAC mittente, in una sezione del codice di processo, usare un DFP <code>MOVE</code> per copiare il contenuto dell'array "tab_p" nell'array definito sopra nella struttura del dispositivo Modbus:</p> 
10	<p>Sul PAC ricevente, usare l'Editor dati di sicurezza per creare un array di 100 interi (Array5) come ingresso nell'area Interfaccia:</p> <p>Creare nello stesso Editor dati di sicurezza un array di 4 interi (CtrlData5) come uscita nell'area Interfaccia.</p> 
11	<p>Sul PAC ricevente, nell'Editor dati di processo creare un array di 100 interi (Array3) come uscita dell'area Interfaccia. Collegare questo Array3 all'Array5 (creato al passo 10) nella colonna Parametro effettivo. I dati inviati dal PAC mittente verranno scritti in questo Array3 tramite lo scanner Modbus, a condizione che questo Array3 sia localizzato all'indirizzo definito nello scanner del PAC mittente (in questo esempio %MW0).</p> <p>Creare nello stesso Editor dati di processo un array di 4 interi (CtrlData3) come ingresso nell'area Interfaccia. Collegare questo CtrlData3 all'CtrlData5 (creato al passo 10) nella colonna Parametro effettivo.</p> 

Pas- so	Azione
12	<p>Sul PAC ricevente, utilizzare l'Editor dati di sicurezza per creare un array di 100 interi (Array6):</p> 
13	<p>Nel PAC ricevente, in una sezione di codice nel task SAFE, creare un'istanza del DFB S_RD_ETH_MX2 con l'array creato al passo 10 (Array5) quale parametro di ingresso e con gli array creati al passo 10 (CtrlData5) e al passo 12 (Array6) quali parametri di uscita:</p> 
14	<p>Sul PAC ricevente, ripetere i passi da 4 a 9 per configurare una comunicazione a 4 interi per inviare l'array CtrlData2 dal PAC ricevente al PAC mittente.</p> <p>In questo esempio, CtrlData deve essere scritto nel PAC mittente all'indirizzo %MW100.</p>

Black channel peer-to-peer

Ogni trasmissione dati peer-to-peer è costituita da *Dati di sicurezza utente*, che trasmettono il contenuto legato all'applicazione, e *Dati riservati*. I *Dati riservati* servono al PAC di sicurezza per testare l'affidabilità della trasmissione, che deve soddisfare i requisiti SIL3. I *Dati riservati* sono formati dai seguenti elementi:

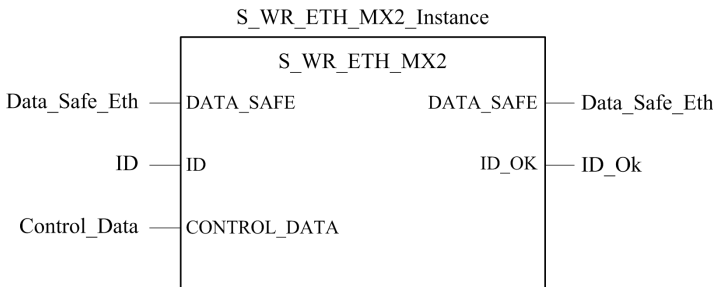
- Un CRC calcolato dal PAC mittente a partire dai dati che devono essere trasmessi. Il PAC ricevente verifica il CRC prima di usare i dati trasmessi.
- Un identificativo di comunicazione, che è incluso nel calcolo del CRC per evitare bit mascherati e cyberattacchi sulla trasmissione dei dati di sicurezza.

- Un'indicazione oraria contenente la durata della trasmissione in ms. Con firmware della CPU 3.20 o successivo, questa indicazione dell'ora è il valore di tempo sicuro fornito dalla CPU ricevente. Il PAC mittente aggiunge un valore temporale ai dati inviati al PAC ricevente. Il PAC ricevente confronta l'indicazione oraria con il proprio valore orario e la usa per:
 - Verificare l'età dei dati.
 - Rifiutare trasmissioni doppie.
 - determinare l'ordine cronologico delle trasmissioni ricevute
 - determinare il tempo trascorso tra la le notifiche di ricezione delle trasmissioni dati.

Configurazione del DFB S_WR_ETH_MX2 nella logica di programma del PAC mittente

Rappresentazione

Rappresentazione del DFB:



Per una descrizione estesa di questo DFB, consultare *EcoStruxure™ Control Expert, Safety, Block Library*.

Descrizione

Il DFB S_WR_ETH_MX2 è per PAC con firmware della CPU 3.20 o successivo. Calcola i dati (dati riservati contenenti un CRC e un timestamp) richiesti dal ricevitore per controllare e gestire gli errori rilevati durante la comunicazione peer-to-peer.

Il blocco funzione DFB S_WR_ETH_MX2 deve essere richiamato in ogni ciclo nel PAC mittente. Nell'ambito del ciclo, questo blocco deve essere eseguito nella logica dopo che sono state eseguite tutte le modifiche necessarie sui dati da inviare. Questo significa che i dati da inviare non possono essere modificati nel ciclo dopo l'esecuzione del DFB, altrimenti

Le informazioni CRC utilizzate nell'area dati riservati non saranno corrette e la comunicazione peer-to-peer sicura non potrà avere luogo.

È necessario assegnare al parametro `ID` un valore univoco che identifichi la comunicazione peer-to-peer sicura tra un mittente e un ricevente.

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Il valore del parametro `ID` deve essere univoco e fisso nella rete per una coppia mittente/ricevente.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Descrizione dell'array `DATA_SAFE`

Utilizzare la scheda **Interfaccia** nell'**Editor dati di sicurezza** ed **Editor dati processo** in per creare il collegamento tra le variabili di processo e le variabili di sicurezza. Control Expert

Il collegamento di processo e variabili di sicurezza in questo modo è possibile per:

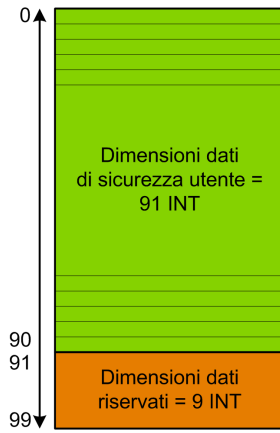
- Trasferire il valore delle variabili di sicurezza alle variabili di processo, tramite variabili globali collegate.
- Inviare valori variabili dall'area processo del PAC mittente all'area processo del PAC ricevente, tramite messaggistica esplicita su Modbus TCP.

L'array `DATA_SAFE` è composto da due aree:

- L'area **Dati sicurezza utente** contiene i dati dell'area di sicurezza del PAC. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Tali dati sono utilizzati dal PAC ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o meno. Quest'area inizia all'indice 91 e finisce all'indice 99.

NOTA: Non scrivere nell'area **Dati riservati**.

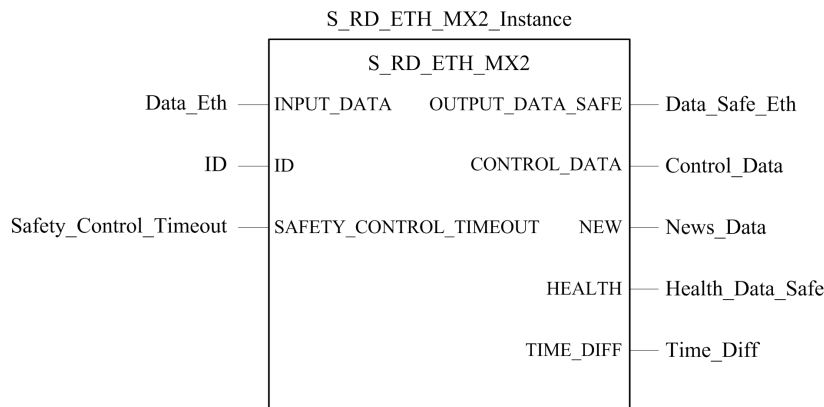
Rappresentazione della struttura dell'array `DATA_SAFE` (array[0..99] of INT):



Configurazione del DFB `s_RD_ETH_MX2` nella logica di programma del PAC ricevente.

Rappresentazione

Rappresentazione del DFB:



Vedere *EcoStruxure™ Control Expert, Safety, Block Library* per una descrizione estesa di questo DFB.

Descrizione

Il DFB `S_RD_ETH_MX2` è per PAC con firmware della CPU 3.20 o successivo. Copia i dati ricevuti nell'area di processo sull'area di sicurezza e convalida la precisione dei dati ricevuti.

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Il blocco funzione DFB `S_RD_ETH_MX2` deve essere richiamato a ogni ciclo nella logica di programma del PAC ricevente e deve essere eseguito prima che i dati del ciclo vengano usati.
- Il valore del parametro `ID` deve essere univoco e fisso nella rete per una coppia mittente/ricevente.
- Occorre testare il valore del bit `HEALTH` del DFB `S_RD_ETH_MX2` a ogni ciclo prima di usare dati sicuri per gestire la funzione di sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il blocco funzione `S_RD_ETH_MX2`:

- copia i dati ricevuti nel registro `INPUT_DATA` al registro `OUTPUT_DATA_SAFE` se supera i seguenti test:
 - Il blocco funzione controlla il CRC dell'ultimo pacchetto dati ricevuto, tramite scanner degli I/O su Ethernet (Modbus TCP). Se CRC non è corretto, i dati vengono considerati non sicuri e non scritti sul registro `OUTPUT_DATA_SAFE` nell'area di sicurezza.
 - Il blocco funzione controlla gli ultimi dati ricevuti per determinare se sono più recenti di quelli già scritti nel registro `OUTPUT_DATA_SAFE` nell'area di sicurezza (confrontando i timestamp). Se gli ultimi dati ricevuti non sono più recenti, non vengono copiati nel registro `OUTPUT_DATA_SAFE` nell'area di sicurezza.
- Verifica l'età dei dati presenti nell'area di sicurezza. Se l'età è superiore a un valore massimo impostato nel registro d'ingresso `SAFETY_CONTROL_TIMEOUT`, i dati sono dichiarati non sicuri e il bit `HEALTH` è impostato a 0.

NOTA: L'età dei dati è data dalla differenza tra l'ora in cui i dati sono calcolati nel PAC di invio e l'ora in cui vengono verificati nel PAC di ricezione.

Se il bit `HEALTH` è impostato a 0, i dati disponibili nell'array `OUTPUT_DATA_SAFE` sono considerati non sicuri. In questo caso, prendere le appropriate misure.

Descrizione degli array INPUT_DATA e OUTPUT_DATA_SAFE

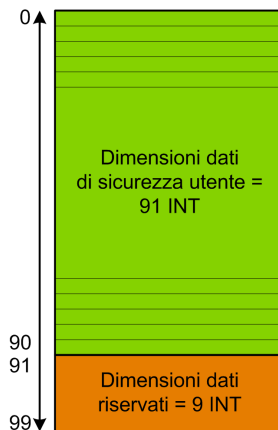
Gli array INPUT_DATA consistono di dati provenienti dall'area di memoria dati di processo. Gli array OUTPUT_DATA_SAFE consistono di variabili di sicurezza. Utilizzare le schede **Interfaccia dati di sicurezza** e **Interfaccia dati di processo** in per creare il collegamento tra le variabili di processo e le variabili di sicurezza. Control Expert

Gli array INPUT_DATA e OUTPUT_DATA_SAFE sono composti da 2 aree:

- L'area **Dati sicurezza utente** contiene i dati dell'utente. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Tali dati sono utilizzati dal PAC ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o meno. Quest'area inizia all'indice 91 e finisce all'indice 99.

NOTA: Si consiglia di non scrivere nell'area **Dati riservati**, in quanto si sovrascriverebbero i dati diagnostici generati automaticamente.

Rappresentazione della struttura degli array INPUT_DATA e OUTPUT_DATA_SAFE (array [0..99] of INT):



Descrizione array CONTROL_DATA

L'array CONTROL_DATA deve essere collegato con variabili nell'area "Globale" (definita tramite "Interfaccia dati di sicurezza") quindi, le variabili "Globali" devono essere collegate a variabili identificate nell'area "Processo" (definita tramite "Interfaccia dati di processo") per poter inviare i dati dallo IO Scanner al mittente corrispondente.

Calcolo di un valore SAFETY_CONTROL_TIMEOUT

Quando si calcola un valore SAFETY_CONTROL_TIMEOUT, considerare quanto segue:

- Valore minimo: $\text{SAFETY_CONTROL_TIMEOUT} > 2 * T1$
- Valore raccomandato: $\text{SAFETY_CONTROL_TIMEOUT} > 3 * T1$

$T1 = \text{tempo ciclo MAST CPU}_{\text{mittente}} + \text{tempo ciclo SAFE CPU}_{\text{mittente}} + \text{SAFE} + \text{Frequenza_ripetizione} + \text{Tempo trasmissione di rete} + \text{tempo ciclo MAST CPU}_{\text{ricevente}} + \text{tempo ciclo SAFE CPU}_{\text{ricevente}}$

Dove:

- *Tempo ciclo CPU_{mittente} MAST* è il tempo di ciclo MAST del PAC mittente.
- *Tempo ciclo CPU_{mittente} SAFE* è il tempo di ciclo SAFE del PAC mittente.
- *Frequenza_ripetizione* è la frequenza di tempo della query di scrittura dello scanner degli I/O dal PAC mittente al PAC ricevente.
- *Tempo trasmissione di rete* è il tempo impiegato sulla rete Ethernet per la trasmissione dei dati dal PAC mittente al PAC ricevente.
- *Tempo ciclo CPU_{ricevente} MAST* è il tempo di ciclo MAST del PAC ricevente.
- *Tempo ciclo CPU_{ricevente} SAFE* è il tempo di ciclo SAFE del PAC ricevente.

Tenere presente che il valore definito per il parametro SAFETY_CONTROL_TIMEOUT ha un effetto diretto sulla robustezza e disponibilità della comunicazione sicura peer-to-peer. Se il valore del parametro SAFETY_CONTROL_TIMEOUT supera di molto T1, la comunicazione tollera vari ritardi (ad esempio i ritardi di rete) o trasmissioni di dati danneggiati.

L'utente è responsabile per la configurazione della rete Ethernet in modo che il carico non provochi un ritardo eccessivo sulla rete durante la trasmissione dei dati, che provocherebbe la scadenza del timeout. Per consentire una comunicazione peer-to-peer sicura senza eccessivi ritardi dovuti ad altri dati non sicuri trasmessi sulla stessa rete, utilizzare una rete Ethernet dedicata per il protocollo peer-to-peer sicuro.

Quando si mette in servizio il progetto, occorre valutare le prestazioni della comunicazione sicura peer-to-peer verificando i valori forniti nel parametro di uscita TIME_DIFF e valutando il margine utilizzando il valore definito nel parametro SAFETY_CONTROL_TIMEOUT.

Note sul bit HEALTH

Quando il bit HEALTH è uguale a:

- 1: l'integrità dei dati è corretta (CRC) e l'età dei dati è inferiore al valore impostato nel registro di ingresso `SAFETY_CONTROL_TIMEOUT`.
NOTA: L'età dei dati considerati è il tempo tra:
 - l'inizio del ciclo dove i dati sono danneggiati nel PAC mittente.
 - l'inizio del ciclo dove i dati sono controllati nel PAC mittente.
- 0: i nuovi dati validi non vengono ricevuti nell'intervallo di tempo richiesto (il timer scade e il bit `HEALTH` è impostato a 0).
NOTA: Se il bit `HEALTH` è impostato a 0, i dati nell'array di uscita `OUTPUT_DATA_SAFE` sono considerati non sicuri; rispondere in modo adeguato.

M580 Comunicazioni black channel

Black channel

Black channel è il sistema utilizzato per crittografare e convalidare i dati di sicurezza trasmessi:

- Solo le apparecchiature di sicurezza Schneider Electric possono crittografare e convalidare i dati inviati tramite il black channel in un sistema di sicurezza M580.
- Lo stato di ogni trasmissione di dati di sicurezza viene testato dai moduli di sicurezza trasmettente e ricevente per ogni messaggio trasmesso.

Grazie all'uso del black channel è possibile trasmettere dati di sicurezza tramite apparecchiature intermedie non sicure, come backplane, cablaggio Ethernet, adattatori di comunicazione, ecc. Dato che le trasmissioni black channel sono crittografate, l'apparecchiatura intermedia non può leggere o modificare il contenuto dei dati di sicurezza trasmessi senza essere rilevata.

Le trasmissioni black channel avvengono in modo indipendente dal protocollo di comunicazione utilizzato per la trasmissione:

- X Bus è la portante per trasmissioni backplane tra dispositivi di sicurezza sullo stesso rack (ad es. dalla CPU a I/O locale o da un adattatore di comunicazione remoto (CRA) a I/O locale).
- EtherNet/IP è la portante per le trasmissioni dati tra rack (ad es. dalla CPU a un CRA).

I moduli I/O di sicurezza e la CPU possono inviare e ricevere comunicazioni black channel. Per ogni trasmissione il dispositivo trasmettente (CPU o I/O) aggiunge le informazioni seguenti al messaggio:

- un tag CRC per attivare la verifica del contenuto del messaggio.
- un time stamp per attivare la verifica della puntualità del messaggio.
- altre informazioni, tra cui la versione dell'applicazione e la configurazione I/O utilizzata, che identificano il modulo di I/O nella trasmissione.

Con firmware della CPU 3.10 o precedente, quando si usano moduli di I/O di sicurezza su un rack remoto, configurare la CPU come server NTP o client NTP.

Se non si implementa una di queste configurazioni, le impostazioni orarie dei moduli di I/O di sicurezza e della CPU non saranno sincronizzate e la comunicazione black channel non funzionerà correttamente. Ingressi e uscite dei moduli di I/O di sicurezza nelle derivazioni RIO entrano nello stato di sicurezza (non alimentato) o di posizionamento di sicurezza.

▲ ATTENZIONE

RISCHIO DI FUNZIONAMENTO IMPREVISTO

Se si installano moduli di I/O di sicurezza in una derivazione RIO, occorre configurare l'ora corrente per il PAC con il firmware della CPU 3.10 o precedente. Attivare il servizio NTP per il sistema M580, quindi configurare la CPU di sicurezza come server NTP o client NTP.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Il dispositivo ricevente (I/O o CPU) decodifica i messaggi e verifica la precisione del contenuto. Possono essere rilevate le seguenti condizioni:

Condizione	Descrizione
Errori di trasmissione	Errore rilevato nell'indirizzo del messaggio o nel routing.
Ripetizioni	Messaggio inviato più volte.
Dati eliminati	Manca una parte del messaggio o il messaggio è andato perduto.
Dati inseriti	Sono stati inseriti dati supplementari al messaggio.
Dati fuori sequenza	L'ordine dei messaggi è cambiato.
Dati danneggiati	Sono stati rilevati uno o più errori di bit nel messaggio.
Ritardi	Il tempo di consegna dei messaggi è eccessivamente lungo.
Mascherato	La sorgente del messaggio non è autorizzata a trasmettere dati.

Quando viene rilevato uno di questi errori, il canale viene considerato danneggiato e viene eseguita la funzione di sicurezza appropriata:

- Se la CPU rileva che una trasmissione da un modulo di ingresso è danneggiata, la CPU imposta i valori di ingresso da tale modulo nello stato sicuro (non alimentato) o di posizionamento di sicurezza).
- Un modulo di uscita imposta le sue uscite nello stato di posizionamento di sicurezza preconfigurato se rileva che una trasmissione della CPU è danneggiata.

Le uscite entrano automaticamente nello stato comandato dalla CPU dopo il corretto ripristino della comunicazione tra la CPU e il modulo di uscita.

AVVISO

MODIFICA IMPREVISTA DELLO STATO DELL'USCITA AL RIPRISTINO DELLA COMUNICAZIONE

La logica del programma deve monitorare lo stato dei canali di uscita e attivare la funzione di sicurezza di conseguenza, impostando i comandi di uscita nello stato di sicurezza.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Comunicazione tra la CPU M580 e gli I/O di sicurezza

Introduzione

Questa sezione descrive la comunicazione tra la CPU di sicurezza M580 e i moduli di I/O di sicurezza.

Comunicazioni tra PAC M580 Safety e I/O

Comunicazione tra PAC e I/O

La CPU e il coprocessore di sicurezza M580 insieme controllano tutti gli scambi sul backplane, mentre gli I/O di sicurezza rispondono ai comandi di CPU e coprocessore. I moduli di I/O di sicurezza possono essere installati in un rack X Bus BMXXBP**** o in un rack Ethernet BMEXBP****.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza nel rack principale locale avvengono tramite il backplane.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza installati in una derivazione RIO avvengono attraverso un modulo adattatore installato nella derivazione RIO:

- un adattatore BMEXRA31210 per un rack Ethernet, oppure
- un adattatore BMXCRA31210 per un rack X Bus.

NOTA: Con firmware della CPU 3.20 o successivo, il modulo adattatore BM•CRA31210 richiede un firmware 2.60 o successivo.

NOTA: Un adattatore BMXCRA31200 non può essere utilizzato per collegare i moduli di I/O di sicurezza al PAC di sicurezza M580.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza, sia nel rack principale locale che in una derivazione RIO, avvengono tramite il **black channel**, pagina 210.

Il modo per sincronizzare le impostazioni dell'ora della CPU e dei moduli di I/O di sicurezza dipende dalla versione del firmware della CPU:

- Per PAC con firmware della CPU 3.10 o precedente, è richiesta la configurazione del servizio NTP.

NOTA: Se si installano i moduli di I/O di sicurezza in un rack locale (o in un'estensione del rack locale) non è necessario attivare il servizio NTP.

- Per PAC con firmware della CPU 3.20 o successivo, la sincronizzazione dell'ora sicura si basa su un orologio interno e "monotonico".

Per ulteriori informazioni, consultare il capitolo *Sincronizzazione dell'ora*, pagina 177.

Opzionalmente, si possono utilizzare i moduli ripetitori a fibre ottiche BMXNRP0200 oppure BMXNRP0201 per estendere il collegamento fisico tra la CPU e il coprocessore nel rack locale e l'adattatore nella derivazione RIO. I moduli ripetitori a fibre ottiche migliorano l'immunità ai disturbi della rete RIO e garantiscono al contempo il mantenimento della massima disponibilità dinamica della rete e il livello di integrità di sicurezza.

Il protocollo di comunicazione tra gli I/O di sicurezza e il PAC consente gli scambi sulla rete. Questo protocollo permette ad entrambi i dispositivi di verificare l'accuratezza dei dati ricevuti, di rilevare eventuali dati corrotti e di determinare se il modulo di trasmissione diventa non operativo. Pertanto, un loop di sicurezza può includere qualsiasi adattatore RIO e backplane non interferente, pagina 29.

Alimentazione per gli I/O di sicurezza

Gli I/O di sicurezza sono alimentati a 24 VCC e 3,3 VCC sul backplane mediante il M580 modulo alimentatore di sicurezza, pagina 130. Il modulo alimentatore di sicurezza monitora l'alimentazione fornita in modo che non superi 36 VCC.

Alimentazione per funzioni non di sicurezza:

5 VCC forniti dal backplane vengono utilizzati da ogni modulo di I/O di sicurezza per le proprie funzioni non di sicurezza.

Alimentazione esterna per gli I/O di sicurezza digitali:

Per il processo non di sicurezza (sensore, attuatore) è richiesto un alimentatore esterno, non superiore a 60 VCC, che può essere una bassissima tensione di protezione (SELV/ PELV) di categoria di sovratensione II. L'alimentatore di processo non di sicurezza è controllato dal modulo di I/O di sicurezza, che rileva eventuali condizioni di sovratensione e sottotensione.

Diagnostica di un sistema di sicurezza M580

Contenuto del capitolo

Diagnostica della CPU e del coprocessore di sicurezzaM580	216
Diagnostica dell'alimentatore di sicurezza del modulo M580	229
Diagnostica degli ingressi analogici del BMXSAI0410	231
Diagnostica degli ingressi digitali del BMXSDI1602	235
Diagnostica delle uscite digitali del BMXSDO0802	241
Diagnostica delle uscite relè digitali del BMXSRA0405	247

Introduzione

Questo capitolo fornisce informazioni sulle operazioni di diagnostica che possono essere eseguite in base agli indicatori hardware (basati sullo stato dei LED) e i bit o le parole di sistema per un sistema di sicurezza M580.

Diagnostica della CPU e del coprocessore di sicurezza M580

Introduzione

Questa sezione descrive la diagnostica disponibile per le CPU di sicurezza e il coprocessore di sicurezza BME•58•040S BMEP58CPROS3.

Diagnostica di condizioni bloccanti

Introduzione

Le condizioni di blocco che si verificano durante l'esecuzione del programma di sicurezza o di processo derivano dal rilevamento di errori di sistema o dello stato HALT di un task nel quale è stato rilevato l'errore.

NOTA: Il PAC di sicurezza M580 presenta due stati HALT indipendenti:

- HALT di processo si applica ai task non SAFE (MAST, FAST, AUX0 e AUX1). Quando un task di processo entra nello stato HALT, anche tutti gli altri task di processo entrano nello stato HALT.
- SAFE HALT si applica solo al task SAFE.

Per una descrizione degli stati HALT e STOP, vedere la sezione *Stati operativi del PAC di sicurezza M580*, pagina 262.

Diagnostica

Quando la CPU rileva una condizione di blocco che provoca un errore di sistema, una descrizione dell'errore rilevato viene fornita nella parola di sistema %SW124.

Quando la CPU rileva una condizione di blocco che provoca uno stato HALT, una descrizione dell'errore rilevato viene fornita nella parola di sistema %SW125.

I valori della parola di sistema %SW124 e la corrispondente descrizione della condizione di blocco:

Valore %SW124 (hex)	Descrizione della condizione di blocco
5AF2	Errore RAM rilevato nel controllo memoria
5AFB	Errore del codice firmware di sicurezza rilevato
5AF6	Overrun del watchdog di sicurezza rilevato

Valore %SW124 (hex)	Descrizione della condizione di blocco
5AFF	Overrun del watchdog di sicurezza rilevato sul coprocessore
5B01	Coprocessore non rilevato all'avvio

I valori della parola di sistema %SW125 e la corrispondente descrizione della condizione di blocco:

Valore %SW125 (hex)	Descrizione della condizione di blocco
0...	esecuzione di una funzione sconosciuta
0002	caratteristica firma della scheda SD (usata con le funzioni funzioni <i>SIG_CHECK</i> e <i>SIG_WRITE</i>)
2258	esecuzione dell'istruzione HALT
2259	flusso di esecuzione diverso dal flusso di riferimento
23..	esecuzione di una funzione CALL verso una subroutine non definita
5AF3	errore di confronto rilevato dalla CPU
5AF9	errore di istruzione rilevato all'avvio o al runtime
5AFA	errore di confronto rilevato sul valore CRC
5AFC	errore di confronto rilevato dal coprocessore
5AFD	errore interno rilevato dal coprocessore; sottocodice in %SW126: 1 (risultato sconosciuto), 2 (applicazione CRC), 7 (errore contatore attività)
5AFE	Errore di sincronizzazione coprocessore rilevato - solo CPU; sottocodice in % SW126: 3 (diagnostica), 4 (fine UL), 5 (confronto), 6 (BC out), 8 (HALT durante UL), 9 HALT durante confronto), 10 (HALT durante BC out).
81F4	Nodo SFC non corretto
82F4	Codice SFC non accessibile
83F4	Workspace SFC non accessibile
84F4	Troppi passi SFC iniziali
85F4	Troppi passi SFC attivi
86F4	Sequenza codice SFC non corretta
87F4	Descrizione codice SFC non corretta
88F4	Tabella di riferimento SFC non corretta
89F4	errore di calcolo indice interno SFC rilevato
8AF4	Stato passo SFC non disponibile
8BF4	Memoria SFC troppo piccola dopo un cambio dovuto a un download
8CF4	Sezione Transazione/Azione non accessibile

Valore %SW125 (hex)	Descrizione della condizione di blocco
8DF4	Workspace SFC troppo piccolo
8EF4	Versione del codice SFC maggiore dell'interprete
8FF4	Versione del codice SFC più recente dell'interprete
90F4	Descrizione insufficiente di un oggetto SFC: puntatore NULL
91F4	Identificativo azione non autorizzato
92F4	Definizione insufficiente del tempo di un identificativo azione
93F4	Impossibile trovare passo macro nella lista di passi attivi per disattivazione
94F4	Overflow nella tabella azione
95F4	Overflow nella tabella di attivazione/disattivazione dei passi
9690	Errore rilevato nel controllo CRC applicazione (checksum)
DE87	Errore virgola mobile rilevato nel calcolo
DEB0	Overrun watchdog del task (%S11 e %S19 sono impostati)
DEF0	Divisione per 0
DEF1	Errore di trasferimento stringa di caratteri
DEF2	Capacità superata
DEF3	Overrun indice
DEF4	Periodi del task incoerenti
DEF7	Errore di esecuzione SFC
DEFE	Passi SFC non definiti

Riavvio dell'applicazione

Dopo che si è verificata una condizione di blocco, occorre inizializzare il task arrestato. Se si è verificato un HALT per un:

- task di processo (MAST, FAST, AUX0 o AUX1), l'inizializzazione viene eseguita dal comando **PLC > Init** di Control Expert oppure impostando il bit %S0 a 1.
- task SAFE, l'inizializzazione viene eseguita dal comando **PLC > Init Safety** di Control Expert.

Quando viene inizializzata, l'applicazione si comporta nel seguente modo:

- i dati riprendono il loro valore iniziale
- i task vengono arrestati al termine del ciclo

- l'immagine d'ingresso viene aggiornata
- le uscite vengono controllate nella posizione di sicurezza

Il comando RUN consente a questo punto il riavvio dell'applicazione o dei task.

Diagnostica di condizioni non bloccanti

Introduzione

Nel sistema si verifica una condizione non bloccante quando viene rilevato un errore di ingresso/uscita sul bus del backplane (X Bus o Ethernet) o quando viene eseguita un'istruzione che può essere elaborata dal programma utente e che non modifica lo stato operativo della CPU.

Questa sezione descrive alcuni bit e parole di sistema che possono essere utilizzati per rilevare lo stato del sistema di sicurezza e dei moduli che lo compongono.

NOTA: I bit e le parole di sistema disponibili non includono tutte le informazioni relative allo stato dei moduli di sicurezza. Schneider Electric raccomanda di utilizzare la struttura DDDT della CPU di sicurezza e dei moduli di I/O di sicurezza per determinare lo stato del sistema di sicurezza M580.

Per informazioni sul DDDT della CPU di sicurezza M580, vedere la sezione *Struttura dati DDT standalone per le CPU M580* nel documento *Modicon M580 Manuale di riferimento hardware*.

Per informazioni sui DDDT dei moduli di I/O di sicurezza M580, vedere le seguenti sezioni:

- Struttura dati BMXSAI0410, pagina 61 per il modulo di ingresso analogico di sicurezza.
- Struttura dati BMXSDI1602, pagina 94 per il modulo di ingresso digitale di sicurezza.
- Struttura dati BMXSDO0802, pagina 108 per il modulo di uscita digitale di sicurezza.
- Struttura dati BMXSRA0405, pagina 125 per il modulo di uscita relè digitale di sicurezza.

NOTA: È possibile anche eseguire operazioni diagnostiche più sofisticate dei dispositivi Ethernet per mezzo della messaggistica esplicita. A questo scopo, utilizzare:

- il blocco funzione READ_VAR (vedi EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi funzione) per i dispositivi Modbus TCP.
- il blocco funzione DATA_EXCH (vedi Modicon M580, Hardware, Manuale di riferimento), specificando il protocollo CIP nel blocco ADDM per i dispositivi EtherNet/IP.

Condizioni associate alla diagnostica I/O

Una condizione non bloccante relativa agli I/O viene diagnosticata con le seguenti indicazioni:

- comportamento del LED **I/O** della CPU: acceso fisso
 - **I/O** comportamento del LED del modulo: acceso fisso
 - bit di sistema (tipo di errore rilevato):
 - %S10 impostato a 0: errore I/O globale rilevato su uno dei moduli nel rack Ethernet o X Bus locale o remoto
 - %S16 impostato a 0: errore I/O rilevato nel task in corso su un rack X Bus
 - %S40...%S47 impostato a 0: errore I/O rilevato su un rack X Bus all'indirizzo 0 ... 7
 - %S117 impostato a 0: errore RIO rilevato su un rack X Bus remoto
 - %S119 impostato a 0: errore I/O rilevato su un rack X Bus locale
- NOTA:** Questi bit (%S10, %S16, %S40...%S47, %S117 e %S119) segnalano molti possibili errori rilevati (ma non tutti), correlati ai moduli di I/O di sicurezza.
- bit e parole di sistema relativi al canale sul quale è stato rilevato un errore (numero di canale I/O e tipo di errore rilevato) o informazioni I/O per il modulo di Device DDT (per i moduli configurati in modalità di indirizzamento Device DDT):
 - bit %Ir.m.c.ERR impostato a 1: errore canale rilevato (scambi impliciti)
 - parola %MWr.m.c.2: il valore della parola indica il tipo di errore rilevato nel canale specificato e dipende dal modulo di I/O (scambi impliciti)

Condizioni relative all'esecuzione della diagnostica del programma

Una condizione non bloccante relativa all'esecuzione del programma viene diagnosticata con i seguenti bit e parole di sistema:

- bit di sistema - tipo di errore rilevato:
 - %S15 impostato a 1: errore manipolazione stringa di caratteri rilevato.
 - %S18 impostato a 1: overrun capacità, errore rilevato su un valore a virgola mobile, o divisione per 0.
(Per maggiori informazioni, vedere la sezione *Bis di sistema per l'esecuzione sicura dei task*, pagina 399.)
Quando %S18 è impostato a 1, %SW17 contiene una descrizione dell'evento che ha causato l'errore, pagina 401.
 - %S20 impostato a 1: overrun indice.
NOTA: Se il bit di sistema configurabile %S78 è impostato nel programma, il task SAFE entra in stato HALT quando il bit di sistema %S18 è impostato a 1.
- parola di sistema - natura dell'errore rilevato:
 - %SW125 (vedi Modicon M580, Hardware, Manuale di riferimento)
(sempre aggiornato)

Diagnostica mediante LED della CPU di sicurezza M580

LED della CPU

I LED situati sul lato anteriore della CPU (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) permettono di eseguire la diagnostica dello stato del PAC, nel seguente modo.

In *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente*, consultare l'argomento Diagnostica LED per CPU M580 Hot Standby per informazioni su come diagnosticare i LED correlati alla ridondanza, compresi **[A]**, **[B]**, **[PRIM]**, **[STBY]** e **[REMOTE RUN]**.

NOTA: I LED non sono indicatori affidabili e non è possibile garantire che forniscano informazioni precise. Si consiglia di utilizzarli solo per una diagnostica di carattere generale durante la messa in servizio o la risoluzione dei problemi.

▲ AVVERTIMENTO

















RISCHIO DIAGNOSTICA IMPRECISA DEL SISTEMA

Non utilizzare i LED come indicatori operativi.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.




Stato del PAC	Nomi e colori dei LED:							
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rosso	Rosso	Verde/ Rosso	Verde/ Rosso	Verde	Verde	Verde
Alimentazione OFF								
Alimentazione ON • Autotest								
Non configurata					Nessun cavo inserito e collegato a un altro dispositivo alimentato			
					 Altrimenti			
Configurato: • Nessun errore esterno rilevato							-	-
• Errore esterno rilevato				-	-		-	-
• Nessun collegamento Ethernet, incluso il backplane Ethernet							-	-
• Indirizzo IP doppio			-				-	-

Stato del PAC	Nomi e colori dei LED:									
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD		
	Verde	Rosso	Rosso	Verde/ Rosso	Verde/ Rosso	Verde	Verde	Verde		
• Stato STOP										
			Rilevato errore su modulo, canale o configurazione di I/O		Non collegato				Task SAFE in corso	Modalità di sicurezza
										Nessun errore rilevato su ingresso/uscita configurati
Task SAFE interrotto	Modalità di manutenzione									
• Stato RUN			-							
					Non collegato				Task SAFE in corso	Modalità di sicurezza
Nessun cavo	Task SAFE interrotto	Modalità di manutenzione								
Stato HALT (errore reversibile rilevato)			-							
									Task SAFE in corso	Modalità di sicurezza
	Task SAFE	Task SAFE					Task SAFE	Modalità di		

Stato del PAC	Nomi e colori dei LED:							
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rosso	Rosso	Verde/ Rosso	Verde/ Rosso	Verde	Verde	Verde
							inter- rotto	manutenzio- ne
Stato SAFE (errore irreversibile rilevato)								
Aggiornamento sistema operativo								

1. Non tutti gli errori rilevati per un modulo di I/O di sicurezza sono segnalati tramite LED. Per maggiori informazioni in merito, vedere i DDDT per i moduli di I/O di sicurezza.

Legenda:

Simbolo	Descrizione	Simbolo	Descrizione	Simbolo	Descrizione
	Verde fisso		Rosso fisso		OFF
	Verde lampeggiante (500 ms ON, 500 ms OFF)		Rosso lampeggiante (500 ms ON, 500 ms OFF)	–	Non applicabile

Diagnostica mediante LED del coprocessore di sicurezza M580



LED del coprocessore

I LED situati sul pannello anteriore del coprocessore (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) permettono di effettuare la diagnostica dello stato del PAC, come indicato di seguito:

Stato del coprocessore	Nomi e colori dei LED:			
	SRUN	ERR	SMOD	DL
	Verde	Rosso	Verde	Verde
Alimentazione OFF				
Stato WAIT (attesa di download del firmware dalla CPU)				
Non configurato (nessuna applicazione)				
Configurato e funzionante in modalità di sicurezza: • Task SAFE arrestato				
• Task SAFE in esecuzione				
Configurato e funzionante in modalità Manutenzione: • Task SAFE arrestato				
• Task SAFE in esecuzione				
Task SAFE in HALT (errore reversibile rilevato)				
Stato SAFE (errore irreversibile rilevato)				

Legenda:

Simbolo	Descrizione	Simbolo	Descrizione	Simbolo	Descrizione
	Verde fisso		Rosso fisso		OFF

Simbolo	Descrizione		Simbolo	Descrizione		Simbolo	Descrizione
	Verde lampeggiante (500 ms ON, 500 ms OFF)			Rosso lampeggiante (500 ms ON, 500 ms OFF)			

LED per l'accesso alla scheda di memoria

Introduzione

Il LED verde di accesso alla scheda di memoria situato sotto lo sportellino della scheda di memoria SD indica l'accesso alla scheda di memoria da parte della CPU quando si inserisce una scheda. Questo LED è visibile quando lo sportello è aperto.

Stati dedicati del LED

















Il LED di **accesso alla scheda di memoria** LEDs indica i seguenti stati:

Stato dei LED	Descrizione
ACCESO	La scheda di memoria è stata riconosciuta, ma la CPU non sta eseguendo l'accesso.
lampeggiante	La CPU sta accedendo alla scheda di memoria.
lampeggiante	La scheda di memoria non è stata riconosciuta.
OFF	La scheda di memoria può essere rimossa dallo slot della CPU o la CPU non riconosce la scheda.





NOTA: Verificare che il LED sia spento prima di rimuovere la scheda dallo slot.

Significati delle combinazioni di LED

Il LED di accesso alla scheda funziona assieme al LED (vedi Modicon M580, Hardware, Manuale di riferimento) di **BACKUP**. La combinazione di questi LED indica le seguenti informazioni di diagnostica:

Stato della scheda di memoria	Condizioni	Stato della CPU	LED di accesso alla scheda di memoria	LED BACKUP
nessuna scheda di memoria nello slot	—	nessuna configurazione		
problema con la scheda di memoria	—	nessuna configurazione		
scheda di memoria senza progetto	—	nessuna configurazione		
scheda di memoria con progetto non compatibile	—	nessuna configurazione		
scheda di memoria con progetto compatibile	Viene rilevato un errore quando il progetto è ripristinato dalla scheda di memoria nella RAM della CPU.	nessuna configurazione	durante il trasferimento:  fine del trasferimento: 	durante il trasferimento:  fine del trasferimento: 
	Non vengono rilevati errori quando il progetto è ripristinato dalla scheda di memoria nella RAM della CPU.	—	durante il trasferimento:  fine del trasferimento: 	durante il trasferimento:  fine del trasferimento: 
— nessuna condizione o stato specifico della CPU				

Questa legenda mostra i diversi stati del LED:

Simbolo	Significato	Simbolo	Significato
	spento		rosso fisso
	verde fisso		verde lampeggiante

Diagnostica dell'alimentatore di sicurezza del modulo M580

Introduzione

Questa sezione descrive la diagnostica disponibile per gli alimentatori di sicurezza M580.

Diagnostica mediante LED dell'alimentatore

LED dell'alimentatore

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S dispongono di un pannello anteriore che contiene i seguenti LED di diagnostica:

- **OK**: stato operativo
- **ACT**: attività
- **RD**: ridondanza (per strutture di alimentazione ridondanti)

I LED dell'alimentatore di sicurezza M580 possono fornire le seguenti informazioni di diagnostica:

LED	Descrizione
OK	<ul style="list-style-type: none"> • ON (verde) indica che tutte le condizioni seguenti sono vere: <ul style="list-style-type: none"> ◦ Tensione backplane 24 Vdc corretta. ◦ Tensione backplane 3,3 Vdc corretta. ◦ Il pulsante RESET non è stato attivato. • Il lampeggio indica che una delle seguenti condizioni è vera: <ul style="list-style-type: none"> ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta e pulsante RESET non attivato. • OFF indica che almeno una delle seguenti condizioni è vera: <ul style="list-style-type: none"> ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta. ◦ Il pulsante RESET è stato attivato.
ACT	<ul style="list-style-type: none"> • ON (verde) indica che l'alimentatore sta fornendo l'alimentazione. In una struttura con alimentazione ridondante, il modulo è l'alimentatore primario. • OFF indica che l'alimentatore non sta fornendo alimentazione. In una struttura con alimentazione ridondante, il modulo è l'alimentatore di standby.
RD	<ul style="list-style-type: none"> • ON (verde) indica che la comunicazione tra i due moduli alimentatori è corretta. • Il lampeggio indica che una delle seguenti condizioni è vera: <ul style="list-style-type: none"> ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta. • OFF indica che almeno una delle seguenti condizioni è vera: <ul style="list-style-type: none"> ◦ La comunicazione tra i due moduli alimentatori non è corretta. ◦ Esecuzione di autotest in corso.

Diagnostica degli ingressi analogici del BMXSAI0410

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di ingresso analogico di sicurezza BMXSAI0410.

Diagnostica DDDT BMXSAI0410

Introduzione

Il modulo di ingresso analogico di sicurezza BMXSAI0410 offre la seguente diagnostica mediante i propri `T_U_ANA_SIS_IN_4`, pagina 61 elementi DDT del dispositivo:

- diagnostica degli ingressi
- rilevamento errori interni
- diagnostica del cablaggio del canale

Diagnostica degli ingressi

Viene monitorata la capacità dei sensori collegati ad ogni canale di misurare con precisione 10 valori di ingresso analogici compresi tra 4 e 20 mA. Se i test di misura degli ingressi non vengono superati, il bit `CH_HEALTH` nella struttura DDT `T_U_ANA_SIS_CH_IN`, pagina 63 è impostato a 0; questo valore indica che non è operativo.

Rilevamento degli errori interni

Il modulo elabora il valore di ingresso mediante due circuiti paralleli separati. I due valori vengono confrontati per determinare se si è verificato un errore nell'elaborazione del modulo. Se i valori confrontati sono diversi, il bit `IC` nella struttura DDDT `T_U_ANA_SIS_CH_IN` viene impostato a 1; questo valore indica che non è operativo.

Per una descrizione visiva di questo processo, vedere il diagramma dell'architettura, pagina 143 del modulo di ingresso analogico di sicurezza BMXSAI0410.

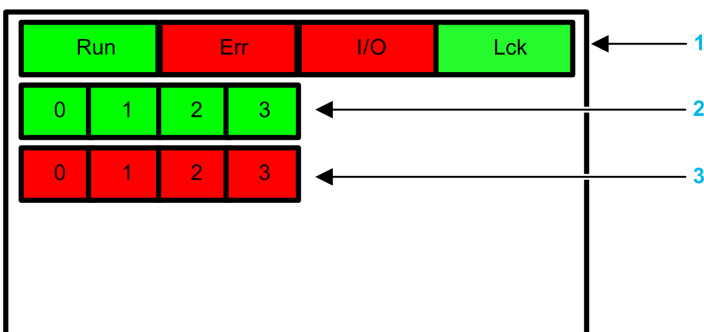
Diagnostica del cablaggio del canale

Viene effettuata costantemente la diagnostica del cablaggio del sensore al canale di ingresso per individuare un'eventuale condizione di conduttore interrotto, che viene rilevata quando la corrente di ingresso è inferiore a 3,75 mA o superiore a 20,75 mA. In questo caso, il bit OOR nella struttura DDDT `T_U_ANA_SIS_CH_IN` viene impostato a 1.

Diagnostica dei LED degli ingressi analogici del BMXSAI0410

Pannello LED

Il modulo di ingresso analogico BMXSAI0410 presenta il seguente pannello di LED sul frontalino:



1 LED di stato del modulo

2 LED di stato canale

3 LED errore rilevato sul canale

NOTA:

- I LED dell'errore di canale rilevato sono funzionanti solo dopo che il modulo è stato configurato correttamente. Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.
- Dato che il modulo di ingresso dispone di quattro canali soltanto, i LED nelle posizioni 4...7 non sono utilizzati e non sono mai accesi.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di ingresso analogico BMXSAI0410:

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Autotest all'accensione.	–
Lampeggio ¹	ON	OFF	Lampeggio ¹	L'autotest all'accensione ha rilevato un errore interno sui canali di ingresso.	Sostituire il modulo.
OFF	ON	OFF	OFF	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
OFF	Lampeggio ¹	OFF	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
X	X	ON	X	Errore esterno rilevato su canale di ingresso.	Vedere oltre la sezione <i>Diagnostica del canale</i> , pagina 234.
ON	Lampeggio ¹	X	X	Nessuna comunicazione tra CPU e modulo I/O.	Verificare che: <ul style="list-style-type: none"> la CPU sia una CPU di sicurezza M580 funzionante; il backplane sia funzionante (se il modulo I/O si trova sul rack principale); il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
ON	Sfarfallio ²	X	OFF	Comunicazione non sicura e configurazione non bloccata.	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 61 per l'istanza del modulo di I/O.
ON	Sfarfallio ²	X	ON	Comunicazione non sicura e configurazione bloccata.	Verificare che: <ul style="list-style-type: none"> la configurazione bloccata nel modulo coincida con quella salvata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert.

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
					<ul style="list-style-type: none"> Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 61 per l'istanza del modulo di I/O.
ON	ON	OFF	X	Rilevato errore interno canale di ingresso	Sostituire il modulo se la condizione persiste.
ON	OFF	OFF	OFF	La comunicazione con la CPU è regolare e la configurazione è sbloccata.	–
ON	OFF	OFF	ON	La comunicazione con la CPU è regolare e la configurazione è bloccata.	–

X indica che lo stato del LED può essere ON o OFF.

1. Lampeggio: 500 ms ON / 500 ms OFF.

2. Sfarfallio: 50 ms ON / 50 ms OFF.

Diagnostica del canale

Usare tutti i LED sul modulo di ingresso analogico BMXSAI0410 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...3)	Errore rilevato (LED 0...3)		
ON	OFF	Spento	X	ON	OFF	La corrente di ingresso è compresa tra 4 e 20 mA sul canale.	–
ON	OFF	ON	X	OFF	OFF	La corrente di ingresso è compresa tra 4 e 20 mA sul canale.	Verificare che l'alimentatore esterno, il cablaggio esterno e il sensore siano funzionanti.
ON	ON	OFF	X	OFF	ON	Il canale non è operativo.	Sostituire il modulo se la condizione persiste.

X indica che lo stato del LED può essere ON o OFF.

Diagnostica degli ingressi digitali del BMXSDI1602

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di ingresso digitale di sicurezza BMXSDI1602.

Diagnostica DDDT BMXSDI1602

Introduzione

Il modulo di ingresso digitale di sicurezza BMXSDI1602 fornisce la seguente diagnostica mediante i rispettivi elementi DDT del dispositivo `T_U_DIS_SIS_IN_16`, pagina 94:

- diagnostica degli ingressi
- rilevamento errori interni
- diagnostica del cablaggio del canale
- diagnostica di sovratensione e sottotensione

Diagnostica degli ingressi

Ogni canale di ingresso viene testato all'inizio di ogni ciclo (o scansione) per verificarne l'efficacia operativa. Ogni canale viene forzato nello stato alimentato e testato per verificare che lo stato alimentato sia stato raggiunto. Il canale viene quindi forzato nello stato non alimentato e viene nuovamente testato per verificare che lo stato non alimentato sia stato raggiunto.

Se il canale non commuta correttamente tra lo stato alimentato e quello non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_IN`, pagina 96 viene impostato a 0, per indicare che non è operativo.

Rilevamento degli errori interni

Ad ogni ciclo, il modulo esegue una sequenza di diagnostica degli ingressi. Il modulo elabora il valore di ingresso utilizzando due circuiti identici separati. I due valori vengono confrontati per determinare se nel processo interno del modulo si è verificato un errore interno. Se i valori confrontati sono diversi, il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_IN` è impostato a 1 per indicare che non è operativo.

Vedere il diagramma dell'architettura, pagina 144 del modulo di ingresso digitale di sicurezza BMXSD1602 per una descrizione visiva di questo processo.

Diagnostica del cablaggio del canale

Il cablaggio del sensore al canale di ingresso può essere diagnosticato in modo continuo per rilevare una delle seguenti condizioni:

- conduttore interrotto (circuito aperto)
- cortocircuito a 24 Vcc
- cortocircuito a 0 Vcc
- circuito incrociato tra due canali paralleli

La disponibilità di queste funzioni di diagnostica dipende dalla sorgente di alimentazione utilizzata dalla configurazione di cablaggio specifica, pagina 73, e dalla funzione di diagnostica attivata nella pagina di configurazione del modulo.

Se viene rilevata una di queste condizioni, la struttura DDDT `T_U_DIS_SIS_CH_IN` imposta il valore del bit associato a 1, nel seguente modo:

- il bit `OC` viene impostato a 1 se viene rilevata una condizione di conduttore aperto (interrotto) o di cortocircuito verso terra 0 Vdc.
- il bit `SC` viene impostato a 1 se viene rilevato un cortocircuito alla sorgente 24 Vdc o un circuito incrociato tra due canali.

Diagnostica di sovratensione e sottotensione

Il modulo effettua continuamente test per rilevare condizioni di sovratensione e sottotensione. Valgono i seguenti valori di soglia:

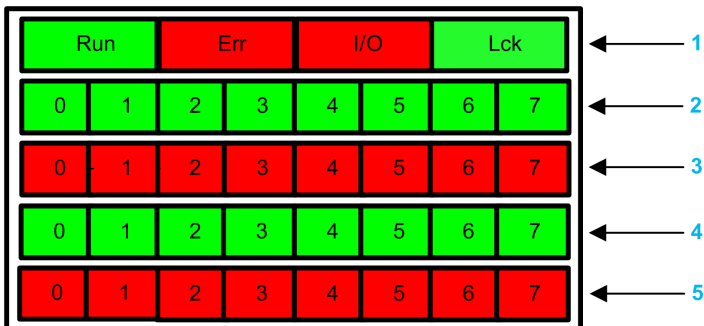
- Soglia di sottotensione = 18,6 Vdc
- Soglia di sovratensione = 33 Vdc

Se viene rilevata una di queste due condizioni, il modulo imposta il bit `PP_STS` nel DDT dispositivo `T_U_DIS_SIS_IN_16` a 0.

Diagnostica dei LED degli ingressi digitali del BMXSDI1602

Pannello LED

Il modulo di ingresso digitale BMXSDI1602 presenta il seguente pannello di LED sul frontalino:



1 LED di stato del modulo

2 LED di stato canale rank A

3 LED errore rilevato sul canale per rank A

4 LED di stato canale rank B

5 LED errore rilevato sul canale per rank B

NOTA: Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di ingresso digitale BMXSDI1602:

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggiante	Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Autotest all'accensione.	–
Lampeggiante	ON	OFF	Lampeggio ¹	L'autotest all'accensione ha rilevato un errore interno sui canali di ingresso.	Sostituire il modulo.

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggiante	ON	ON	Lampeggio ¹	<ul style="list-style-type: none"> L'autotest all'accensione ha rilevato un errore interno nei canali di ingresso; oppure Alimentazione 24VDC esterna fuori intervallo 	Verificare che l'alimentatore esterno 24 Vdc dei preattuatori sia funzionante e collegare l'alimentazione 24 Vdc.
OFF	ON	OFF	OFF	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
OFF	Lampeggio ¹	OFF	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
X	XX	ON	X	<ul style="list-style-type: none"> Alimentazione 24 Vdc esterna fuori intervallo; oppure Errore esterno rilevato su canale di ingresso. 	<ul style="list-style-type: none"> Verificare che l'alimentatore esterno 24 Vdc dei preattuatori sia funzionante. Vedere <i>Diagnostica del canale</i>, pagina 239.
ON	Lampeggio ¹	X	X	Nessuna comunicazione tra CPU e modulo.	<p>Verificare che:</p> <ul style="list-style-type: none"> la CPU sia una CPU di sicurezza M580 funzionante; il backplane sia funzionante (se il modulo I/O si trova sul rack principale); il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
ON	Sfarfallio ²	X	OFF	Comunicazione non sicura e configurazione non bloccata.	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 94 per l'istanza del modulo di I/O.
ON	Sfarfallio ²	X	ON	Comunicazione non sicura e configurazione bloccata.	<ul style="list-style-type: none"> Verificare che la configurazione bloccata nel modulo coincida con quella salvata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert. Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 94 per l'istanza del modulo di I/O.

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
ON	ON	OFF	X	Rilevato errore interno canale di ingresso.	Sostituire il modulo se la condizione persiste.
ON	OFF	OFF	OFF	La comunicazione con la CPU è regolare e la configurazione è sbloccata.	–
ON	OFF	OFF	ON	La comunicazione con la CPU è regolare e la configurazione è bloccata.	–

X indica che lo stato del LED può essere ON o OFF.

1. Lampeggio: 500 ms ON / 500 ms OFF.
2. Sfarfallio: 50 ms ON / 50 ms OFF.

Diagnostica del canale

Usare tutti i LED sul modulo di ingresso digitale BMXSDI1602 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...7, rank A/B)	Errore rilevato (LED 0...7, rank A/B)		
ON	OFF	OFF	X	ON	OFF	Stato dell'ingresso ON.	–
ON	OFF	OFF	X	OFF	OFF	Stato dell'ingresso OFF.	–
ON	ON	OFF	X	OFF	ON	Stato dell'ingresso OFF. È stato rilevato un errore interno nel canale.	Sostituire il modulo se la condizione persiste.
ON	ON	ON	X	OFF	ON	Alimentazione 24 Vdc esterna fuori intervallo.	Verificare che l'alimentatore esterno 24 Vdc dei preattuatori sia funzionante.
ON	OFF	ON	X	X	Lampeggio ¹	L'ingresso si trova in: <ul style="list-style-type: none"> • Una condizione di circuito aperto, oppure • Una condizione di cortocircuito con 0 Vdc. 	Verificare che il cablaggio sia funzionante e collegato correttamente.

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...7, rank A/B)	Errore rilevato (LED 0...7, rank A/B)		
ON	OFF	ON	X	X	Sfarfallio ²	L'ingresso si trova in: <ul style="list-style-type: none"> • Una condizione di cortocircuito con 24 Vdc, oppure • Una condizione di cortocircuito con 0 Vdc. 	Verificare che il cablaggio sia funzionante e collegato correttamente.
X indica che lo stato del LED può essere ON o OFF.							

Diagnostica delle uscite digitali del BMXSDO0802

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di uscita digitale di sicurezza BMXSDO0802.

Diagnostica DDDT BMXSDO0802

Introduzione

Il modulo di uscita digitale di sicurezza BMXSDO0802 offre le seguenti funzioni di diagnostica mediante i propri `T_U_DIS_SIS_OUT_8`, pagina 109 elementi DDT del dispositivo:

- diagnostica delle uscite
- rilevamento errori interni
- diagnostica del cablaggio del canale
- diagnostica di sovratensione e sottotensione

Diagnostica delle uscite

Ogni canale di uscita viene testato all'inizio di ogni ciclo (o scansione) per verificarne l'efficacia operativa. Il test consiste nella commutazione degli stati dei contatti delle uscite (da ON a OFF, oppure da OFF a ON) per un periodo di tempo troppo breve per provocare una risposta dell'attuatore (meno di 1 ms). Se il canale non commuta correttamente tra lo stato alimentato e lo stato non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_OUT`, pagina 111 è impostato a 0, per indicare che non è operativo.

Rilevamento degli errori interni

Il modulo elabora il valore di uscita utilizzando due circuiti identici separati. Ogni circuito legge la tensione del punto intermedio sul canale. I due valori vengono confrontati e, se non corrispondono a quelli previsti, viene segnalato un errore interno impostando il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_OUT` a 1, per indicare che non è operativo.

Vedere il diagramma dell'architettura, pagina 145 del modulo di uscita digitale di sicurezza BMXSDO0802 per una rappresentazione visiva di questo processo.

Diagnostica del cablaggio del canale

La diagnostica del cablaggio tra l'attuatore e il canale di uscita può essere effettuata in modo continuo per rilevare la presenza di una delle seguenti condizioni:

- conduttore interrotto (circuito aperto)
- cortocircuito a 24 Vcc
- cortocircuito a 0 Vcc
- circuito incrociato tra due canali paralleli
- sovraccarico del canale

NOTA: Il sovraccarico del canale può essere rilevato solo se l'uscita non è alimentata.

La disponibilità di queste azioni di diagnostica dipende dalla funzione di diagnostica abilitata nella pagina di configurazione del modulo.

Se viene rilevata una di queste condizioni, la struttura DDDT `T_U_DIS_SIS_CH_OUT` imposta il valore del bit associato a 1, nel seguente modo:

- il bit `OC` viene impostato a 1 se viene rilevata una condizione di conduttore aperto (interrotto).
- il bit `SC` viene impostato a 1 se viene rilevato un cortocircuito alla sorgente 24 Vdc o un circuito incrociato tra due canali.
- il bit `OL` è impostato a 1 se viene rilevato un cortocircuito verso terra 0 Vdc o una condizione di sovraccarico del canale.

Diagnostica di sovratensione e sottotensione

Il modulo effettua continuamente test per rilevare condizioni di sovratensione e sottotensione. Valgono i seguenti valori di soglia:

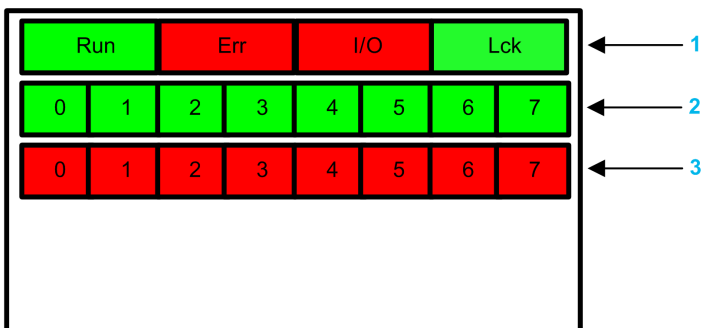
- Soglia di sottotensione = 18 Vdc
- Soglia di sovratensione = 31,8 Vdc

Se viene rilevata una di queste due condizioni, il modulo imposta il bit `PP_STS` nel DDT dispositivo `T_U_DIS_SIS_OUT_8` a 0.

Diagnostica dei LED delle uscite digitali del BMXSDO0802

Pannello LED

Il modulo di uscita digitale BMXSDO0802 presenta il seguente pannello di LED sul frontalino:



1 LED di stato del modulo

2 LED di stato canale

3 LED errore rilevato sul canale

NOTA: Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di uscita digitale BMXSDO0802:

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Autotest all'accensione.	–
Lampeggio ¹	ON	OFF	Lampeggio ¹	L'autotest all'accensione ha rilevato un errore interno sui canali di uscita.	Sostituire il modulo.

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggio ¹	ON	ON	Lampeggio ¹	<ul style="list-style-type: none"> L'autotest all'accensione ha rilevato un errore interno nei canali di uscita; oppure Alimentazione 24VDC esterna fuori intervallo 	Verificare che l'alimentatore esterno 24 Vdc dei preattuatori sia funzionante e collegare l'alimentazione 24 Vdc.
OFF	ON	OFF	OFF	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
OFF	Lampeggio ¹	OFF	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
X	X	ON	X	<ul style="list-style-type: none"> Alimentazione 24 Vdc esterna fuori intervallo; oppure Errore esterno rilevato su canale di uscita. 	<ul style="list-style-type: none"> Verificare che l'alimentatore esterno 24 Vdc dei preattuatori sia funzionante. Vedere oltre la sezione <i>Diagnostica del canale</i>, pagina 245.
ON	Lampeggio ¹	X	X	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Verificare che: <ul style="list-style-type: none"> la CPU sia una CPU di sicurezza M580 funzionante; il backplane sia funzionante (se il modulo I/O si trova sul rack principale); il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
ON	Sfarfallio ²	X	OFF	Comunicazione non sicura e configurazione non bloccata. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Per verificare le variabili disponibili per effettuare il debug della comunicazione sicura in DDDT
ON	Sfarfallio ²	X	ON	Comunicazione non sicura e configurazione bloccata. Il modulo è nello stato di posizionamento di sicurezza.	<ul style="list-style-type: none"> Verificare che la configurazione bloccata nel modulo coincida con quella salvata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert.

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
					<ul style="list-style-type: none"> Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 108 per l'istanza del modulo di I/O.
ON	ON	OFF	X	Errore interno rilevato su un canale di uscita.	Sostituire il modulo se la condizione persiste.
ON	OFF	OFF	OFF	La comunicazione con la CPU è sicura e la configurazione è sbloccata.	–
ON	OFF	OFF	ON	La comunicazione con la CPU è sicura e la configurazione è bloccata.	–

X indica che lo stato del LED può essere ON o OFF.

1. Lampeggio: 500 ms ON / 500 ms OFF.
 2. Sfarfallio: 50 ms ON / 50 ms OFF.

Diagnostica del canale

Usare tutti i LED sul modulo di uscita digitale BMXSDO0802 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...7)	Errore rilevato (LED 0...7)		
ON	OFF	OFF	X	ON	OFF	Stato dell'uscita ON.	–
ON	OFF	OFF	X	OFF	OFF	Stato dell'uscita OFF.	–
ON	ON	OFF	X	OFF	ON	Stato dell'uscita OFF. Rilevato errore interno su canale di uscita.	Sostituire il modulo se la condizione persiste.
ON	ON	ON	X	OFF	ON	L'alimentatore esterno 24 Vdc dei preattuatori è fuori intervallo	Verificare che l'alimentatore 24 Vdc sia funzionante.
ON	OFF	ON	X	OFF	Lampeggio ¹	L'uscita si trova in: <ul style="list-style-type: none"> una condizione di circuito aperto, oppure 	Verificare che il cablaggio sia funzionante e collegato correttamente.

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...7)	Errore rilevato (LED 0...7)		
						<ul style="list-style-type: none"> • una condizione di cortocircuito con 0 Vdc, oppure • sovraccarico di tensione. 	
ON	OFF	ON	X	ON	Sfarfallio ²	L'uscita si trova in: <ul style="list-style-type: none"> • una condizione di cortocircuito con 24 Vdc, oppure • una condizione di cortocircuito con un altro canale di uscita attivo. 	Verificare che il cablaggio sia funzionante e collegato correttamente.
X indica che lo stato del LED può essere ON o OFF. 1. Lampeggio: 500 ms ON / 500 ms OFF. 2. Sfarfallio: 50 ms ON / 50 ms OFF.							

Diagnostica delle uscite relè digitali del BMXSRA0405

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di uscita relè digitale di sicurezza BMXSRA0405.

Diagnostica DDDT BMXSRA0405

Introduzione

Il modulo di uscita relè digitale di sicurezza BMXSRA0405 offre la seguente diagnostica mediante i propri elementi DDT del dispositivo `T_U_DIS_SIS_OUT_4`, pagina 126:

- diagnostica dei contatti di uscita
- rilevamento errori interni

Diagnostica dei contatti di uscita

A seconda del numero di applicazione che è stato configurato per il modulo, il modulo può verificare automaticamente la sua capacità di cambiare gli stati dei contatti di uscita (da ON a OFF o da OFF a ON) per un tempo troppo breve per provocare una risposta dell'attuatore. Se il canale non cambia efficacemente dallo stato alimentato a quello non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_ROUT`, pagina 128 è impostato a 0, a indicare che non è operativo.

NOTA: I numeri di applicazione 2, 4, 6 e 8 eseguono questo test automatico del segnale. I numeri di applicazione 1, 3, 5 e 7 non lo eseguono e pertanto richiedono una transizione manuale quotidiana dello stato del canale di uscita per confermare la sua operatività.

Diagnostica dei comandi di uscita (rilevamento errori interni)

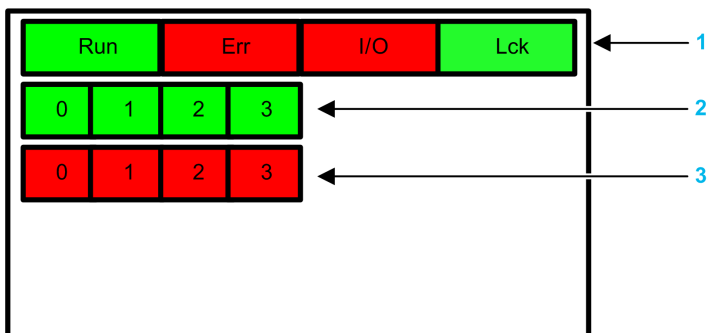
Il comando relè viene elaborato tramite due circuiti paralleli separati. I valori dei circuiti vengono confrontati. Se i valori confrontati sono diversi, il canale viene definito come non operativo e il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_ROUT` è impostato a 1.

Per una descrizione visiva di questo processo, vedere il diagramma dell'architettura, pagina 146 del modulo relè di uscita digitale di sicurezza BMXSRA0405.

Diagnostica dei LED delle uscite relè digitali del BMXSRA0405

Pannello LED

Il modulo di uscita relè digitale BMXSRA0405 presenta il seguente pannello di LED sul frontalino:



1 LED di stato del modulo

2 LED di stato canale

3 LED errore rilevato sul canale

NOTA:

- Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.
- Dato che il modulo di uscita relè dispone di quattro canali soltanto, i LED nelle posizioni 4...7 non sono utilizzati e non sono mai accesi.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di uscita relè digitale BMXSRA0405:

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Lampeggio ¹	Autotest all'accensione.	–
Lampeggio ¹	ON	Lampeggio ¹	Lampeggio ¹	L'autotest all'accensione ha rilevato un errore	–

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
				interno sui canali di uscita.	
OFF	ON	OFF	OFF	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
OFF	Lampeggio ¹	OFF	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
ON	Lampeggio ¹	OFF	X	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza.	Verificare che: <ul style="list-style-type: none"> la CPU sia una CPU di sicurezza M580 funzionante; il backplane sia funzionante (se il modulo I/O si trova sul rack principale); il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
ON	Sfarfallio ²	OFF	OFF	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 125 per l'istanza del modulo di I/O.
ON	Sfarfallio ²	OFF	ON	Comunicazione non sicura e configurazione bloccata. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	<ul style="list-style-type: none"> Verificare che la configurazione bloccata nel modulo coincida con quella salvata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert. Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 125 per l'istanza del modulo di I/O.
ON	ON	OFF	X	Errore interno rilevato sul canale di uscita.	Sostituire il modulo se la condizione persiste.
ON	OFF	OFF	OFF	La comunicazione con la CPU è sicura e la configurazione è sbloccata.	–

LED del modulo				Stato del modulo	Reazione consigliata
Run	Err	I/O	LCK		
ON	OFF	OFF	ON	La comunicazione con la CPU è sicura e la configurazione è bloccata.	–
<p>X indica che lo stato del LED può essere ON o OFF.</p> <p>1. Lampeggio: 500 ms ON / 500 ms OFF.</p> <p>2. Sfarfallio: 50 ms ON / 50 ms OFF.</p>					

Diagnostica del canale

Usare tutti i LED sul modulo di uscita relè digitale BMXSRA0405 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Reazione consigliata
Run	Err	I/O	LCK	Stato del canale (LED 0...3)	Errore rilevato (LED 0...3)		
ON	OFF	OFF	X	ON	OFF	Il relè di uscita è chiuso.	–
ON	OFF	OFF	X	OFF	OFF	Il relè di uscita è aperto.	–
ON	ON	OFF	X	OFF	ON	Il relè di uscita non è funzionante.	Sostituire il modulo se la condizione persiste.
<p>X indica che lo stato del LED può essere ON o OFF.</p>							

Utilizzo di un sistema di sicurezza M580

Contenuto del capitolo

Aree di processo, sicurezza e dati globali in Control Expert	252
Modalità operative, stati operativi e task.....	257
Creazione di un progetto di sicurezza M580	275
Blocco delle configurazioni del modulo I/O M580 di sicurezza.....	283
Inizializzazione dei dati in Control Expert	286
Lavorare con le tabelle di animazione in Control Expert	287
Aggiunta di sezioni codice	292
Gestione della sicurezza dell'applicazione	302
Gestione della sicurezza della workstation	327
Modifiche a Control Expert per il sistema di sicurezza M580	340

Introduzione

Questo capitolo fornisce informazioni su come operare un sistema di sicurezza M580.

Aree di processo, sicurezza e dati globali in Control Expert

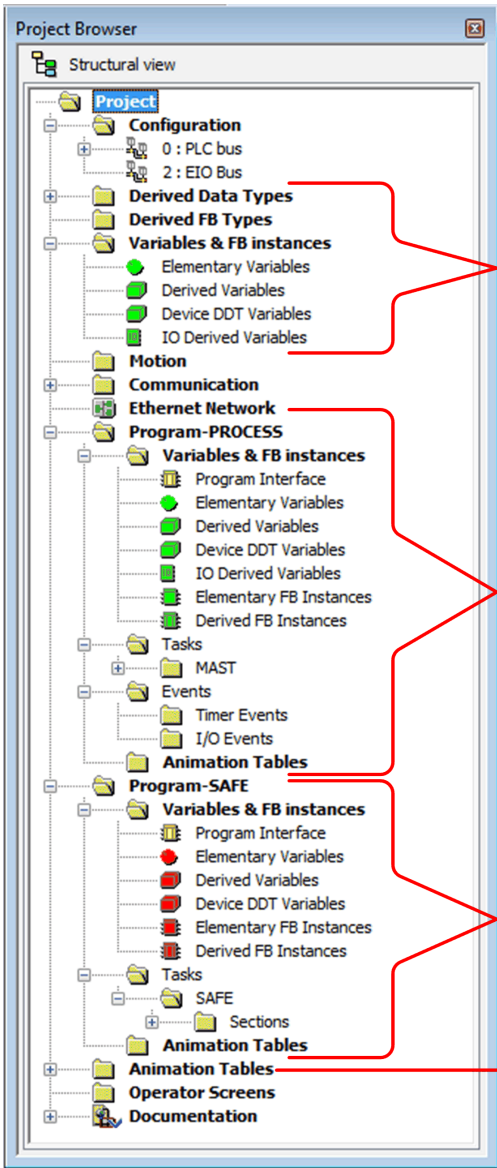
Introduzione

Questa sezione descrive la separazione delle aree dati in un progetto di sicurezza Control Expert M580.

Separazione dei dati in Control Expert

Area dati in Control Expert

La **Vista strutturale** del **Browser del progetto** visualizza la separazione dei dati in Control Expert.. Come indicato di seguito, ogni area dati dispone del proprio editor dati e raccolta di tabelle di animazione:



Editor dati globali e definizioni dei tipi

Editor dati processo, task MAST, FAST, AUX0, AUX1, tabelle di animazione processo

Editor dati di sicurezza, task di sicurezza, tabelle di animazione di sicurezza

Tabelle di animazione globali

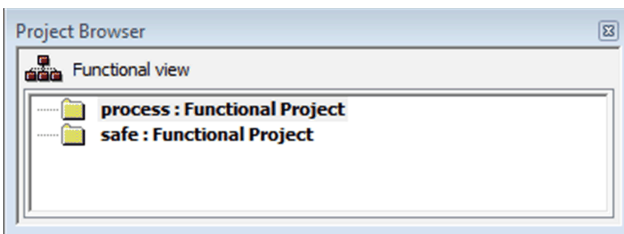
Osservando il **Browser di progetto** si potrà notare che:

- L'area sicura contiene un Editor dei dati di sicurezza, logica di sicurezza e istanze del blocco funzione utilizzati dal task SAFE. Tenere tuttavia presente che:
 - Eventi I/O, eventi timer e subroutine non sono supportati in un programma di sicurezza.
 - Le variabili IODDT non sono supportate dal task SAFE e non sono incluse nell'area di sicurezza.
 - Le icone rosse permettono di identificare le parti SAFE del programma.
- L'area di processo contiene un Editor dei dati di processo, logica di processo e istanze del blocco funzione utilizzati dai task non sicuri (ossia, MAST, FAST, AUX0 e AUX1).
- L'area globale contiene un Editor dati globali, dati derivati e tipi di blocco funzione istanziati nel processo e nei programmi di sicurezza.

NOTA: Il termine *dati globali* utilizzato in questo argomento si riferisce all'intero ambito, globale, dell'applicazione di oggetti dati in un progetto di sicurezza. Non si riferisce al servizio Global Data supportato da molti moduli Ethernet Schneider Electric.

Browser di progetto nella vista funzionale

La **Vista funzionale** del **Browser di progetto** di Control Expert, per un sistema di sicurezza M580 presenta due progetti funzionali, uno per lo spazio dei nomi del processo, l'altro per lo spazio dei nomi sicuro:



La gestione di ciascun progetto funzionale in un sistema di sicurezza M580 è uguale alla gestione di un progetto nella vista funzionale di un sistema non sicuro M580, tranne per le tabelle di animazione e le sezioni di codice.

Effetto sulla vista strutturale:

Quando si aggiunge una sezione di codice o una tabella di animazione a un progetto funzionale, questo viene associato allo spazio dei nomi di questo progetto funzionale. Aggiungendo una sezione di codice o una tabella di animazione a:

- **processo: Progetto funzionale** il progetto viene associato allo spazio dei nomi di processo del progetto nella vista strutturale.
- **sicuro: Progetto funzionale** il progetto viene associato allo spazio dei nomi sicuro del progetto nella vista strutturale.

Disponibilità delle selezioni di task e linguaggio:

Quando si crea una nuova sezione codice per un progetto funzionale (selezionando **Crea > Nuova sezione...**), le selezioni di **Linguaggio** e **Task** disponibili dipendono dal progetto funzionale:

Quando si crea una nuova sezione codice per un progetto funzionale (selezionando **Crea > Nuova sezione...**), le selezioni di **Linguaggio** e **Task** disponibili dipendono dal progetto funzionale associato:

Progetto funzionale	Task e linguaggi disponibili	
	Linguaggi ¹	Task ²
processo: Progetto funzionale	<ul style="list-style-type: none"> • IL • FBD • LD • segmento LL984 • SFC • ST 	<ul style="list-style-type: none"> • MAST • FAST • AUX0 • AUX1
sicuro: Progetto funzionale	<ul style="list-style-type: none"> • FBD • LD 	<ul style="list-style-type: none"> • SAFE

1. Selezionato nella scheda **Generale** della finestra di dialogo della nuova sezione.

2. Selezionato nella scheda **Identificazione** della finestra di dialogo della nuova sezione. Per impostazione predefinita, il task MAST è disponibile. Altre sezioni sono disponibili solo per la selezione dopo essere state create nel programma di processo.

Icone con codifica colore

Per facilitare la distinzione tra le parti sicure e quelle di processo del processo, le parti sicure dell'applicazione sono contrassegnate con icone di colore rosso.

Modalità operative, stati operativi e task

Introduzione

Questa sezione descrive le modalità operative, gli stati operativi e i task supportati dal PAC di sicurezza M580.

Modalità operativi del PAC M580 Safety

Due modalità operative

Il PAC M580 Safety presenta due modalità operative:

- Modalità di sicurezza: la modalità operativa predefinita per le operazioni di sicurezza.
- Modalità di manutenzione: una modalità operativa opzionale a cui è possibile accedere temporaneamente per eseguire debug e modificare il programma applicativo o cambiare la configurazione.

Il software Control Expert Safety è uno strumento esclusivo che consente di gestire le transizioni tra le modalità operative.

NOTA: L'impostazione della modalità operativa di un PAC di sicurezza Hot Standby, in modalità di sicurezza o di manutenzione, non è inclusa nel trasferimento di un'applicazione dal PAC primario al PAC di standby. Durante lo switchover, quando un PAC di sicurezza passa da PAC di standby a PAC primario, viene impostata automaticamente la modalità operativa di sicurezza.

La modalità di sicurezza e relative limitazioni

La modalità di sicurezza è la modalità predefinita del PAC di sicurezza. Quando si accende il PAC di sicurezza con una valida applicazione presente, il PAC entra nella modalità di sicurezza. La modalità di sicurezza consente di controllare l'esecuzione della funzione di sicurezza. È possibile caricare, scaricare, avviare e arrestare il progetto in modalità di sicurezza.

Quando il PAC M580 di sicurezza opera in modalità di sicurezza, le seguenti funzioni **non** sono disponibili:

- Download di una configurazione modificata da Control Expert nel PAC.
- Modifica e/o forzatura dei valori delle variabili e degli stati degli I/O di sicurezza.
- Debug della logica dell'applicazione, per mezzo di punti di interruzioni, punti di controllo ed esecuzione del codice passo passo.

- Utilizzo delle tabelle di animazione o richieste UMAS (ad esempio, da HMI) per scrivere su variabili di sicurezza e I/O di sicurezza.
- Modifica delle impostazioni di configurazione dei moduli di sicurezza tramite CCOTF. (Tenere presente che è supportato l'uso di CCOTF per moduli non interferenti.)
- Esecuzione della modifica online dell'applicazione di sicurezza.
- Impiego dell'animazione collegamento.

NOTA: In modalità di sicurezza, tutte le variabili di sicurezza e gli stati degli I/O di sicurezza sono di sola lettura. Non è possibile modificare direttamente il valore di una variabile di sicurezza.

È possibile creare una variabile globale e utilizzarla per passare un valore tra una variabile di processo collegato (non sicuro) e una variabile di sicurezza collegata mediante le schede dell'interfaccia dell'Editor dati processo e dell'Editor dati di sicurezza. Dopo aver creato il collegamento, il trasferimento viene eseguito nel modo seguente:

- All'inizio di ciascun task SAFE, i valori della variabile non sicura vengono copiati nelle variabili sicure.
- Al termine del task SAFE, i valori della variabile di uscita sicura vengono copiati nelle variabili non sicure.

Funzionalità della modalità di manutenzione

La modalità di manutenzione è paragonabile alla modalità normale di una CPU M580 non di sicurezza. Viene utilizzata solo per il debug e la regolazione del task SAFE dell'applicazione. La modalità di manutenzione è temporanea perché il PAC di sicurezza entra automaticamente nella modalità di sicurezza se viene persa la comunicazione tra Control Expert e il PAC, oppure quando si esegue un comando di disconnessione. Nella modalità di manutenzione, gli utenti con le autorizzazioni appropriate possono leggere e scrivere nelle variabili di sicurezza e I/O di sicurezza configurati per accettare modifiche.

In modalità di manutenzione, avviene la doppia esecuzione del codice del task SAFE, ma i risultati non vengono confrontati.

Quando il PAC M580 di sicurezza opera in modalità di manutenzione, sono disponibili le seguenti funzioni:

- Download di una configurazione modificata da Control Expert nel PAC.
- Modifica e/o forzatura dei valori delle variabili e degli stati degli I/O di sicurezza.
- Debug della logica dell'applicazione, per mezzo di punti di interruzioni, punti di controllo ed esecuzione del codice passo passo.
- Utilizzo delle tabelle di animazione o richieste UMAS (ad esempio, da HMI) per scrivere su variabili di sicurezza e I/O di sicurezza.
- Modifica della configurazione tramite CCOTF.
- Esecuzione della modifica online dell'applicazione di sicurezza.

- Impiego dell'animazione collegamento.

In modalità di manutenzione, il livello SIL del PLC di sicurezza non è garantito.

⚠ AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Mentre il PAC di sicurezza è in modalità di sicurezza, occorre prendere le misure appropriate per garantire lo stato sicuro del sistema.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

- La transizione dalla modalità di manutenzione alla modalità di sicurezza può essere effettuata nei modi seguenti:
 - Manualmente, tramite comando di menu o barra degli strumenti in Control Expert.
 - Automaticamente, dal PAC di sicurezza, quando la comunicazione tra Control Expert e il PAC viene persa per circa 50 secondi.
- La funzione ingresso di manutenzione, quando configurata, opera come controllo sulla transizione dalla modalità di sicurezza alla modalità di manutenzione. La funzione ingresso di manutenzione viene configurata in Control Expert nella scheda **Configurazione** della CPU:
 - Selezionando l'impostazione **Ingresso manutenzione** e
 - Specificando l'indirizzo topologico di un bit di ingresso (%I) per un modulo di ingresso digitale non interferente sul rack locale.



Quando è configurato l'ingresso di manutenzione, la transizione dalla modalità di sicurezza alla modalità di manutenzione prende in considerazione lo stato del bit di ingresso designato (%I). Se il bit è impostato a 0 (false), il PAC è bloccato in modalità di sicurezza. Se il bit è impostato a 1 (true), può verificarsi una transizione alla modalità di manutenzione.

Passaggio tra modalità di sicurezza e modalità di manutenzione in Control Expert

Il passaggio del PAC di sicurezza dalla modalità di manutenzione alla modalità di sicurezza non è possibile se:

- Il PAC è in modalità debug.
- È attivato un punto di interruzione in una sezione del task SAFE.
- È attivato un punto di controllo in una sezione del task SAFE.

Quando la modalità di debug non è attiva, non è attivato alcun punto di interruzione del task SAFE e non è impostato alcun punto di controllo del task SAFE, è possibile attivare manualmente una transizione tra modalità di sicurezza e modalità di manutenzione nel modo seguente:

- Per passare da modalità di sicurezza a modalità di manutenzione:
 - Selezionare **PLC > Manutenzione**, oppure
 - Fare clic sul pulsante della barra degli strumenti .
- Per passare da modalità di manutenzione a modalità di sicurezza:
 - Selezionare **PLC > Sicurezza**, oppure
 - Fare clic sul pulsante della barra degli strumenti .

NOTA: Gli eventi di ingresso e uscita nella modalità di sicurezza sono registrati nel server SYSLOG nella CPU.

Determinazione della modalità operativa

È possibile determinare la modalità operativa corrente di un PAC di sicurezza M580 tramite i LED **SMOD** di CPU e coprocessore, oppure Control Expert.

Quando i LED **SMOD** di CPU e coprocessore sono:

- Accessi *lampeggianti*, il PAC è in modalità di manutenzione.
- Accessi *fissi*, il PAC è in modalità di sicurezza.

Quando Control Expert è collegato al PAC, viene identificata la modalità operativa del PAC di sicurezza M580 in diverse posizioni:

- Le parole di sistema %SW12 (coprocessore) e %SW13 (CPU), pagina 401 insieme indicano la modalità operativa del PAC, come indicato di seguito:
 - se %SW12 è impostata a 16#A501 (esa) e %SW13 è impostata a 16#501A (esa), il PAC è in modalità di manutenzione.
 - Se una o entrambe le parole di sistema sono impostate a 16#5AFE (esa), il PAC è in modalità di sicurezza.
- Le sottoschede **Task** e **Informazioni** della scheda **Animazione** della CPU visualizzano la modalità operativa del PAC.
- La barra dei task, al fondo della finestra principale di Control Expert, indica la modalità operativa come MANUTENZIONE o SICUREZZA.

Stati operativi del PAC M580 Safety

Stati operativi

Gli stati operativi del PAC di sicurezza M580 sono descritti di seguito.

NOTA: Per una descrizione della relazione tra gli stati operativi del PAC di sicurezza M580 e quelli del PAC di Hot Standby M580, consultare il documento *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente e gli argomenti Stati del sistema Hot Standby e Transizioni e assegnazioni dello stato Hot Standby*.

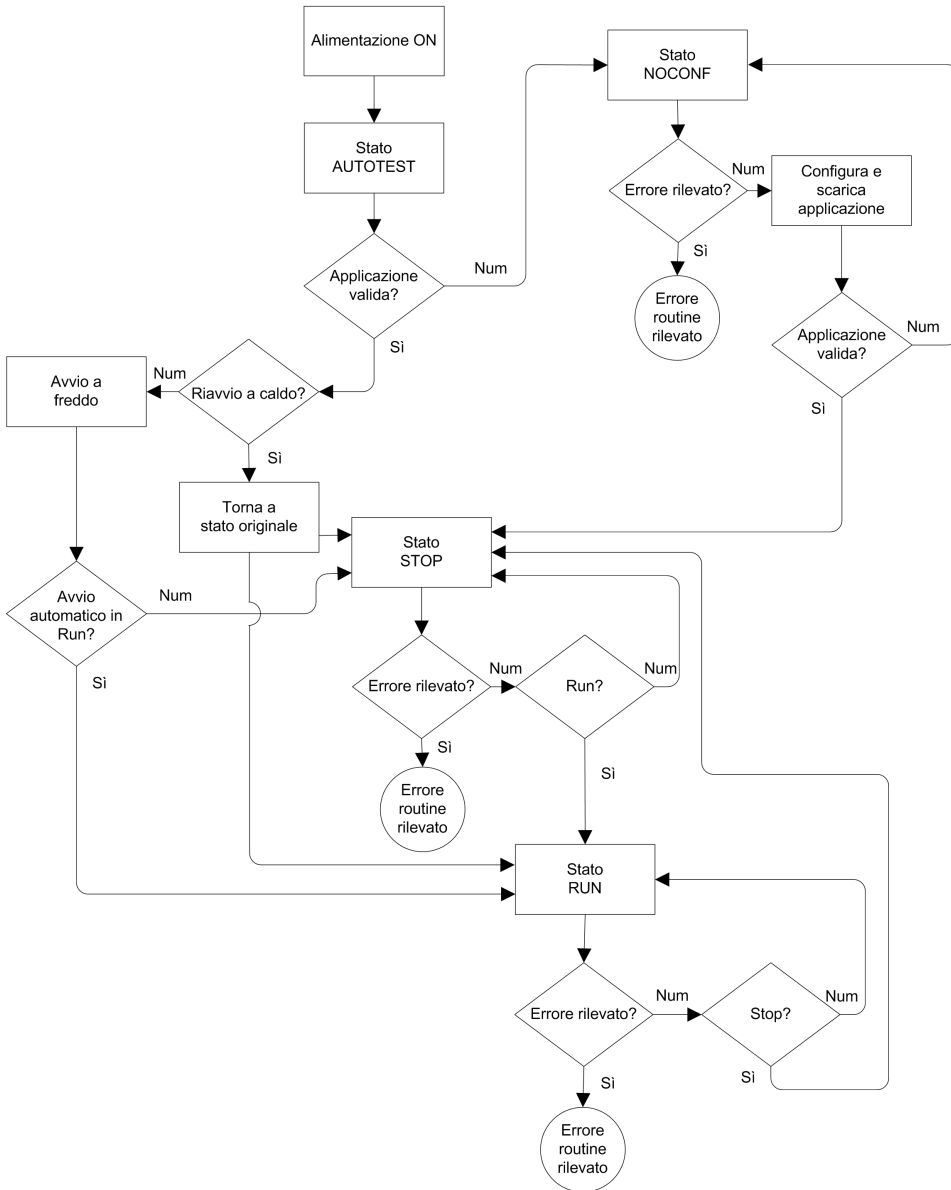
Stato operativo	Si applica a...	Descrizione
AUTOTEST	PAC	<p>La CPU sta eseguendo test automatici interni.</p> <p>NOTA: Se al rack locale principale sono collegate estensioni rack e ai connettori non utilizzati del modulo di estensione rack non sono state applicate le terminazioni di linea, la CPU rimane in AUTOTEST dopo il completamento dei test automatici.</p>
NOCONF	PAC	<p>Il programma applicativo non è valido.</p>
STOP	PAC o Task	<p>Il PAC ha una applicazione valida e non è stato rilevato alcun errore, ma il funzionamento si è interrotto perché:</p> <ul style="list-style-type: none"> All'avvio non è impostato Avvio automatico in Run (modalità di sicurezza, pagina 257). L'esecuzione è arrestata dall'esecuzione di un comando STOP (modalità di sicurezza, pagina 257 o manutenzione, pagina 258). Sono stati impostati punti di interruzione in modalità di manutenzione, quindi la connessione tra Control Expert e la CPU è stata persa per oltre 50 secondi. <p>La CPU legge gli ingressi associati a ciascun task, ma non aggiorna le uscite, che entrano nel rispettivo stato di posizionamento di sicurezza. La CPU può essere riavviata quando l'utente è pronto.</p> <p>NOTA: l'emissione di un comando STOP in Control Expert arresta tutti i task. L'evento STOP viene registrato nel server SYSLOG della CPU.</p>
HALT	Task	<p>Il PAC di sicurezza M580 presenta due stati HALT indipendenti:</p> <ul style="list-style-type: none"> HALT di processo si applica ai task non SAFE (MAST, FAST, AUX0 e AUX1). Quando un task di processo entra nello stato HALT, anche tutti gli altri task di processo entrano nello stato HALT. Il task SAFE non è influenzato da una condizione di HALT processo. SAFE HALT si applica solo al task SAFE. I task di processo non sono influenzati da una condizione SAFE HALT. <p>In ciascun caso, le operazioni del task vengono arrestate in quanto è stata rilevata una condizione di blocco imprevista, determinando una condizione ripristinabile, pagina 219.</p> <p>La CPU legge gli ingressi associati a ciascun task arrestato, ma non aggiorna le uscite, che entrano in stato di posizionamento di sicurezza.</p>
RUN	PAC o Task	<p>Con una applicazione valida e nessun errore rilevato, la CPU legge gli ingressi associati a ciascun task, esegue il codice associato a ciascun task e aggiorna le uscite associate.</p> <ul style="list-style-type: none"> in modalità di sicurezza, pagina 257: la funzione di sicurezza viene eseguita e tutte le limitazioni applicate. in modalità di manutenzione, pagina 258: il PAC funziona come qualsiasi CPU non di sicurezza. Avviene la doppia esecuzione del codice del task SAFE, ma i risultati non vengono confrontati. <p>NOTA: l'emissione di un comando RUN in Control Expert avvia tutti i task. L'evento RUN viene registrato nel server SYSLOG della CPU.</p>

Stato operativo	Si applica a...	Descrizione
WAIT	PAC	<p>La CPU si trova in stato transitorio durante il backup dei dati quando viene rilevata una condizione di disinserzione. La CPU si riavvia solo quando viene ripristinata l'alimentazione e viene rifornita la riserva di energia.</p> <p>Poiché WAIT è uno stato transitorio, potrebbe non essere visibile. La CPU esegue un riavvio a caldo, pagina 270 per uscire dallo stato WAIT.</p>
ERROR	PAC	<p>La CPU viene arrestata perché è stato rilevato un errore non ripristinabile, pagina 216 hardware o del sistema. Lo stato ERROR attiva la funzione di sicurezza, pagina 16.</p> <p>Quando il sistema è pronto per il riavvio, eseguire un avvio a freddo, pagina 270 della CPU per uscire dallo stato ERROR, facendo clic per spegnere e riaccendere o eseguendo un RESET.</p>
OS DOWNLOAD	PAC	Download del firmware della CPU o del COPRO in corso.

Consultare gli argomenti *Diagnostica LED CPU M580 CPU*, pagina 221 e *Diagnostica LED coprocessore M580 Safety*, pagina 221 per informazioni sugli stati operativi del PAC.

Transizioni dello stato operativo

Le transizioni tra diversi stati in un PAC di sicurezza M580 sono descritte di seguito:



Per informazioni su come vengono gestiti gli errori rilevati dal sistema di sicurezza, consultare *Elaborazione degli errori rilevati*, pagina 266.

Elaborazione degli errori rilevati

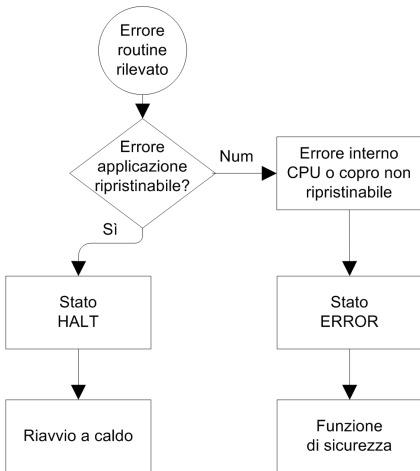
Il PAC di sicurezza M580 gestisce i seguenti tipi di errori rilevati della CPU:

- Errori rilevati dell'applicazione ripristinabili: questi eventi provocano l'ingresso degli eventi correlati nello stato HALT.

NOTA: Poiché i task MAST, FAST e AUX operano nella stessa area di memoria, un evento che provoca l'ingresso di uno di questi task nello stato HALT determina l'ingresso nello stato HALT anche degli altri task non sicuri. Poiché lo stato SAFE opera in un'area di memoria separata, i task non sicuri non vengono influenzati se il task SAFE entra nello stato HALT.

- Errori rilevati dell'applicazione non ripristinabili: errori interni rilevati di CPU o coprocessore: questi eventi provocano l'ingresso del PAC nello stato ERROR. La funzione di sicurezza viene applicata alla parte interessata del loop di sicurezza.

La logica del processo di gestione errori rilevati è descritta di seguito:



L'impatto degli errori rilevati sui singoli task è descritta di seguito:

Tipo di errore rilevato	Stato del task			
	FAST	SAFE	MAST	AUX
Errori overrun watchdog task FAST	HALT	RUN ¹	HALT	HALT
Overrun watchdog task SAFE	RUN	HALT ²	RUN	RUN
Overrun watchdog task MAST	HALT	RUN	HALT	HALT
Overrun watchdog task AUX	HALT	RUN	HALT	HALT
Errore rilevato di esecuzione codice doppio CPU	RUN	HALT ²	RUN	RUN

Tipo di errore rilevato	Stato del task			
	FAST	SAFE	MAST	AUX
Overrun watchdog di sicurezza ³	ERROR	ERROR ²	ERROR	ERROR
Errore interno rilevato CPU	ERROR	ERROR ²	ERROR	ERROR

1. Poiché il task FAST è una priorità più alta del task SAFE, il ritardo del task FAST può provocare l'ingresso del task SAFE nello stato HALT o ERROR invece dello stato RUN.

2. Gli stati ERROR e HALT sul task SAFE provocano l'impostazione delle uscite di sicurezza nel relativo stato configurabile dall'utente (posizione di sicurezza o mantieni).

3. Il watchdog di sicurezza viene impostato a un valore uguale a 1,5 volte il watchdog del task SAFE.

Visualizzatore di stato di sicurezza della barra dei task

Quando Control Expert è collegato al PAC di sicurezza M580, la barra dei task include un campo che descrive gli stati operativi combinati del task SAFE e dei task di processo (MAST, FAST, AUX0, AUX1), come indicato di seguito:

Stato task di processo	Stato task SAFE	Messaggio
STOP (tutti i task di processo in stato STOP)	STOP	STOP
STOP (tutti i task di processo in stato STOP)	RUN	RUN
STOP (tutti i task di processo in stato STOP)	HALT	SAFE HALT
RUN (almeno un task di processo in stato RUN)	STOP	RUN
RUN (almeno un task di processo in stato RUN)	RUN	RUN
RUN (almeno un task di processo in stato RUN)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

Sequenze di avvio

Introduzione

Il PAC di sicurezza M580 può accedere alla sequenza di avvio nelle seguenti circostanze:

- All'accensione iniziale.

- In risposta a una interruzione di alimentazione.

In base al tipo di task e al contesto dell'interruzione di alimentazione, il PAC di sicurezza M580 può eseguire un avvio a freddo, pagina 270 o un avvio a caldo, pagina 270 al ripristino dell'alimentazione.

Avvio iniziale

All'avvio iniziale, il PAC di sicurezza M580 esegue un avvio a freddo. Tutti i task, compresi il task SAFE e i task non sicuri (MAST, FAST, AUX0, AUX1), entrano in stato STOP a meno che non sia attivato **Avvio automatico in RUN**, in tale caso tutti i task entrano nello stato RUN.

Avvio dopo un'interruzione dell'alimentazione

L'alimentatore di sicurezza M580 fornisce una riserva di alimentazione che continua ad alimentare tutti i moduli nel rack per un massimo di 10 ms in caso di interruzione dell'alimentazione. Quando la riserva di alimentazione si esaurisce, il PAC di sicurezza M580 esegue un ciclo di spegnimento e riaccensione completo.

Prima di spegnere il sistema, la CPU di sicurezza memorizza i seguenti dati che definiscono il contesto operativo al momento dello spegnimento:

- Data e ora dello spegnimento (memorizzate in %SW54...%SW58).
- Stato di ciascun task.
- Stato dei timer evento.
- Valori dei contatori in esecuzione.
- Firma dell'applicazione.
- Dati dell'applicazione (valori correnti delle variabili dell'applicazione)
- Checksum dell'applicazione.

Dopo lo spegnimento, l'avvio può essere automatico (se l'alimentazione è stata ripristinata prima del completamento dell'arresto) o manuale (in caso contrario).

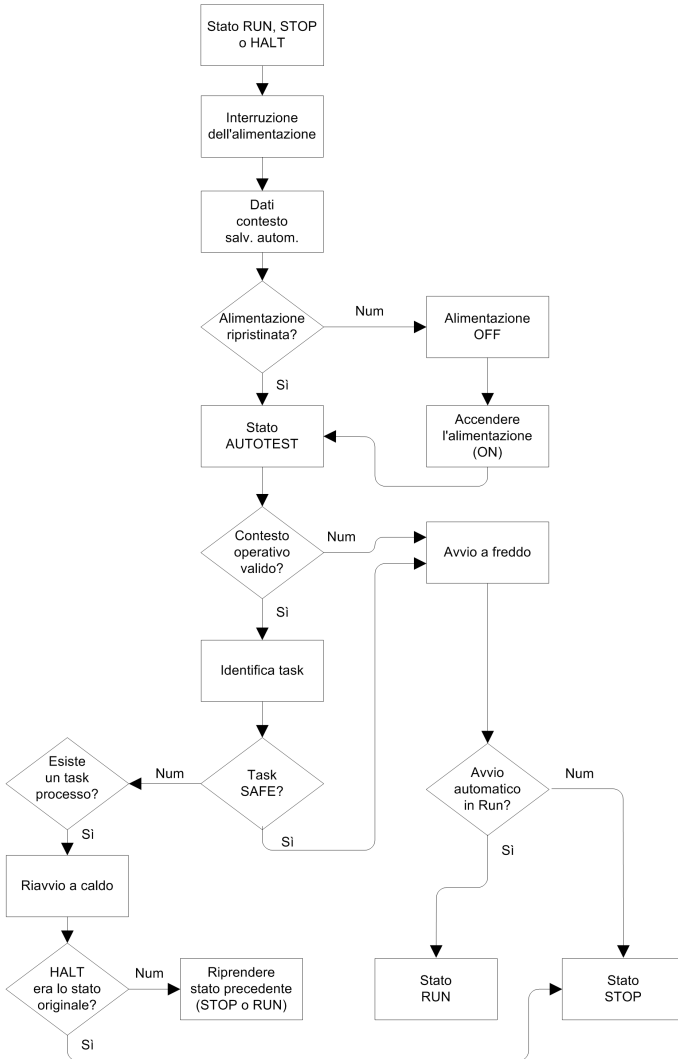
Quindi, il PAC di sicurezza M580 esegue test automatici e controlla la validità dei dati del contesto operativo salvati al momento dell'interruzione di alimentazione, come indicato di seguito:

- Viene verificato il checksum dell'applicazione.
- Viene letta la scheda di memoria SD per confermare che contenga un'applicazione valida.
- Se l'applicazione nella scheda di memoria SD è valida, vengono controllate le firme per confermare che siano identiche.

- La firma dell'applicazione salvata viene verificata confrontandola con la firma dell'applicazione memorizzata.

Se il contesto operativo è valido, i task non sicuri eseguono un avvio a caldo. Se il contesto operativo non è valido, i task non sicuri eseguono un avvio a freddo. In un caso o nell'altro, il task SAFE esegue un avvio a freddo.

Dopo un'interruzione di alimentazione viene presentata la seguente sequenza di avvio:



Avvio a freddo

L'avvio a freddo determina per tutti i task, compresi il task SAFE e i task non sicuri (MAST, FAST, AUX0, AUX1) l'ingresso nello stato STOP, a meno che non sia attivato **Avvio automatico in RUN**, nel qual caso tutti i task entrano in stato RUN.

L'avvio a freddo determina le operazioni seguenti:

- Ai dati dell'applicazione (compresi bit interni, dati di I/O, parole interne e così via) vengono assegnati i valori iniziali definiti dall'applicazione.
- Le funzioni elementari vengono impostate ai valori predefiniti.
- I blocchi funzione elementari e le rispettive variabili vengono impostati ai valori predefiniti.
- Bit e parole di sistema vengono impostati ai valori predefiniti.
- Inizializza tutte le variabili forzate applicandone i valori predefiniti (inizializzati).

È possibile eseguire l'avvio a freddo per dati, variabili e funzioni nello spazio dei nomi di processo selezionando **PLC > Init** in *Control Expert*, pagina 286, oppure impostando il bit di sistema %S0 (COLDSTART) a 1. Il bit di sistema %S0 non ha alcun effetto su dati e funzioni appartenenti allo spazio dei nomi sicuro.

NOTA: A seguito di un avvio a freddo, il task SAFE può avviarsi solo dopo l'avvio del task MAST.

Avvio a caldo

L'avvio a caldo determina per ciascun task L di processo, compresi i task (MAST, FAST, AUX0, AUX1), l'ingresso nel relativo stato operativo al momento dell'interruzione di alimentazione. Per contro, l'avvio a caldo determina l'ingresso del task SAFE nello stato STOP, a meno che non sia selezionato **Avvio automatico in RUN**.

NOTA: Se un task era in stato HALT o in un punto di interruzione al momento dell'interruzione di alimentazione, tale task entra nello stato STOP dopo l'avvio a caldo.

L'avvio a caldo determina le operazioni seguenti:

- Ripristina l'ultimo valore conservato per le variabili dello spazio dei nomi di processo.
- Inizializza le variabili dello spazio dei nomi sicuro applicandone i valori predefiniti (inizializzati).
- Inizializza tutte le variabili forzate applicandone i valori predefiniti (inizializzati).
- Ripristina l'ultimo valore conservato per le variabili dell'applicazione.
- Imposta %S1 (WARMSTART) a 1.
- Le connessioni tra il PAC e la CPU vengono reimpostate.
- I moduli di I/O vengono riconfigurati (se necessario) con le rispettive impostazioni memorizzate.

- Gli eventi, il task FAST e i task AUX vengono disattivati.
- Il task MAST viene riavviato dall'inizio del ciclo.
- %S1 viene azzerato al termine della prima esecuzione del task MAST.
- Gli eventi, il task FAST e i task AUX vengono attivati.

Se era in corso l'esecuzione di un task al momento dell'interruzione dell'alimentazione, dopo l'avvio a caldo il task riprende l'esecuzione dall'inizio.

⚠ AVVERTIMENTO

FUNZIONAMENTO ANOMALO DELL'APPARECCHIATURA

Si è responsabili per confermare che la selezione di **Avvio automatico in RUN** sia conforme con il corretto comportamento del proprio sistema. In caso contrario, disattivare questa funzione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Task del PAC di sicurezza M580

Introduzione

Un PAC di sicurezza M580 può eseguire applicazioni che comprendono uno o più task. A differenza di un'applicazione a task singolo che esegue solo il task MAST, un'applicazione a più task definisce la priorità di ogni task.

Il PAC di sicurezza M580 supporta i seguenti task:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Caratteristiche dei task

I task supportati dal PAC di sicurezza M580 presentano le seguenti caratteristiche:

Nome task	Prio-rità	Modello ora	Intervallo periodo	Periodo predefinito	Campo watchdog	Watchdog predefinito
FAST	1	Periodico	1...255 ms	5 ms	10...500 ms ²	100 ms ²
SAFE	2	Periodico	10...255 ms	20 ms	10...500 ms ²	250 ms ²
MAST ¹	3	Ciclico ⁴ o Periodico	1...255 ms	20 ms	10...1500 ms ²	250 ms ²
AUX0 ³	4	Periodico	10...2550 ms	100 ms	100...5000 ms ²	2000 ms ²
AUX1 ³	5	Periodico	10...2550 ms	200 ms	100...5000 ms ²	2000 ms ²

1. Il task MAST è richiesto e non può essere disattivato.

2. Se è attivato CCOTF (selezionando **Modifica online in modalità RUN o STOP** nella scheda **Configurazione** della finestra di dialogo delle proprietà della CPU), l'impostazione **Watchdog** minima è 64 ms.

3. Supportato dai PAC di sicurezza BMEP58•040S standalone. Non supportato dai PAC Hot Standby di sicurezza BMEH58•040S.

4. I PAC di sicurezza BMEP58•040S standalone supportano i modelli di tempo ciclico e periodico. I PAC Hot Standby di sicurezza BMEH58•040S supportano solo il modello di tempo periodico.

Priorità task

I PAC M580 Safety eseguono i task in attesa in base alla loro priorità. Quando un task è in esecuzione, è possibile interromperlo con un altro task con priorità relativa più alta. Ad esempio, un task periodico, quando è pianificato per l'esecuzione del proprio codice, interrompe un task a priorità più bassa, ma attende fino al completamento di un task a priorità più alta.

Considerazioni sulla configurazione del task

Tutti i task non sicuri (MAST, FAST, AUX0 e AUX1) operano nella stessa area di memoria, mentre il task SAFE opera nella propria area di memoria separata. Di conseguenza:

- Se un task non sicuro eccede il proprio watchdog, tutti i task non sicuri entrano in stato HALT, mentre il task SAFE continua a essere operativo.
- Se il task SAFE supera il proprio watchdog, solo il task SAFE entra in stato HALT, mentre i task non sicuri continuano a essere operativi.

Quando si creano e configurano task per l'applicazione, tenere presente le seguenti caratteristiche del task:

Task SAFE:

Progettare questo task periodico per eseguire solo sezioni di codice correlate alla sicurezza per i moduli I/O di sicurezza. Poiché al task SAFE è assegnata una priorità più bassa del task FAST, l'esecuzione del task SAFE può essere interrotta dal task FAST.

Definire il tempo di esecuzione massimo per il task SAFE impostando il valore appropriato di watchdog. Considerare il tempo richiesto per eseguire il codice e per leggere e scrivere i dati sicuri. Se il tempo per eseguire il task SAFE supera l'impostazione del watchdog, il task SAFE entra nello stato HALT e la parola di sistema %SW125 visualizza il codice di errore rilevato 16#DEB0.

NOTA:

- Poiché il task FAST ha una priorità più alta del task SAFE, è possibile includere un componente per il tempo di ritardo del task FAST nell'impostazione del watchdog del task SAFE.
- Se l'overrun dell'esecuzione del task SAFE è uguale al "Watchdog di sicurezza" (ossia il valore uguale a una volta e una volta e mezza dell'impostazione del watchdog del task SAFE), la CPU e il Copro entrano nello stato ERROR e viene applicata la funzione di sicurezza.

Task MAST:

Può essere configurato come ciclico o periodico. Quando si opera in modalità ciclica, definire un tempo di esecuzione massimo immettendo un valore appropriato del watchdog MAST. Aggiungere un piccolo intervallo di tempo a questo valore al termine di ogni ciclo per consentire l'esecuzione di altri task di sistema a bassa priorità. Poiché i task AUX hanno una priorità più bassa di MAST, se questo intervallo di tempo non viene fornito, i task AUX non possono mai essere eseguiti. Considerare l'aggiunta di un intervallo di tempo uguale al 10% del tempo di esecuzione del ciclo, con un minimo di 1 ms e un massimo di 10 ms.

Se il tempo per eseguire il task MAST ciclico supera l'impostazione del watchdog, il task MAST e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Quando si opera in modalità periodica, è possibile che il task MAST superi il proprio periodo. In tale caso, il task MAST opera in modalità ciclica e viene impostato il bit di sistema %S11.

Task FAST:

Lo scopo di questo task periodico è di eseguire una parte ad alta priorità dell'applicazione. Definire un tempo di esecuzione massimo impostando il valore di watchdog FAST. Poiché il task FAST interrompe l'esecuzione di tutti gli altri task, compreso il task SAFE, si consiglia di configurare un tempo di esecuzione del task FAST il più corto possibile. Si consiglia un valore di watchdog del task FAST non molto più grande del periodo FAST.

Se il tempo per eseguire il task FAST supera l'impostazione del watchdog, il task FAST e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Task AUX:

AUX0 e AUX1 sono task periodici opzionali. Il loro scopo è di eseguire una parte a bassa priorità dell'applicazione. I task AUX vengono eseguiti solo al termine dell'esecuzione dei task MAST, SAFE e FAST.

Definire un tempo di esecuzione massimo per i task AUX impostando il valore appropriato di watchdog. Se il tempo per eseguire un task AUX supera l'impostazione del watchdog, il task AUX e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Creazione di un progetto di sicurezza M580

Creazione di un progetto di sicurezza M580

Creazione di un progetto di sicurezza M580

Il menu **Crea** di Control Expert Safety presenta tre diversi comandi di creazione e un comando Firma Safe, come segue:

Comando	Descrizione
Crea modifiche	Compila solo le modifiche apportate al programma applicativo dal precedente comando di creazione e le aggiunge al programma generato in precedenza.
Ricrea tutto il progetto	Ricompila l'intero programma applicativo, sostituendo il programma creato in precedenza. NOTA: Per i moduli I/O di sicurezza M580, questo comando non genera un nuovo valore dell'identificativo esclusivo del modulo (MUID). Al contrario, viene conservato il valore MUID generato in precedenza.
Rinnova ID e Ricrea tutto	Ricompila l'intero programma applicativo, sostituendo il programma creato in precedenza. NOTA: <ul style="list-style-type: none"> Eseguire questo comando solo quando i moduli I/O di sicurezza sono sbloccati, pagina 283. Per i moduli I/O di sicurezza M580, questo comando genera un nuovo valore dell'identificativo esclusivo del modulo (MUID) e sostituisce il valore MUID esistente con uno nuovo.
Aggiorna Firma Safe	Da utilizzare per generare manualmente una firma di origini SAFE, pagina 275 per l'applicazione Safe. NOTA: Questo comando viene abilitato solo quando il parametro Generale > Impostazioni crea > Gestione Firma Safe è impostato su Su richiesta utente .

Firma Safe

Introduzione

M580PAC di sicurezza, sia indipendenti che Hot Standby, comprendono un meccanismo di produzione di un'impronta creata da un algoritmo SHA256 dell'applicazione sicura: firma di origini SAFE. Durante il trasferimento dell'applicazione dal PC a PAC, Control Expert confronta la firma di origini SAFE nel PC con quella nel PAC per determinare se l'applicazione sicura nel PC sia la stessa o o sia diversa da quella presente nel PAC.

La funzionalità firma sicura è opzionale. La generazione di una firma di origini SAFE può richiedere molto tempo, in base alla dimensione dell'applicazione sicura. Utilizzando le opzioni di gestione della firma sicura, è possibile generare una firma di origini SAFE che crea un valore algoritmico per l'applicazione sicura

- su ogni creazione oppure
- solo quando si desidera generare manualmente una firma di origini SAFE e aggiungerla alla creazione più recente oppure
- non apportare modifiche

Azioni che modificano la firma di origini SAFE

Sia le modifiche di configurazione che le modifiche di valore di variabili possono causare modifiche alla firma di origini SAFE.

Modifiche di configurazione: Le seguenti azioni di configurazione portano a una modifica della firma:

Dispositivo	Azione
CPU di sicurezza	Modificare i riferimenti di CPU tramite Sostituisci processore...
	Modificare la versione di CPU tramite Sostituisci processore...
	Modificare qualsiasi parametro sulle schede di configurazione della CPU Configurazione o Hot Standby
	Modificare un parametro su una scheda dell'installazione di comunicazione Ethernet della CPU (Sicurezza , IP Config , RSTP , SNMP , NTP , Porta Service , Sicurezza ...).
Coprocessore di sicurezza	Non applicabile, in quanto il coprocessore non è configurabile.
Altro modulo di sicurezza	Aggiunta/Eliminazione/Spostamento di un modulo, sia <ul style="list-style-type: none"> • Direttamente (con un comando) • Indirettamente (ad esempio, sostituendo un backplane Ethernet a 8 slot con un modulo di sicurezza nello slot 7, con un backplane Ethernet a 4 slot, eliminando quindi un modulo)
	Modificare un parametro del modulo di sicurezza, situato sulla scheda Configurazione (ad esempio, Rilevamento di cortocircuito a 24 V , Rilevamento di conduttore aperto) e sul pannello di sinistra dell'editor (ad esempio Funzione , Posizionamento di sicurezza).
	Modifica dell'ID di un modulo tramite il comando Rinnova ID e Ricrea tutto .
	Modifica del nome istanza DDT del dispositivo.
Modulo CIP Safety	Aggiunta/rimozione di un modulo.
	Modificare un parametro del modulo CIP Safety tramite l'editor DTM del dispositivo CIP Safety, o l' Elenco dispositivi DTM master della CPU.

Dispositivo	Azione
	Modifica del nome istanza DDT del dispositivo.
Alimentatore di sicurezza	Aggiunta/rimozione di un'alimentazione di sicurezza.
Altre apparecchiature correlate alla sicurezza	Modifica di un indirizzo topologico di un'apparecchiatura di supporto ad un dispositivo di sicurezza, ad esempio: <ul style="list-style-type: none"> • Spostamento di un rack contenente un dispositivo di sicurezza. • Spostamento di un bus o una derivazione contenente un dispositivo di sicurezza.

Modifiche di valori: Ad eccezione di quanto definito, i seguenti elementi sono compresi nel computo della firma di origini SAFE. Una modifica di tali valori causa una modifica della firma di origini SAFE:

Tipo	Elementi
Programma	Task SAFE e sezioni di codice correlate.
Variabili	Tutte le variabili dell'area sicura e i loro attributi.
DDT	Ciascun attributo DDT sicuro, eccetto quelli di data e di versione.
	Le variabili interne a ciascun DDT, compresi i loro attributi.
	I DDT sicuri, anche se non vengono utilizzati nell'applicazione sicura.
DFB	Ciascun attributo DFT sicuro, eccetto quelli di data e di versione.
	Le variabili interne a ciascun DFB, compresi i loro attributi.
	I DFB sicuri, anche se non vengono utilizzati nell'applicazione sicura.
Impostazioni di ambito sicuro	Tutte le Impostazioni di progetto per Ambito = sicuro.
Impostazioni di ambito comuni	Le seguenti Impostazioni di progetto per Ambito = comune.
	Variabili <ul style="list-style-type: none"> • Consenti cifre iniziali • Set di caratteri • Consenti l'uso di fronte EBOOL • Consenti INT/DINT al posto di ANY_BIT • Consenti estrazione bit di INT, WORD e BYTE • Variabili array rappresentate direttamente • Attiva analisi veloce per il trending • Forza inizializzazione riferimenti
	Programma > Lingue > Comune <ul style="list-style-type: none"> • Consenti procedure • Consenti commenti annidati • Consenti assegnazioni multiple [a:=b:=c:] (ST/LD)

Tipo	Elementi
	<ul style="list-style-type: none"> • Consenti parametri vuoti in chiamata non formale (ST/IL) • Mantieni collegamenti di output su EF disattivato (EN=0) • Visualizza commenti completi dell'elemento di struttura
	Programma > Lingue > LD <ul style="list-style-type: none"> • Rilevamento fronte di scansione singolo per EBOOL
	Generale > Ora¹ <ul style="list-style-type: none"> • Fuso orario personalizzato • Fuso orario • Offset ora • Passa automaticamente all'ora legale <ul style="list-style-type: none"> ◦ Tutte le impostazioni START e END sotto Regola automaticamente per l'ora legale
<p>1. Queste variabili non sono esportate, ma ogni modifica ai loro valori modifica la firma parziale di configurazione.</p>	

Gestione della firma di origini SAFE

La firma di origini SAFE è gestita in Control Expert nella finestra **Strumenti > Impostazioni di progetto**, selezionando **Generale > Crea impostazioni**, quindi selezionando una delle seguenti impostazioni di **Gestione firma sicura**:

- **Automatico** (impostazione predefinita): genera una nuova firma di origini SAFE ad ogni esecuzione del comando **Crea**.
- **Su richiesta dell'utente**: genera una nuova firma di origini SAFE quando viene eseguito il comando **Crea > Aggiorna Firma sicura**.

NOTA: Selezionando **Su richiesta dell'utente**, Control Expert genera una firma di origini SAFE pari a 0 per ciascuna creazione. Se non viene eseguito il comando **Crea > Aggiorna Firma sicura**, si sceglie di non utilizzare la funzionalità Firma sicura.

Trasferimento di un'applicazione da PC al PLC

Quando viene scaricata un'applicazione dal PC al PAC, Control Expert confronta la firma di origini SAFE nell'applicazione scaricata con una presente nel PAC. Control Expert si comporta come segue:

Nuova Firma Safe	Firma Safe PAC	Visualizzazioni Control Expert
Qualsiasi	Nessuna applicazione	Trasferisci conferma
Qualsiasi (eccetto 0)	0	Trasferisci conferma

Nuova Firma Safe	Firma Safe PAC	Visualizzazioni Control Expert
0	0	Trasferisci conferma
0	Qualsiasi (eccetto 0)	Trasferisci conferma, seguito da un avviso "Ciò causerà un reset della Firma sicura", seguito da una nuova conferma di trasferimento
XXXX = YYYY ²	YYYY	Trasferisci conferma
XXXX ≠ YYYY ³	YYYY	Trasferisci conferma, seguito da un avviso "Ciò modifica la Firma sicura", seguito da una nuova conferma di trasferimento
<p>1. Il valore "0" indica che la firma di origini SAFE non è stata generata automaticamente o manualmente.</p> <p>2. L'applicazione sicura nel PC (XXXX) e l'applicazione sicura nel PAC (YYYY) sono UGUALI.</p> <p>3. L'applicazione sicura nel PC (XXXX) e l'applicazione sicura nel PAC (YYYY) sono DIVERSE.</p>		

Visualizzazione della firma di origini SAFE

Quando viene utilizzata, la firma di origini SAFE consiste di una serie di valori esadecimali e può essere molto lunga, rendendo difficoltosa la lettura diretta e il confronto del valore da parte dell'utente. Tuttavia, è possibile copiare e incollare la firma di origini SAFE in uno strumento di testo adeguato per effettuare confronti. La firma di origini SAFE può essere trovata in una delle seguenti destinazioni Control Expert:

- **Proprietà di progetto > scheda** Identificazione (vedi EcoStruxure™ Control Expert, Modalità operative): da **Browser progetto**, fare clic con il pulsante destro del mouse su **Progetto** e selezionare **Proprietà**.
- **PLCScreen > scheda** Informazioni (vedi EcoStruxure™ Control Expert, Modalità operative): da **Browser progetto**, spostarsi fino a **Progetto > Configurazione > Bus PLC > <CPU>**, fare clic con il pulsante destro del mouse e selezionare **Apri**, quindi selezionare la scheda **Animazione**.
- **Finestra di dialogo** Confronto PC < - - > PLC (vedi EcoStruxure™ Control Expert, Modalità operative): selezionare questo comando dal menu **PLC**.
- Finestra di dialogo (vedi EcoStruxure™ Control Expert, Modalità operative) **Trasferisci progetto al PLC**: selezionare questo comando dal menu **PLC** (o dalla finestra di dialogo **Confronto PC < - - > PLC**).

Confronto tra la firma di origini SAFE e SAId

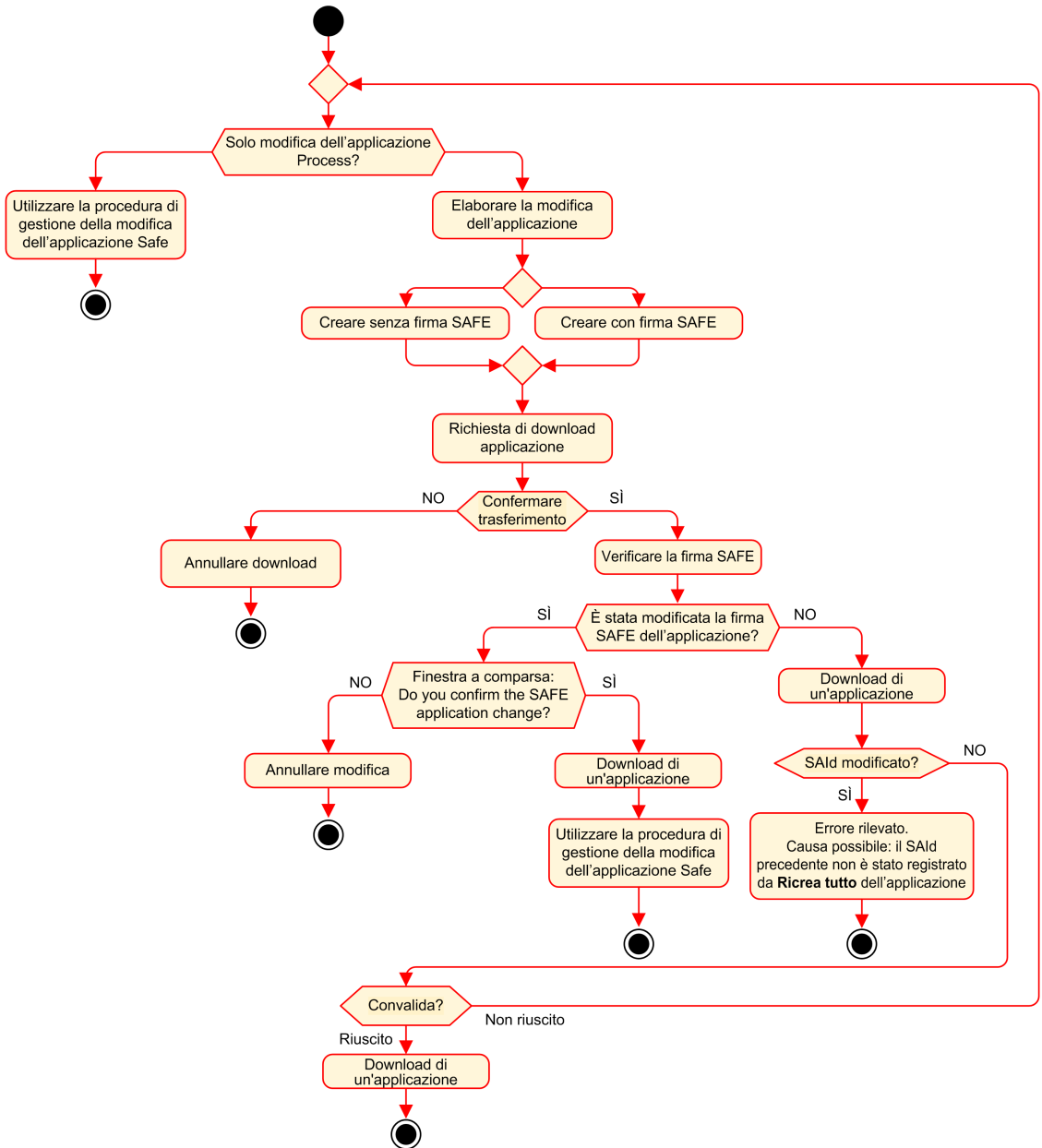
La firma di origini SAFE è stata creata per fornire una verifica *a priori* che l'applicazione non sia stata modificata. Si consiglia di utilizzare questa funzionalità ogni volta che l'applicazione di processo viene modificata, pagina 281 per prevenire modifiche non previste dell'applicazione sicura.

La firma di origini SAFE è un meccanismo affidabile, ma non è sufficiente per le applicazioni di sicurezza perché lo stesso codice sorgente può corrispondere a diversi codici binari (eseguibili), in base al tipo di creazione utilizzata dopo l'ultima modifica del codice sicuro.

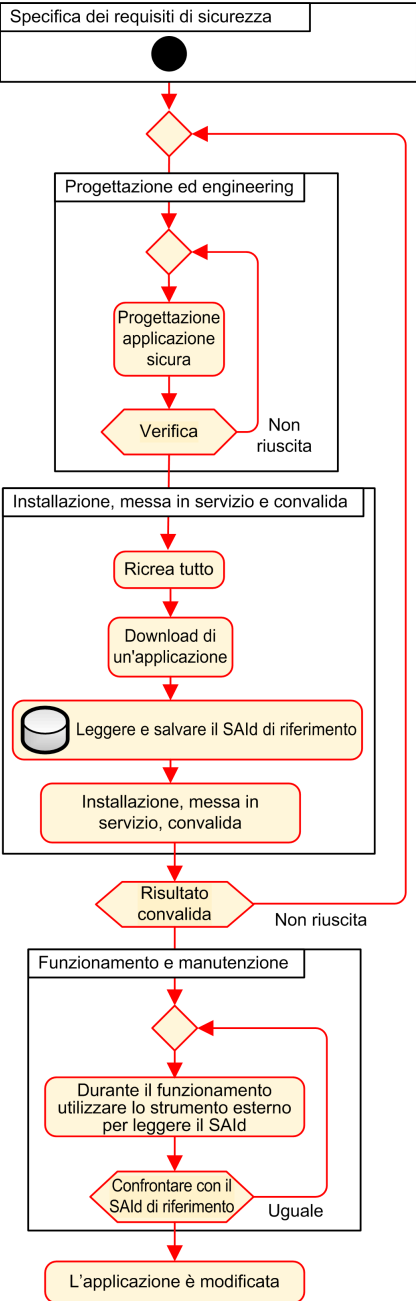
SAId, pagina 369 può essere valutato solo in runtime. Viene calcolato due volte e confrontato sia da CPU che da COPRO, sulla base di un codice binario eseguito dall'applicazione sicura. Siccome SAId è sensibile alle modifiche, comprese quelle apportate dal comando **Ricrea tutto** dopo una modifica di creazione, si consiglia di utilizzare il comando **Ricrea tutto** per generare una versione di riferimento dell'applicazione sicura. Questo processo, pagina 282 consente di utilizzare qualsiasi forma di creazione (**Ricrea tutto**, **Crea Modifiche** online o offline) per le modifiche dell'applicazione di processo senza che vengano apportate modifiche al SAId.

SAId è il metodo consigliato per confermare che l'applicazione sicura sia quella convalidata. Il valore SAId non viene verificato automaticamente dall'applicazione. Per tale motivo, si consiglia di verificare regolarmente SAId con qualsiasi strumento adeguato (ad esempio, utilizzando Control Expert o un HMI) leggendo l'uscita del blocco funzione S_SYST_STAT_MX o il contenuto della parola di sistema %SW169, pagina 401.

Modifiche del Processo semplificato di applicazione di processo



Gestione SAId



Blocco delle configurazioni del modulo I/O M580 di sicurezza

Blocco delle configurazioni del modulo I/O M580 di sicurezza

Blocco della configurazione del modulo I/O di sicurezza

Ogni modulo I/O di sicurezza dispone di un pulsante di blocco di configurazione (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza), in alto nella parte anteriore del modulo. Lo scopo della funzione di blocco è impedire modifiche indesiderate alla configurazione del modulo I/O. Ad esempio, il blocco della configurazione corrente del modulo I/O può impedire il tentativo di assegnare al modulo una configurazione falsa o semplicemente proteggere da errori di configurazione.

Per raggiungere il livello di sicurezza integrata (SIL) previsto, bloccare ogni modulo I/O di sicurezza dopo averlo configurato, ma prima di iniziare o riprendere le operazioni.

⚠ AVVERTIMENTO

RISCHIO DI DEGRADAZIONE IMPREVISTA AL LIVELLO DI INTEGRITÀ DI SICUREZZA DEL PROGETTO

Occorre bloccare ciascun modulo di I/O di sicurezza dopo averlo configurato ma prima di iniziare le operazioni.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

I meccanismi di blocco e sblocco funzionano come segue:

- Per bloccare la configurazione di un modulo I/O di sicurezza, tenere premuto il pulsante di blocco per oltre 3 secondi, quindi rilasciare il pulsante.
- Per sbloccare la configurazione di un modulo I/O di sicurezza, tenere premuto il pulsante di blocco per oltre 3 secondi, quindi rilasciare il pulsante.

Scenari per il blocco delle configurazioni del modulo I/O di sicurezza

La procedura da seguire per bloccare le configurazioni dei moduli I/O di sicurezza SIL3 varia in base allo scenario, che può essere:

- Prima configurazione dei moduli I/O
- Sostituzione dispositivo veloce dei moduli I/O
- Eseguire una modifica della configurazione al volo (CCOTF) per i moduli I/O

La procedura per ogni scenario è descritta di seguito.

Prima configurazione dei moduli di sicurezza I/O SIL3:

Pas- so	Azione
1	Collegare Control Expert al PAC di sicurezza M580.
2	Utilizzare il comando Trasferimento progetto dal PLC per caricare il progetto dal PAC in Control Expert.
3	Nella finestra Bus PLC in Control Expert, aprire ciascun modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
4	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo è la stessa del passo 3 precedente.
5	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) per oltre 3 secondi, quindi rilasciare il pulsante.
6	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.

Sostituzione dispositivo veloce di un modulo di sicurezza I/O SIL3:

Pas- so	Azione
1	Sostituire il modulo I/O di sicurezza SIL3 con uno nuovo.
2	Collegare Control Expert al PAC di sicurezza M580 in modalità operativa di manutenzione, pagina 258.
3	Nella finestra Bus PLC in Control Expert, aprire ciascun modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
4	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo non è cambiata ed è la stessa del passo 3 precedente.
5	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) per oltre 3 secondi, quindi rilasciare il pulsante.
6	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.

Esecuzione di CCOTF per aggiungere un nuovo modulo di sicurezza I/O SIL3:

Pas- so	Azione
1	Collegare Control Expert al PAC di sicurezza M580 in modalità operativa di manutenzione, pagina 258.
2	Aggiungere un nuovo modulo di I/O di sicurezza SIL3 alla configurazione e modificarne le impostazioni se necessario.
3	Eseguire il comando Crea > Crea modifiche .
4	Nella finestra Bus PLC in Control Expert, aprire ciascun modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
5	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo non è cambiata ed è la stessa del passo 3 precedente.
6	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) per oltre 3 secondi, quindi rilasciare il pulsante.
7	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.
8	Nel menu PLC di Control Expert, comandare al PAC di entrare in modalità di sicurezza, pagina 257.

Inizializzazione dei dati in Control Expert

Inizializzazione dei dati in Control Expert per il PAC M580 Safety

Due comandi di Init

Il menu **PLC** in Control Expert fornisce due comandi separati per l'inizializzazione dei dati:

- Il comando **Init** inizializza i dati per lo spazio dei nomi di processo (o non sicuro), utilizzabile dai task MAST, FAST, AUX0 e AUX1. È possibile eseguire questo comando se il PAC opera in modalità di sicurezza o manutenzione mentre il PAC è in stato STOP. Questo comando è analogo all'impostazione a 1 del bit di sistema %S0 (COLDSTART).

NOTA: Impostando il bit %S0 a 1 si inizializzano i dati solo nello spazio dei nomi di processo. Non si influisce sui dati nello spazio dei nomi sicuro.

- Il comando **Iniz sicurezza** inizializza i dati solo per lo spazio dei nomi sicuro, dati utilizzabili esclusivamente dal task SAFE. È possibile eseguire questo comando solo se il task SAFE opera in modalità di manutenzione, mentre il task SAFE è in stato STOP o HALT. L'esecuzione di questo comando quando il task SAFE è in stato HALT determina il riavvio del task SAFE nello stato STOP.

Entrambi i comandi **Init** e **Iniz sicurezza** eseguono un avvio a freddo., pagina 270

Lavorare con le tabelle di animazione in Control Expert

Tabelle di animazione e schermate operatore

Introduzione

Un PAC di sicurezza M580 supporta tre tipi di tabelle di animazione, ciascuna associata a una delle seguenti aree dati:

- Le tabelle di animazione dell'area processo possono includere solo i dati nello spazio dei nomi processo.
- Le tabelle di animazione dell'area di sicurezza possono includere solo i dati nello spazio dei nomi sicuro.
- Le tabelle di animazione globali possono includere dati per l'intera applicazione, compresi i dati creati per gli spazi dei nomi sicuro e processo e variabili globali.

NOTA: In una tabella di animazione globale, i nomi della variabile dati includono un prefisso che indica lo spazio dei nomi sorgente, come segue:

- Una variabile dati dallo spazio dei nomi Sicuro viene visualizzata come “SAFE.<nomevar>”.
- Una variabile dati dallo spazio dei nomi Processo viene visualizzata come “PROCESS.<nome variabile>”.
- Una variabile dati dallo spazio dei nomi Globale (o Applicazione) visualizza solo il proprio <nome variabile>, senza prefisso dello spazio dei nomi.

I dati di processo e sicurezza da un PAC di sicurezza M580 sono accessibili anche da processi esterni (ad esempio, SCADA o HMI).

La possibilità di creare e modificare una tabella di animazione e la possibilità di eseguirne le funzioni dipendono dallo spazio dei nomi delle variabili interessate e dalla modalità operativa del progetto di sicurezza.

Condizioni per creare e modificare le tabelle di animazione

La creazione e modifica delle tabelle di animazione coinvolge l'aggiunta o la rimozione delle variabili dati. La possibilità di aggiungere variabili dati alla tabella di animazione o di eliminarle dipende da:

- Spazio dei nomi (sicuro o processo) in cui risiede la variabile dati.
- Modalità operativa (sicurezza o manutenzione) del PAC di sicurezza M580.

Quando si collega Control Expert al PAC di sicurezza M580, è possibile creare e modificare le tabelle di animazione nel modo seguente:

- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi processo a una tabella di animazione processo o globale è supportata mentre il PAC di sicurezza M580 opera in modalità sicura o in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi a una tabella di animazione di sicurezza è supportata mentre il PAC di sicurezza M580 opera in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi sicuro a una tabella di animazione sicura è supportata mentre il PAC di sicurezza M580 opera in modalità di sicurezza solo se le impostazioni di progetto non comprendono tabelle di animazione nelle informazioni di caricamento.

NOTA: Le tabelle di animazione vengono incluse o escluse dalle informazioni di caricamento in Control Expert selezionando **Strumenti > Impostazioni progetto...** per aprire la finestra **Impostazioni progetto...**, quindi passando a **Impostazioni progetto > Generale > Dati integrati PLC > Informazioni di caricamento > Tabelle di animazione.**

Condizioni per il funzionamento delle tabelle di animazione

È possibile utilizzare le tabelle di animazione per forzare il valore di una variabile, annullare la forzatura del valore di una variabile, modificare un singolo valore di variabile o modificare più valori di variabili. La possibilità di eseguire queste funzioni dipende dallo spazio dei nomi in cui risiede una variabile e dalla modalità operativa del PAC di sicurezza M580, come indicato di seguito:

- I valori della variabile di processo o globale possono essere letti o scritti in modalità operativa di sicurezza e manutenzione.
- I valori della variabile di sicurezza possono essere letti o scritti in modalità operativa di manutenzione
- I valori della variabile di sicurezza possono solo essere letti in modalità operativa di sicurezza.

Processo di creazione delle tabelle di animazione nello spazio dei nomi di processo o sicuro in Control Expert

Control Expert fornisce due modi per creare tabelle di animazione per lo spazio dei nomi di processo o sicuro:

- Da una finestra della sezione codice di sicurezza o processo, fare clic con il pulsante destro del mouse nella finestra codice, quindi selezionare:
 - **Inizializza Tabella di animazione** per aggiungere l'oggetto dati a una tabella di animazione esistente nello spazio dei nomi sicuro o di processo, oppure
 - **Inizializza nuova tabella di animazione** per aggiungere l'oggetto dati a una nuova tabella di animazione nello spazio dei nomi sicuro o di processo.

In ciascun caso, tutte le variabili nella sezione codice vengono aggiunte alla tabella di animazione nuova o esistente.

- Dal **Browser di progetto**, nell'area dati sicura o processo, fare clic con il pulsante destro del mouse sulla cartella **Tabelle di animazione**, quindi selezionare **Nuova tabella di animazione**. Control Expert crea una nuova tabella di animazione vuota. È quindi possibile aggiungere singole variabili dallo spazio dei nomi (sicurezza o processo) correlato alla tabella.

Processo per creare tabelle di animazioni con ambito globale

Creare una tabella di animazione globale nel **Browser di progetto** facendo clic con il pulsante destro del mouse sulla cartella **Tabelle di animazione** globali, quindi selezionando **Nuova tabella di animazione**. È possibile aggiungere variabili alla nuova tabella di animazione in modi diversi:

- *Trascinamento della selezione*: è possibile trascinare una variabile da un editor dati e rilasciarla nella tabella di animazione globale. Poiché l'ambito della tabella di animazione comprende l'intera applicazione, è possibile trascinare la variabile dall'**Editor dati di sicurezza**, dall'**Editor dati processo** o dall'**Editor dati globali**.
- *Finestra di dialogo Selezione istanza*: è possibile fare doppio clic in una riga nella tabella di animazione, quindi fare clic sul pulsante con i puntini per aprire la finestra di dialogo **Selezione istanza**. Utilizzare l'elenco di filtraggio nella parte in alto a destra della finestra di dialogo per selezionare una delle seguenti aree di progetto:
 - SICURO: per visualizzare gli oggetti dati associati all'area di sicurezza.
 - PROCESSO: per visualizzare gli oggetti dati associati all'area di processo.
 - APPLICAZIONE: per visualizzare gli oggetti dati di ambito applicazione di più alto livello.

Selezionare un oggetto dati, quindi fare clic su **OK** per aggiungere la voce alla tabella di animazione.

NOTA: Oggetti dati aggiunti a una tabella di animazione globale da:

- Area Processo hanno il prefisso "PROCESS" che precede il nome della variabile (ad esempio PROCESS.variable_01)
- Area Sicurezza hanno il prefisso "SAFE" che precede il nome della variabile (ad esempio SAFE.variable_02)
- L'area Globale non ha alcun prefisso aggiunto al nome della variabile.

Visualizzazione dei dati sulle schermate operatore

È possibile visualizzare i dati su una schermata dell'operatore, ad esempio un'applicazione HMI, SCADA o FactoryCast, nello stesso modo in cui si collegano i dati in una tabella di animazione. Le variabili dati disponibili per la selezione sono quelle incluse nel dizionario dati di Control Expert.

È possibile attivare il dizionario dati aprendo la finestra **Strumenti > Impostazioni progetto...**, quindi nell'area **Ambito > comune** della finestra, selezionando **Generale > Dati integrati PLC > Dizionario dati**.

Il dizionario dati rende le variabili dati disponibili nelle schermate operatore come segue:

- Le variabili dello spazio dei nomi sicuro includono sempre il prefisso “SAFE” e possono essere raggiunte solo mediante il formato “SAFE.<nome della variabile>”.
- Le variabili dello spazio dei nomi applicazione o globale non comprendono prefisso e possono essere raggiunte solo utilizzando il “<nome variabile>” senza prefisso.
- L'impostazione **Uso dello spazio dei nomi di processo** determina come una schermata operatore può raggiungere le variabili dello spazio dei nomi Processo.
 - Se si seleziona **Uso dello spazio dei nomi di processo**, la schermata dell'operatore può leggere le variabili dell'area processo solo mediante il formato “PROCESS.<nome della variabile>”.
 - Se si deseleziona **Uso dello spazio dei nomi di processo**, la schermata dell'operatore può leggere le variabili dell'area processo solo mediante il formato “<nome variabile>” senza il prefisso PROCESS.

NOTA: Se si dichiarano due variabili con lo stesso nome, una nello spazio dei nomi Processo e l'altra nello spazio dei nomi Globale, solo la variabile dello spazio dei nomi Globale è accessibile da un'applicazione HMI, SCADA o Factory Cast.

È possibile utilizzare la finestra di dialogo **Selezione istanza** per accedere ai singoli oggetti dati.

▲ ATTENZIONE

VALORE IMPREVISTO DELLA VARIABILE

- Verificare che l'applicazione presenti le corrette impostazioni di progetto.
- Verificare la sintassi per accedere alle variabili nei diversi spazi dei nomi.

Il mancato rispetto di queste istruzioni può provocare infortuni o danni alle apparecchiature.

Per evitare di accedere alla variabile errata:

- Utilizzare nomi diversi per le variabili dichiarate nello spazio dei nomi Processo e nello spazio dei nomi Globale, oppure

- Selezionare **Uso dello spazio dei nomi di processo** e utilizzare la seguente sintassi per accedere alle variabili con lo stesso nome:
 - “PROCESS.<nome variabile>” per le variabili selezionate nello spazio dei nomi Processo.
 - “<nome variabile>” senza prefisso per le variabili dichiarate nello spazio dei nomi Globale

Strumento di trending

Lo strumento di trending di Control Expert non è supportato per l'uso con un progetto di sicurezza M580.

Aggiunta di sezioni codice

Aggiunta di codice a un processo di sicurezza M580

Operazioni con i task in Control Expert

Nello spazio dei nomi di processo, Control Expert include il task MAST per impostazione predefinita. Il task MAST non può essere eliminato. Tuttavia, è possibile aggiungere i task FAST, AUX0 e AUX1. Tenere presente che la creazione di un task nella parte processo di un progetto di sicurezza è analoga alla creazione di un task in un progetto non di sicurezza. Per ulteriori informazioni, vedere l'argomento *Creazione e configurazione di un task* nel manuale *EcoStruxure™ Control Expert - Modalità operative*.

Nello spazio dei nomi sicuro, per impostazione predefinita, Control Expert include il task SAFE. Il task SAFE non può essere rimosso e non è possibile aggiungere altri task alla sezione **Sicurezza programma** del **Browser di progetto** in Control Expert. È possibile aggiungere più sezioni al task SAFE.

Configurazione delle proprietà del task SAFE

Il task SAFE supporta solo l'esecuzione del task periodico (l'esecuzione ciclica non è supportata). Le impostazioni **Periodo** e **Watchdog** del task SAFE vengono immesse nella finestra di dialogo **Proprietà di SAFE** e supportano il seguente campo di valori:

- Periodo task SAFE: 10...255 ms con valore predefinito di 20 ms.
- Watchdog task SAFE: 10...500 ms, in incrementi di 10 ms, con un valore predefinito di 250 ms.

Impostare il task SAFE **Periodo** a un valore minimo in base alla dimensione dati sicuri e al modello di PLC. Il periodo minimo del task SAFE può essere calcolato con le formule seguenti:

- Minimo assoluto necessario per la comunicazione sicura degli I/O:
 - 10 ms
- Tempo (in ms) necessario per trasferire e confrontare i dati sicuri tra la CPU e il COPRO:
 - $(0,156 \times \text{Dimensione_dati_sicuri}) + 2$ ms (per BMEP584040S, BMEP586040S, BMEH584040S e BMEH586040S)
 - $(0,273 \times \text{Dimensione_dati_sicuri}) + 2$ ms (per BMEP582040S e BMEH582040S)

Dove Dimensione_dati_sicuri è la dimensione in KB dei dati sicuri.

- Tempo aggiuntivo (in ms) richiesto dai PAC Hot Standby per trasferire i dati sicuri dal PAC primario al PAC di standby:
 - $(K1 \times \text{Task}_{kb} + K2 \times \text{Task}_{DFB}) / 500$

In questa formula:

- Task_{DFB} = il numero di DFB dichiarati nella parte sicura dell'applicazione.
- Task_{kb} = la dimensione (in KB) dei dati sicuri scambiati dal task SAFE tra i PAC primario e di standby.
- K1 e K2 sono costanti, con valori determinati dal modulo CPU specifico utilizzato nell'applicazione:

Coefficiente	BMEH582040S	BMEH584040S e BMEH586040S
K1	32,0	10,0
K2	23,6	7,4

NOTA:

- Il valore prodotto da queste formule è un minimo assoluto per il periodo del task SAFE valido solo per una prima valutazione del limite del tempo di ciclo SAFE. Non comprende il tempo necessario per l'esecuzione del codice utente o per il margine necessario per il funzionamento previsto del sistema multi-task del PAC. Consultare l'argomento Considerazioni sul throughput del sistema in *Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente*.
- Per impostazione predefinita, Dimensione_dati_sicuri e Size_{kbyte} sono uguali. È possibile visualizzarne i valori, rispettivamente, nel menu **PLC > Consumo di memoria** e nella schermata **PLC > Hot Standby**.

Calcoli di esempio

I risultati di esempio del calcolo del periodo minimo del task SAFE sono indicati di seguito

Periodo minimo task SAFE (ms)					
Size_{kbyte}^1	Nb_{DFB_Inst}	BMEP582040S	BMEP584040S oppure BMEP586040S	BMEH582040S	BMEH584040S oppure BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29
200	10	57	33	70	37

Periodo minimo task SAFE (ms)					
Size _{kbyte} ¹	Nb _{D_{FB}_Inst}	BMEP582040S	BMEP584040S oppure BMEP586040S	BMEH582040S	BMEH584040S oppure BMEH586040S
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179

1. Si suppone che Dimensione_{kbyte} e Dimensione_{dati_sicuri} siano uguali.

NOTA: Configurare il watchdog del task SAFE con un valore maggiore del **Periodo** del task SAFE.

Consultare l'argomento *Tempo di sicurezza del processo*, pagina 154, per informazioni su come la configurazione del task SAFE influisce sul tempo di sicurezza del processo.

Consultare l'argomento *Task PAC M580 Safety*, pagina 271 per informazioni sulla descrizione della priorità di esecuzione del task SAFE.

Creazione di sezioni codice

Fare clic con il pulsante destro del mouse sulla cartella **Sezione** di un task e selezionare **Nuova sezione...** per aprire una finestra di dialogo di configurazione. Per i task di sicurezza e processo, sono disponibili i seguenti linguaggi di programmazione:

Linguaggio	Task di sicurezza	Task di processo			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
segmento LL984	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓: disponibile –: non disponibile					

Tranne queste limitazioni sulla disponibilità del linguaggio di programmazione per il task SAFE, la finestra di dialogo di configurazione Nuova sezione ha la stessa funzionalità per un progetto non di sicurezza M580. Per ulteriori informazioni, vedere l'argomento *Finestra di dialogo delle proprietà per sezioni FBD, LD, IL o ST* nel manuale *EcoStruxure™ Control Expert - Modalità operative*.

Aggiunta di dati alle sezioni di codice

Poiché il task SAFE è separato dai task di processo, solo i dati accessibili nell'**Editor dati di sicurezza** sono disponibili per l'aggiunta a una sezione di codice del task SAFE. Tali dati comprendono:

- Variabili di sicurezza non identificate (ossia senza indirizzo %M o %MW) create nell'**Editor dati di sicurezza**.
- Oggetti dati che fanno parte delle strutture DDT dispositivo del modulo di sicurezza M580.

Analogamente, i dati disponibili per sezioni di codice del task non di sicurezza comprendono tutti i dati nell'ambito dello spazio dei nomi di processo. Questi comprendono tutti i dati di progetto tranne:

- Dati esclusivamente disponibili nello spazio dei nomi SAFE (vedere sopra).
- Oggetti dati creati nell'**Editor dati globali**.

Analisi del codice

Quando si analizza o crea un progetto, Control Expert visualizza un messaggio di errore rilevato se:

- I dati appartenenti allo spazio dei nomi di processo sono inclusi nel task SAFE.
- I dati appartenenti allo spazio dei nomi sicuro sono inclusi in un task di processo (MAST, FAST, AUX0, AUX1).
- Bit (%M) o parole (%MW) identificati sono inclusi in una sezione del task SAFE.

Richiesta diagnostica

Introduzione

La richiesta diagnostica è disponibile solo per alimentatori di sicurezza M580 situati su un rack principale utilizzando il blocco funzione PWS_DIAG. Un rack principale è un rack con indirizzo 0 e una CPU o un modulo adattatore di comunicazione (CRA) nello slot 0 o 1. Un rack di estensione non è un rack principale.

La CPU può effettuare una richiesta diagnostica di alimentatori ridondanti sul rack locale e, tramite un modulo adattatore di comunicazione (CRA), di alimentatori ridondanti su un rack remoto. Se gli alimentatori master e slave sono funzionanti, l'alimentatore master entra in modalità diagnostica master e l'alimentatore slave entra in modalità diagnostica slave. I LED indicano che il test è in corso.

NOTA: Questa richiesta non è implementata all'accensione (Power On)

Una volta terminato il test di diagnostica, il master torna allo stato operativo normale e lo slave passa allo stato normale o di errore a seconda dei risultati dei test. I risultati dei test vengono archiviati nella memoria degli alimentatori.

Dati restituiti dalla richiesta diagnostica

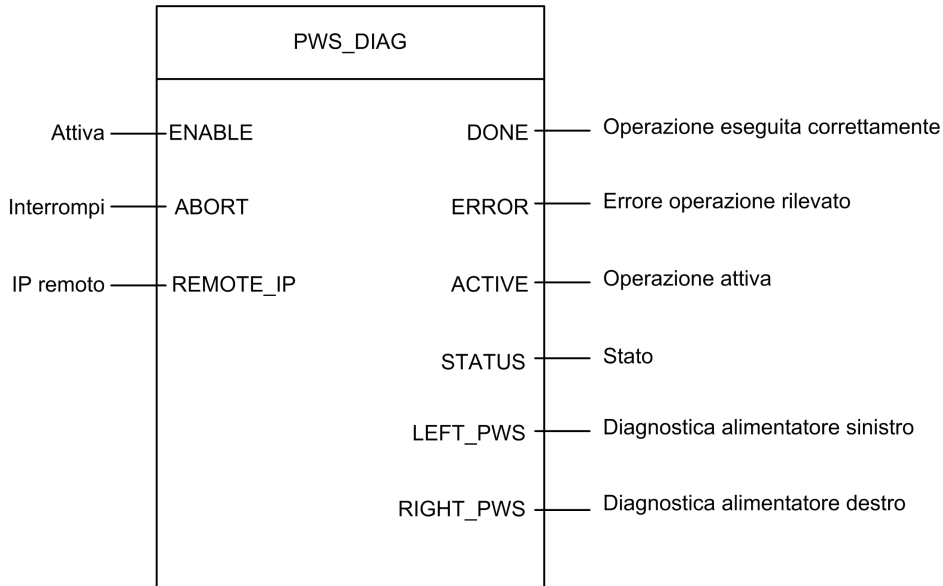
Le informazioni di diagnostica inviate alla CPU dagli alimentatori sono le seguenti:

- Temperatura ambiente dell'alimentatore.
- Tensione e corrente sulla linea backplane 3,3V.
- Tensione e corrente sulla linea backplane 24V.
- Energia cumulata totale dell'alimentatore dalla data di fabbricazione sulle linee backplane 3,3V e 24V.
- Tempo operativo come master dall'ultima accensione e dal momento della produzione
- Tempo operativo come master dall'ultima accensione e dalla produzione.
- Durata di vita residua in percentuale (LTPC): il tempo che intercorre prima della manutenzione preventiva, dal 100% allo 0%.

NOTA: Nessuna sostituzione a 0%.

- Numero di volte in cui l'alimentatore è stato inserito.
NOTA: Dda SCADA è possibile resettare il numero di inserzioni dal momento dell'installazione ed effettuare tutte le altre operazioni di diagnostica.
- Numero di volte in cui la tensione principale BMXCPS4002S è scesa sotto il livello di sottotensione 1 (95 Vca).
- Numero di volte in cui la tensione principale BMXCPS4002S è salita oltre il livello di sovratensione 2 (195 Vca).
- Numero di volte in cui la tensione principale BMXCPS4022S è scesa sotto il livello di sottotensione 1 (20 Vcc).
- Numero di volte in cui la tensione principale BMXCPS4022S è salita oltre il livello di sovratensione 2 (40 Vcc).
- Numero di volte in cui la tensione principale BMXCPS3522S è scesa sotto il livello di sottotensione 1 (110 Vcc).
- Numero di volte in cui la tensione principale BMXCPS3522S è salita oltre il livello di sovratensione 2 (140 Vcc).
- Stato corrente dell'alimentatore (master/slave/non funzionante).

Rappresentazione in FBD



Parametri

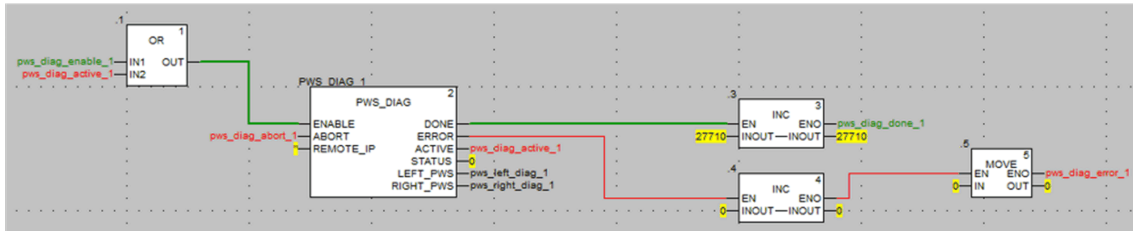
Parametri di ingresso:

Nome parametro	Tipo di dati	Descrizione
ENABLE	BOOL	Quando è ON, l'operazione è attivata.
ABORT	BOOL	Quando è ON, l'operazione corrente viene interrotta.
REMOTE_IP	STRING	Indirizzo IP ("ip1.ip2.ip3.ip4") della derivazione che contiene il modulo alimentatore. Lasciare in questo campo una stringa vuota ("") oppure non associare alcuna variabile al relativo contatto per indirizzare l'alimentatore nel rack locale.

Parametri di uscita:

Nome parametro	Tipo di dati	Descrizione
DONE	BOOL	ON quando l'operazione viene conclusa correttamente.
ERROR	BOOL	ON quando l'operazione non è eseguita correttamente e viene interrotta.
ACTIVE	BOOL	ON quando l'operazione è attiva.
STATUS	WORD	Identificatore errore rilevato.
LEFT_PWS	ANY	Dati diagnostici per alimentatore sinistro. Utilizzare una variabile di tipo PWS_DIAG_DDT_V2, pagina 136 per un'interpretazione corretta.
RIGHT_PWS	ANY	Dati diagnostici per alimentatore destro. Utilizzare una variabile di tipo PWS_DIAG_DDT_V2 per un'interpretazione corretta.

Esempio



pws_left_diag_1		PWS_DIAG_DDT	
pws_right_diag_1		PWS_DIAG_DDT	
● PwsMajorVersion	153	BYTE	Power Supply major version
● PwsMinorVersion	162	BYTE	Power Supply minor version
● Model	0	BYTE	Power Supply Model identifier
● State	12	BYTE	Power Supply state
● I33BacPos	0	UINT	Measure current of 3V3 Bac in nominal role (producer)
● V33Buck	0	UINT	Measure voltage of 3V3 Buck
● I24Bac	0	UINT	Measure current of 24V Bac
● V24Int	0	UINT	Measure voltage of 24V Int
● Temperature	0	INT	Measure of Ambient Temperature
● OperTimeMaster...	16935	DINT	Operating Time as Master since last Power ON
● OperTimeSlaveSi...	2	DINT	Operating Time as Slave since last Power ON
● OperTimeMaster	282128	DINT	Operating Time as Master since Manufacturing
● OperTimeSlave	44	DINT	Operating Time as Slave Since Manufacturing
● Work	0	DINT	Work supplied since Manufacturing
● RemainingLTPC	0	UINT	Remaining Life Time in percent
● NbPowerOn	0	UINT	Number of Power ON since Manufacturing
● NbVoltageLowFail	0	UINT	Number of failure detected on Primary Voltage by Low Threshold
● NbVoltageHighFail	0	UINT	Number of failure detected on Primary Voltage by High Threshold

Comandi Scambia e Azzera

Introduzione

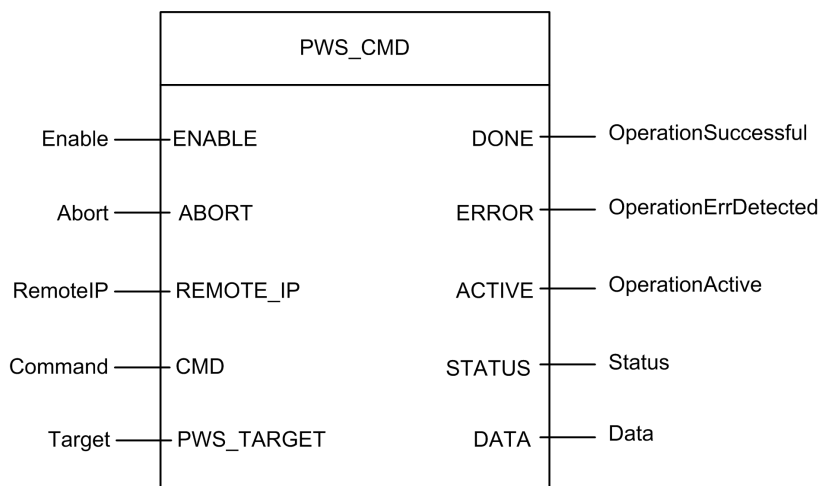
Il blocco funzione PWS_CMD può essere utilizzato per emettere due comandi:

- Richiesta Scambia: questo comando richiede all'alimentatore di operare come master. Se sono operativi entrambi gli alimentatori, l'alimentatore specificato diventa il master e l'altro diventa lo slave.
- Richiesta Azzera: questo comando azzera i contatori del numero di volte in cui:
 - la tensione principale è scesa sotto il livello di sottotensione 1.
 - la tensione principale è scesa sotto il livello di sottotensione 2.
 - l'alimentatore è stato inserito.

Entrambe le richieste sono disponibili solo per gli alimentatori che si trovano nel rack principale. Un rack principale è un rack con indirizzo 0 e una CPU o un modulo adattatore di comunicazione (CRA) nello slot 0 o 1. Un rack di estensione non è un rack principale.

I LED indicano che il comando è in corso. Una registrazione dell'evento viene memorizzata nell'alimentatore.

Rappresentazione in FBD



Parametri

Parametri di ingresso:

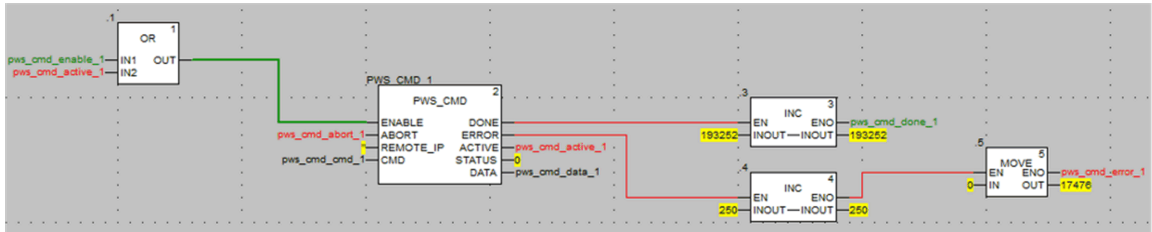
Nome parametro	Tipo di dati	Descrizione
ENABLE	BOOL	Quando è ON, l'operazione è attivata.
ABORT	BOOL	Quando è ON, l'operazione corrente viene interrotta.
REMOTE_IP	STRING	Indirizzo IP ("ip1.ip2.ip3.ip4") della derivazione che contiene il modulo alimentatore. Lasciare in questo campo una stringa vuota (""), oppure non associare alcuna variabile al relativo contatto per indirizzare l'alimentatore nel rack locale.
CMD	ANY	Usare una variabile di tipo PWS_CMD_DDT per un'interpretazione corretta. Codice di comando disponibile: <ul style="list-style-type: none"> • 1 = Scambia • 3 = Azzera
PWS_TARGET	BYTE	Alimentatore da indirizzare: <ul style="list-style-type: none"> • 1 = sinistro • 2 = destro • 3 = entrambi

Parametri di uscita:

Nome parametro	Tipo di dati	Descrizione
DONE	BOOL	ON quando l'operazione viene conclusa correttamente.
ERROR	BOOL	ON quando l'operazione non è eseguita correttamente e viene interrotta.
ACTIVE	BOOL	ON quando l'operazione è attiva.
STATUS	WORD	Identificatore errore rilevato.
DATA	ANY	Dati di risposta (a seconda del codice di comando)- Nessun dato segnalato per i comandi di scambio e azzeramento.

Esempio

Il seguente diagramma descrive un blocco PWS_CMD utilizzato per una richiesta di scambio:



La seguente schermata dell'editor di dati mostra i valori delle variabili di una richiesta di scambio:

Name	Value	Type	Comment
pws_cmd_enable_1	1	BOOL	
pws_cmd_abort_1	0	BOOL	
pws_cmd_active_1	0	BOOL	
pws_cmd_done_1	1	BOOL	
pws_cmd_error_1	0	BOOL	
pws_cmd_status_1	16#0000	WORD	
pws_cmd_last_error_1	16#4444	WORD	
pws_cmd_OKCount_1	195842	DINT	
pws_cmd_KOCount_1	251	DINT	
pws_cmd_cmd_1		PWS_CMD_DDT	
Code	3	BYTE	Command code: 1 = swap, 3 = clear, etc.
Pws Target	2	BYTE	Power supply target: 1 for left, 2 for right, 3 for both
pws_cmd_ip_str_1	''	string[64]	
pws_cmd_data_1		PWS_DATA_DDT	

Gestione della sicurezza dell'applicazione

Introduzione

Control Expert consente di limitare l'accesso al PAC di sicurezza M580 agli utenti con password assegnate. Questa sezione fa riferimento ai processi di assegnazione password disponibili in Control Expert.

Protezione dell'applicazione

Panoramica

Control Expert fornisce un meccanismo di password che consente di proteggere dall'accesso non autorizzato all'applicazione.

Control Expert utilizza la password quando:

- Si apre l'applicazione in Control Expert.
- Si collega il PAC in Control Expert.

L'impostazione della password di un'applicazione impedisce la modifica, il download o l'apertura indesiderati dei file dell'applicazione. La password è memorizzata nell'applicazione in modo codificato.

Oltre a impostare la password, è possibile crittografare i file `.STU`, `.STA` e `.ZEF`. La funzione di crittografia dei file di Control Expert impedisce modifiche da parte di persone malintenzionate e rafforza la protezione contro il furto della proprietà intellettuale. L'opzione di crittografia file è protetta da un meccanismo di password.

NOTA: Quando un controller viene gestito come parte di un progetto di sistema, la password dell'applicazione e la crittografia dei file vengono disattivate nell'editor Control Expert e devono essere gestite mediante Gestore topologia.

Creazione della password

La creazione della password è basata sulle raccomandazioni dello standard IEEE 1686-2013.

Una password deve contenere almeno 8 caratteri e deve essere costituita da almeno un carattere maiuscolo (A, B, C, ...), uno minuscolo (a, b, c, ...), un numero e un carattere non alfanumerico (!, \$, %, &, ...).

NOTA: quando si esporta un progetto non crittografato in un file `.XEF` o `.ZEF`, la password dell'applicazione viene cancellata.

Creazione di un nuovo progetto

Per impostazione predefinita, un progetto non è protetto da password e i file dell'applicazione non sono crittografati.

Durante la creazione del progetto, la finestra **Applicazione sicurezza** consente di:

- Impostare una password dell'applicazione, oppure
- Impostare una password dell'applicazione e applicare la crittografia ai file dell'applicazione. L'applicazione della crittografia dei file richiede anche l'impostazione di una password e si consiglia di impostare due password diverse.

Se non viene immessa alcuna password, la crittografia dei file dell'applicazione non è possibile. In questo caso, alla successiva apertura del progetto Control Expert, si apre la finestra di dialogo **Password**. Per accedere al progetto, non immettere testo per la password, accettando così la stringa vuota e fare clic su **OK**. Successivamente, è possibile seguire la procedura descritta di seguito per impostare una password dell'applicazione e attivare la crittografia dei file.

NOTA: è possibile creare o modificare la password di un'applicazione in qualsiasi momento.

L'impostazione della password di un'applicazione è obbligatoria per attivare la crittografia dei file.

Quando la crittografia file è attivata:

- La modifica della password dell'applicazione è consentita.
- La cancellazione della password dell'applicazione non è consentita.

Impostazione di una password dell'applicazione

Procedura per impostare la password dell'applicazione:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Applicazione , fare clic su Cambia password . Risultato: viene visualizzata la finestra Modifica password .
5	Immettere la nuova password nel campo Immissione .
6	Confermare la nuova password nel campo Conferma .

Passaggio	Azione
7	Fare clic su OK per confermare.
8	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Modifica della password dell'applicazione

Procedura per la modifica della password di protezione dell'applicazione:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Applicazione , fare clic su Cambia password . Risultato: viene visualizzata la finestra Modifica password .
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Eliminazione della password dell'applicazione

La cancellazione della password dell'applicazione non è consentita se è abilitata la crittografia dei file.

Procedura per l'eliminazione della password di protezione dell'applicazione:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Applicazione , fare clic su Cancella password... Risultato: viene visualizzata la finestra Password .
5	Immettere la password nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Funzione di blocco automatico

È disponibile una funzione facoltativa di blocco automatico per la limitazione dell'accesso allo strumento di programmazione software Control Expert dopo un periodo di inattività preconfigurato. È possibile attivare la funzione di blocco automatico con la casella di controllo **Blocco automatico** e selezionare il timeout per il periodo di inattività tramite **Minuti prima del blocco**.

I valori predefiniti sono:

- **Blocco automatico** non è attivato
- **Minuti prima del blocco** è impostato a 10 minuti (valori possibili: 1...999 minuti)

Se la funzione di blocco automatico è attivata e il tempo configurato scade, viene visualizzata una finestra di dialogo modale che richiede l'inserimento della password dell'applicazione. Dietro questa finestra di dialogo modale, tutti gli editor aperti non si chiudono e restano nella stessa posizione. Di conseguenza, chiunque può leggere il contenuto corrente delle finestre di Control Expert, ma non può continuare a utilizzare Control Expert.

NOTA: Se non è stata assegnata alcuna password al progetto, la finestra di dialogo modale non viene visualizzata.

Condizione di richiesta password

Aprire un'applicazione (progetto) esistente in Control Expert:

Gestione della password	
Quando si apre un file applicazione, viene visualizzata una finestra di dialogo Password applicazione .	
Immettere la nuova password.	
Fare clic su OK .	Se la password è corretta, l'applicazione si apre.
	Se la password è errata, un messaggio indica l'inserimento di una password errata e si apre una nuova finestra di dialogo Password applicazione .
Se si fa clic su Annulla , l'applicazione non viene aperta	

Accesso all'applicazione in Control Expert dopo un blocco automatico, quando Control Expert non è collegato al PAC o quando il progetto in Control Expert è UGUALE al progetto nel PAC:

Gestione della password	
Una volta scaduto il tempo del blocco automatico, viene visualizzata la finestra di dialogo Password applicazione :	
Immettere la nuova password.	
Fare clic su OK .	Se la password è corretta, Control Expert diventa nuovamente attivo.
	Se la password è errata, un messaggio indica l'inserimento di una password errata e si apre una nuova finestra di dialogo Password applicazione .
Facendo clic su Chiudi , l'applicazione viene chiusa senza essere salvata.	

Accesso all'applicazione nel PAC dopo un blocco automatico, quando Control Expert è collegato al PAC e l'applicazione in Control Expert è DIVERSA da quella nel PAC:

Gestione della password	
Alla connessione, se l'applicazione software Control Expert e l'applicazione della CPU non sono uguali, viene visualizzata una finestra di dialogo Password applicazione :	
Immettere la nuova password.	
Fare clic su OK .	Se la password è corretta viene stabilito il collegamento.
	Se la password è errata, un messaggio indica l'inserimento di una password errata e si apre una nuova finestra di dialogo Password applicazione .
Se si fa clic su Annulla , non viene stabilito il collegamento.	
NOTA: Alla connessione, se l'applicazione software Control Expert e l'applicazione della CPU sono uguali, non viene richiesta la password. Se inizialmente non è stata immessa alcuna password (cioè se è stata lasciata vuota alla creazione del progetto), fare clic su OK per stabilire il collegamento alla richiesta della password.	

NOTA: Dopo tre tentativi con password errata, occorre attendere un intervallo di tempo crescente tra ogni nuovo tentativo di inserimento della password. Il periodo di attesa aumenta da 15 secondi a 1 ora, con l'incremento che aumenta di un fattore di 2 dopo ogni tentativo non riuscito con password errata.

NOTA: In caso di perdita della password, vedere la procedura descritta nel capitolo *Perdita della password*, pagina 320.

Abilitazione dell'opzione di crittografia file

NOTA: È necessario impostare una password dell'applicazione prima di attivare la crittografia file.

Procedura per attivare l'opzione di crittografia file:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Selezionare la casella di controllo Crittografia file attiva . Risultato: viene visualizzata la finestra Crea la password .
5	Immettere la password nel campo Immissione .
6	Confermare la password nel campo Conferma .
7	Fare clic su OK per confermare.
8	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Disabilitazione dell'opzione di crittografia file

Procedura per disabilitare l'opzione di crittografia file:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa.

Passaggio	Azione
	Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Deselezionare la casella di controllo Crittografia file attiva . Risultato: viene visualizzata la finestra Password crittografia file .
5	Immettere la password e fare clic su OK per confermare. NOTA: L'applicazione non è più crittografata.
6	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Modifica della password di crittografia file

Procedura per la modifica della password di crittografia file:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Crittografia file , fare clic su Modifica password... Risultato: viene visualizzata la finestra Modifica password .
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Cancellazione della password di crittografia file

Procedura per la cancellazione della password di crittografia file:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Crittografia file , fare clic su Cancella password... Risultato: viene visualizzata la finestra Password .
5	Immettere la password nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

NOTA: In caso di perdita della password di crittografia file, vedere la procedura descritta nel capitolo *Perdita della password*, pagina 320.

Regole di compatibilità

Non è possibile aprire i file di applicazione crittografati (.STA e .ZEF) in Control Expert 15.0 Classic o precedenti e i file crittografati (.ZEF) non possono essere importati in Control Expert con Gestore topologia.

Le regole di compatibilità tra la versione dell'applicazione e la versione di Control Expert/Unity Pro si applicano ai file .ZEF esportati senza l'opzione di crittografia.

NOTA: Se l'opzione di crittografia file nel progetto è attivata, i file di applicazione archiviati (.STA) non possono essere salvati senza crittografia.

Protezione con password dell'area sicura

In breve

Le CPU Safety comprendono una funzione di protezione tramite password dell'area sicura, accessibile dalla schermata **Proprietà** del progetto. Questa funzione consente di proteggere gli elementi posizionati nell'area sicura di un progetto di sicurezza.

NOTA: Quando la funzione di protezione tramite password dell'area sicura è attiva, le parti sicure dell'applicazione non possono essere modificate

Le modifiche alle parti seguenti dell'area sicura non sono consentite quando è attivata la protezione tramite password dell'area sicura:

Parte sicura	Azione vietata (offline E online)
Configurazione	Modificare le caratteristiche della CPU
	Aggiungere, eliminare, modificare un modulo di sicurezza nel rack
	Modificare un alimentatore di sicurezza
Tipi	Creare, eliminare, modificare un DDT di sicurezza
	Cambiare un attributo DDT: da non sicuro->sicuro
	Cambiare un attributo DDT: da sicuro->non sicuro
	Creare, eliminare, modificare un DFB di sicurezza
	Cambiare un attributo DFB: da non sicuro->sicuro
	Cambiare un attributo DFB: da sicuro->non sicuro
Programma SAFE	Eventuali modifiche nel nodo Variabili e istanze FB
	Creare task
	Importare task
	Modificare task
	Creare sezione
	Eliminare sezione
	Importare sezione
	Modificare sezione
Impostazioni progetto	Modificare impostazioni di progetto SAFE
	Modificare impostazioni di progetto COMMON

Crittografia

La password dell'area sicura utilizza la crittografia standard SHA-256 con un salt.

Funzione password area sicura rispetto ad autorizzazioni utente progetto di sicurezza

L'attivazione della password dell'area sicura e l'implementazione delle autorizzazioni utente create nell'**Editor di sicurezza** sono funzioni di sicurezza mutuamente esclusive, come segue:

- Se all'utente che lancia Control Expert è stato assegnato un profilo utente, tale utente può accedere alle aree sicure dell'applicazione di sicurezza se conosce la password dell'area sicura e gli sono state concesse le autorizzazioni di accesso nell'**Editor di sicurezza**.
- Se i profili utente non sono stati assegnati, un utente può accedere alle aree sicure dell'applicazione di sicurezza se conosce la password dell'area sicura.

Indicatori visivi in Control Expert

Lo stato della funzione di protezione dell'area sicura può essere rilevato visivamente tramite il nodo **Programma-SAFE** nel **Browser del progetto**:

- Un lucchetto chiuso indica che è stata creata e attivata una password dell'area sicura.
- Un lucchetto aperto indica che è stata creata ma non attivata una password dell'area sicura.
- Nessun lucchetto indica che non è stata creata alcuna password dell'area sicura.

NOTA: Se la password dell'area sicura è stata creata ma non attivata e l'applicazione di sicurezza viene chiusa e riaperta, la password dell'area sicura viene attivata automaticamente alla riapertura. Questo comportamento serve da precauzione se la password dell'area sicura non è stata riattivata involontariamente.

Compatibilità

La funzionalità della password dell'area sicura è disponibile per Control Expert V14.0 o successive, per CPU M580 di sicurezza con firmware 2.80 o successivo.

NOTA:

- I file .STU, .STA e .ZEF del programma applicazione, creati in Control Expert V14.0 o successivi, non possono essere aperti in Unity Pro V13.1 e versioni precedenti.
- La sostituzione di una CPU M580 Safety in un'applicazione Control Expert v14.0 ha l'effetto seguente:
 - L'aggiornamento dal firmware 2.70 a 2.80 (o successivi) aggiunge la funzionalità della password dell'area sicura alla scheda **Protezione programma e Safety** della finestra **Progetto > Proprietà**.
 - Il downgrade dal firmware 2.80 (o successivi) a 2.70 rimuove la funzionalità della password dell'area sicura.

Attivazione della protezione e creazione della password

Procedura per l'attivazione delle sezioni e la creazione della password:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nell'area Safety , attivare la protezione selezionando la casella di Protezione attiva . Risultato: viene visualizzata la finestra di dialogo Modifica password .
5	Specificare una password nel campo Immissione .
6	Confermare la password nel campo Conferma .
7	Fare clic su OK per confermare.
8	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Modifica della password

Procedura per modificare la password di protezione delle sezioni del progetto:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nell'area Safety , fare clic su Cambia password Risultato: viene visualizzata la finestra di dialogo Modifica password :
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Eliminazione della password

Procedura per eliminare la password di protezione delle sezioni del progetto:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nell'area Safety , fare clic su Azzerà password.... Risultato: viene visualizzata la finestra di dialogo Controllo accesso :
5	Immettere la password precedente nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Protezione di Unità programma, sezione e subroutine

In breve

La funzione di protezione è accessibile dalla schermata **Proprietà** del progetto in modalità offline.

Questa funzione permette di proteggere gli elementi del programma (sezioni, Unità programma).

NOTA: la protezione non è attiva finché la protezione non viene attivata nel progetto.

NOTA: la protezione del progetto è attiva solo per gli elementi di programma contrassegnati. Ciò non impedisce le seguenti operazioni:

- Collegamento al PLC
- Caricamento di un'applicazione dalla CPU
- Modifica della configurazione
- Aggiunta di nuove Unità programma e/o sezioni
- Modifica della logica in una nuova sezione (non protetta)

Attivazione della protezione e creazione della password

Procedura per attivare la protezione e creare la password per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nel campo Unità programma e sezioni , attivare la protezione selezionando la casella di controllo Protezione attiva . Risultato: viene visualizzata la finestra di dialogo Modifica password :
5	Specificare una password nel campo Immissione .
6	Confermare la password nel campo Conferma .
7	Selezionare la casella di controllo Criptata se è necessaria un'ulteriore protezione mediante password. NOTA: un progetto con una password criptata non può essere modificato con Unity Pro V4.0 e versioni precedenti.

Passo	Azione
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Note:

Se un elemento di programma è configurato con una protezione (lettura o lettura/scrittura), la protezione attiva viene indicata da un lucchetto chiuso al livello della sezione.

Se l'elemento di programma è configurato con una protezione ma la protezione è disabilitata, al livello dell'elemento di programma viene visualizzato un lucchetto aperto.

Modifica della password

Procedura per cambiare la password di protezione progetto per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nel campo Unità programma e sezioni , fare clic su Modifica password... Risultato: viene visualizzata la finestra di dialogo Modifica password :
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Selezionare la casella di controllo Criptata se è necessaria un'ulteriore protezione mediante password. NOTA: un progetto con una password criptata non può essere modificato con Unity Pro V4.0 e versioni precedenti. Unity Pro è il nome precedente di Control Expert per versione 13.1 o precedenti.
9	Fare clic su OK per confermare.
10	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Eliminazione della password

Procedura per eliminare la password di protezione progetto per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione programma e Safety .
4	Nel campo Unità programma e sezioni , fare clic su Azzerà password... Risultato: viene visualizzata la finestra di dialogo Controllo accesso :
5	Immettere la password precedente nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Protezione del firmware

Panoramica

La protezione del firmware tramite password consente di impedire l'accesso non autorizzato al firmware del modulo.

Password

La password differenzia tra maiuscole e minuscole e contiene da 8 a 16 caratteri alfanumerici. La sicurezza della password è aumentata quando contiene un misto di lettere maiuscole e minuscole, caratteri alfabetici, alfanumerici e caratteri speciali.

NOTA: Quando si importa un file ZEF, la password del firmware viene memorizzata nel modulo solo se è selezionata l'opzione **Crittografia file**.

Modifica della password

È possibile modificare la password in qualsiasi momento.

NOTA: Il valore predefinito della password del firmware nell'applicazione Control Expert è: **fwdownload**.

- Per il firmware V4.01 e versioni successive, è necessario modificare il valore predefinito della password del firmware, altrimenti non sarà possibile creare l'applicazione Control Expert.
- Per le versioni del firmware precedenti alla V4.01 non è obbligatorio, ma è consigliabile modificare il valore predefinito della password del firmware.

Procedura per la modifica della password di protezione del firmware:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Firmware , fare clic su Cambia password... Risultato: viene visualizzata la finestra Modifica password .
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Ripristino della password

Se si reimposta la password, il valore predefinito viene assegnato alla password del firmware nell'applicazione Control Expert se viene confermata la password corrente.

Per reimpostare la password, procedere come segue:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .

Passaggio	Azione
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Firmware , fare clic su Azzerà password... Risultato: viene visualizzata la finestra Password .
5	Immettere la password corrente nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. La nuova password è quella predefinita: <code>fwdownload</code> . Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Protezione Web/Memorizzazione dati

Panoramica

La protezione tramite password impedisce l'accesso non autorizzato all'area di memorizzazione dati della scheda di memoria SD (se nella CPU è inserita una scheda valida).

Per le CPU Modicon M580 in un progetto creato da Control Expert con:

- Versione precedente a 15.1, è possibile fornire una protezione tramite password per l'accesso alla memorizzazione dati.
- Versione 15.1 o successiva, è possibile fornire protezione tramite password per la diagnostica Web e l'accesso alla memorizzazione dati.

Password

La password differenzia tra maiuscole e minuscole e contiene da 8 a 16 caratteri alfanumerici. La sicurezza della password è aumentata quando contiene un misto di lettere maiuscole e minuscole, caratteri alfabetici, alfanumerici e caratteri speciali.

NOTA: Quando si importa un file ZEF, la password Web/memorizzazione dati viene memorizzata all'interno del modulo solo se è selezionata l'opzione **Crittografia file**.

Modifica della password

È possibile modificare la password in qualsiasi momento.

NOTA: La password Web/memorizzazione dati ha un valore predefinito nell'applicazione Control Expert. Questo valore predefinito dipende dalla versione di Control Expert ed è:

- **datadownload** per le versioni Control Expert precedenti alla V15.1.
- **webuser** per le versioni Control Expert V15.1 e successive.

La modifica della password predefinita è obbligatoria o meno, a seconda della versione firmware del modulo:

- Per il firmware V4.01 e versioni successive, è necessario modificare il valore predefinito della password Web/memorizzazione dati, altrimenti non sarà possibile creare l'applicazione Control Expert.
- Per le versioni firmware precedenti alla V4.01 non è obbligatorio ma si consiglia di modificare il valore predefinito della password Web/memorizzazione dati.

Procedura per la modifica della password Web/memorizzazione dati:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Memorizzazione dati (o Diagnostica Web / Memorizzazione dati), fare clic su Modifica password... Risultato: viene visualizzata la finestra Modifica password .
5	Immettere la password precedente nel campo Password precedente .
6	Immettere la nuova password nel campo Immissione .
7	Confermare la nuova password nel campo Conferma .
8	Fare clic su OK per confermare.
9	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Ripristino della password

Ripristinando la password se ne assegna il valore predefinito alla password Web/memorizzazione dati nell'applicazione Control Expert se la password corrente è confermata.

Per reimpostare la password, procedere come segue:

Passaggio	Azione
1	Nel browser del progetto fare clic su Progetto .
2	Selezionare il comando Proprietà nel menu a comparsa. Risultato: viene visualizzata la finestra Proprietà del progetto .
3	Selezionare la scheda Protezione progetto e controller .
4	Nel campo Memorizzazione dati (o Diagnostica Web / Memorizzazione dati), fare clic su Azzerà password.... Risultato: viene visualizzata la finestra Password .
5	Immettere la password corrente nel campo Password .
6	Fare clic su OK per confermare.
7	Fare clic su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. La nuova password è quella predefinita: <code>dataDownload</code> . Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Perdita della password

Panoramica

Se si dimentica la password, procedere nel modo indicato nella seguenti procedure e contattare l'assistenza tecnica di Schneider Electric.

NOTA: La procedura di ripristino della password dell'applicazione varia a seconda che l'opzione di crittografia del file sia attivata o disattivata.

Password applicazione Control Expert senza opzione di crittografia file

La procedura seguente per reimpostare la password dell'applicazione è valida quando l'opzione di crittografia file è disattivata o per il file dell'applicazione gestito con Control Expert 15.0 Classic o versioni precedenti.

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme **SHIFT + F2** nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**, è necessario rispettare le condizioni seguenti:

- Al momento dell'apertura, selezionare l'applicazione; viene visualizzata la finestra di dialogo **Password**.
- Al momento del blocco automatico, viene visualizzata la finestra di dialogo **Password**. Se non si ricorda la password, selezionare **Chiudi**. Aprire di nuovo l'applicazione; viene visualizzata la finestra di dialogo **Password**.

NOTA: Se si chiude l'applicazione senza immettere una password dopo un blocco automatico, tutte le modifiche vanno perse.

Procedura per reimpostare la password dell'applicazione:

Pas-saggio	Azione
1	Condizione: viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. NOTA: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Modificare la password (vecchia password = password fornita dall'assistenza tecnica Schneider Electric).
7	Fare clic su Crea > Crea modifiche .
8	Salvare l'applicazione.

Password dell'applicazione Control Expert con opzione di crittografia file

Se si dimentica la password dell'applicazione quando la crittografia file è attivata, è necessario inviare il file dell'applicazione all'assistenza tecnica Schneider Electric. Viene quindi ricevuto il file dell'applicazione crittografata con una nuova password dell'applicazione file dall'assistenza tecnica Schneider Electric.

NOTA: Si consiglia di modificare la password dell'applicazione.

Password applicazione CPU

Procedura per reimpostare la password dell'applicazione CPU se è disponibile il rispettivo file ***.STU**:

Pas-saggio	Azione
1	Aprire il rispettivo file *.STU.
2	Quando viene visualizzata la finestra di dialogo Password , premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Modificare la password (vecchia password = password fornita dall'assistenza tecnica Schneider Electric).
7	Collegarsi al PLC.
8	Fare clic su Crea > Crea modifiche .
9	Salvare l'applicazione.

Procedura per reimpostare la password dell'applicazione *CPU* se non è disponibile il rispettivo file *.STU:

Pas-saggio	Azione
1	Condizione: al momento della connessione, viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password fornita dall'assistenza tecnica Schneider Electric è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Caricare l'applicazione dalla CPU.
7	Salvare l'applicazione.
8	Modificare la password (vecchia password = quella fornita dall'assistenza tecnica Schneider Electric).
9	Fare clic su Crea > Crea modifiche .
10	Salvare l'applicazione.

Password di crittografia file

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme **SHIFT + F2** nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Crittografia file**, fare clic su **Cancella password....** viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password di crittografia file:

Pas-saggio	Azione
1	Condizione: viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su OK per chiudere la finestra di dialogo Password .
6	Fare clic su Cambia password e cambiare la password (tenere presente che la vecchia password = password fornita dall'assistenza tecnica di Schneider Electric).
7	Fare clic su OK per chiudere la finestra di dialogo Modifica password , quindi su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Password area sicura

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme **SHIFT + F2** nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione programma e Safety**
- Nel campo **Safety**, fare clic su **Modifica password....** viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password dell'area sicura:

Pas-saggio	Azione
1	Condizione: viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su OK per chiudere la finestra di dialogo Password .
6	Fare clic su Cambia password e cambiare la password (tenere presente che la vecchia password = password fornita dall'assistenza tecnica di Schneider Electric).
7	Fare clic su OK per chiudere la finestra di dialogo Modifica password , quindi su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Password del firmware

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme **SHIFT+F2** nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Firmware**, fare clic su **Azzerà password....** viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password del firmware:

Pas-saggio	Azione
1	Condizione: viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.

Pas-saggio	Azione
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su OK per chiudere la finestra di dialogo Password .
6	Fare clic su Cambia password e cambiare la password (tenere presente che la vecchia password = password fornita dall'assistenza tecnica di Schneider Electric).
7	Fare clic su OK per chiudere la finestra di dialogo Modifica password , quindi su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Password Web/Memorizzazione dati

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme **SHIFT+F2** nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Memorizzazione dati**, fare clic su **Azzerà password....** viene visualizzata la finestra di dialogo **Password**.

Procedura per ripristinare la password della memorizzazione dei dati:

Pas-saggio	Azione
1	Condizione: viene visualizzata la finestra di dialogo Password .
2	Premere SHIFT+F2 . Risultato: si apre la finestra a comparsa Password dimenticata e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. Nota: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su OK per chiudere la finestra di dialogo Password .

Pas- saggio	Azione
6	Fare clic su Cambia password e cambiare la password (tenere presente che la vecchia password = password fornita dall'assistenza tecnica di Schneider Electric).
7	Fare clic su OK per chiudere la finestra di dialogo Modifica password , quindi su OK o Applica nella finestra Proprietà del progetto per confermare tutte le modifiche. Se si fa clic su Annulla nella finestra Proprietà del progetto , tutte le modifiche vengono annullate.

Gestione della sicurezza della workstation

Introduzione

Schneider Electric fornisce lo strumento di gestione di accesso dell'**Editor di sicurezza** utilizzabile per limitare e controllare l'accesso alla workstation su cui è installato il software Control Expert. Questa sezione descrive le funzionalità di questo strumento correlato esclusivamente ai progetti di sicurezza M580.

Gestione dell'accesso a Control Expert

Introduzione

Schneider Electric fornisce lo strumento di configurazione **Editor di sicurezza** che consente di gestire l'accesso al software Control Expert installato su una workstation. L'uso dello strumento di configurazione *Editor di sicurezza* per gestire l'accesso al software Control Expert è facoltativo.

NOTA: La gestione dell'accesso è relativa all'hardware, in genere una workstation, su cui è installato il software Control Expert e non al progetto, che dispone del proprio sistema di protezione.

Per ulteriori informazioni, consultare *EcoStruxure™ Control Expert, Editor sicurezza, Guida operativa*.

NOTA: Anche i profili utente di sicurezza richiedono autorizzazioni per accedere alla parte processo dell'applicazione di sicurezza. Quando si crea o modifica un profilo utente, occorre confermare che tutte le modifiche necessarie sono state effettuate.

Categorie di utenti

L'**Editor sicurezza** supporta due categorie di utenti:

- **Super user (Supervisor):**

Il super user è l'unico utente in grado di gestire la sicurezza di accesso al software. Il super user specifica chi può accedere al software e le rispettive autorizzazioni di accesso. Durante l'installazione di Control Expert sulla workstation, solo il super user può accedere alla configurazione di protezione senza alcuna limitazione delle autorizzazioni (senza una password).

NOTA: Il nome utente riservato al super user è Supervisor.

- **Utenti:**

Gli utenti del software vengono definiti dal super user nel relativo elenco, se l'accesso sicuro a Control Expert è attivo. L'utente, il cui nome è incluso nell'elenco utenti, può accedere a un'istanza del software immettendo il proprio nome (esattamente come appare nell'elenco) e la relativa password.

Profilo utente

Il profilo utente comprende tutte le autorizzazioni di accesso per un utente. Il profilo utente può essere personalizzato dal super user, oppure creato applicando un profilo preconfigurato fornito dallo strumento **Editor sicurezza**.

Profili utente preconfigurati

L'**Editor sicurezza** offre i seguenti profili utente preconfigurati, che si applicano al programma di sicurezza o al programma di processo:

Profilo	Tipo di programma applicabile		Descrizione
	Processo	Sicurezza	
Sola lettura	✓	✓	L'utente può accedere al progetto solo in modalità di lettura, tranne che per l'indirizzo PAC, che può essere modificato. L'utente può inoltre copiare o scaricare il progetto.
Operativo	✓	–	L'utente dispone degli stessi diritti concessi al profilo Sola lettura , a cui è stata aggiunta la possibilità di modificare i parametri di esecuzione del programma di processo (costanti, valori iniziali, durate dei cicli di task e così via).
Sicurezza__Operativo	–	✓	L'utente dispone degli stessi diritti concessi al profilo Operativo , ma rispetto al programma di sicurezza, eccetto: <ul style="list-style-type: none"> • Il trasferimento dei valori dei dati al PAC non è consentito. • Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Regolazione	✓	–	L'utente dispone degli stessi diritti concessi al profilo Operativo , con la possibilità aggiuntiva di caricare un progetto (trasferimento al PAC) e di modificare la modalità operativa del PAC (Run, Stop, ...)
Regolazione__Sicurezza	–	✓	L'utente dispone degli stessi diritti concessi al profilo Regolazione , ma rispetto al programma di sicurezza, eccetto: <ul style="list-style-type: none"> • Il trasferimento dei valori dei dati al PAC non è consentito.

Profilo	Tipo di programma applicabile		Descrizione
	Processo	Sicurezza	
			<ul style="list-style-type: none"> Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Debug	✓	–	L'utente dispone degli stessi diritti concessi al profilo Regolazione , con la possibilità aggiuntiva di utilizzare gli strumenti di debug.
Debug_Sicurezza	–	✓	L'utente dispone degli stessi diritti concessi al profilo Debug , ma rispetto al programma di sicurezza, eccetto: <ul style="list-style-type: none"> L'arresto o l'avvio del programma non è consentito. L'aggiornamento dei valori di inizializzazione non è consentito. Il trasferimento dei valori dei dati al PAC non è consentito. La forzatura di ingressi, uscite o bit interni non è consentita. Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Programma	✓	–	L'utente dispone degli stessi diritti concessi al profilo Debug , con la possibilità aggiuntiva di modificare il programma.
Programma_Sicurezza	–	✓	L'utente dispone degli stessi diritti concessi al profilo Programma , ma rispetto al programma di sicurezza, eccetto: <ul style="list-style-type: none"> L'arresto o l'avvio del programma non è consentito. L'aggiornamento dei valori di inizializzazione non è consentito. Il trasferimento dei valori dei dati al PAC non è consentito. Il ripristino del progetto nel PAC da un backup salvato non è consentito. La forzatura di ingressi, uscite o bit interni non è consentita. Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Disattivato	✓	✓	L'utente non può accedere al progetto.

Assegnazione di un utente preconfigurato

Il super user può assegnare un utente preconfigurato, derivato da un profilo preconfigurato, a un utente specifico nella scheda **Utenti** dell'**Editor sicurezza**. Sono disponibili le seguenti selezioni di utente preconfigurato:

- Regolazione_utente_sicurezza
- Debug_utente_sicurezza
- Operativo_utente_sicurezza
- Programma_utente_sicurezza
- Regolazione_utente
- Debug_utente
- Operativo_utente
- Programma_utente

Per ulteriori informazioni su come un super user può assegnare un profilo preconfigurato a un utente, consultare l'argomento *Funzioni utente* (vedi EcoStruxure™ Control Expert, Editor di sicurezza, Guida al funzionamento).

Diritti d'accesso

Introduzione

Control ExpertI diritti di accesso di Control Expert sono classificati nelle seguenti categorie:

- servizi di progetto
- regolazione/debug
- librerie
- modifica globale
- modifica elementare di una variabile
- modifica elementare di dati composti DDT
- modifica elementare di un tipo DFB
- modifica elementare di un'istanza DFB
- editor di configurazione del bus
- editor di configurazione degli I/O
- schermata di runtime
- sicurezza informatica
- sicurezza

Questo argomento presenta i diritti di accesso disponibili per ciascuno dei profili utente preconfigurati.

Servizi del progetto

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Crea un nuovo progetto	-	-	-	-	-	-	✓	✓
Apri un progetto esistente	✓	✓	✓	✓	✓	✓	✓	✓
Salva un progetto	-	-	-	-	-	-	✓	✓
Salva un progetto con nome	✓	✓	✓	✓	✓	✓	✓	✓
Importa un progetto	-	-	-	-	-	-	✓	✓
Crea offline	-	-	-	-	-	-	✓	✓
Crea STOP online	-	-	-	-	-	-	✓	✓
Crea RUN online	-	-	-	-	-	-	✓	✓
Avvia, arresta o inizializza il PLC*	✓	-	✓	-	-	-	✓	✓
Aggiorna i valori iniz con i valori correnti (solo dati non sicuri)	-	-	✓	-	-	-	✓	✓
Trasferimento del progetto dal PAC	✓	✓	✓	✓	✓	✓	✓	✓
Trasferimento del progetto al PAC	✓	✓	✓	✓	-	-	✓	✓
Trasferimento dei valori dei dati da file a PAC (solo dati non sicuri)	✓	-	✓	-	✓	-	✓	✓
Ripristina backup progetto nel PAC	-	-	-	-	-	-	✓	✓
Salva nel backup progetto nel PAC	-	-	-	-	-	-	✓	✓
Imposta indirizzo	✓	✓	✓	✓	✓	✓	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica opzioni	✓	✓	✓	✓	✓	✓	✓	✓
<p>* Solo i task processo vengono avviati o arrestati. Per un PAC non di sicurezza, questo significa che il PAC viene avviato o arrestato. Per un PAC M580 Safety, questo significa che i task diversi dal task SAFE vengono avviati o arrestati.</p> <p>✓ : Incluso – : Non incluso</p>								

Regolazione/debug

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica valori variabili	✓	–	✓		✓		✓	✓
Modifica valori variabile di sicurezza	–	✓	–	✓	–	✓	–	✓
Forza bit interni	–	–	✓	–	–	–	✓	✓
Forza uscite	–	–	✓	–	–	–	✓	✓
Forza ingressi	–	–	✓	–	–	–	✓	✓
Gestione task	–	–	✓	–	–	–	✓	✓
Gestione task SAFE	–	–	–	✓	–	–	–	✓
Modifica del periodo di ciclo del task	✓	–	✓		✓	–	✓	✓
Modifica durata ciclo task SAFE	–	✓	–	✓	–	✓	–	✓
Elimina messaggio nel visualizzatore	✓	✓	✓	✓	✓	✓	✓	✓
Debug dell'eseguibile	–	–	✓	✓	–	–	✓	✓
Sostituisci una variabile del progetto	–	–	–	–	–	–	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Sostituisci una variabile del progetto	-	-	-	-	-	-	-	✓
✓ : Incluso - : Non incluso								

Librerie

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Crea librerie o famiglie	-	-	-	-	-	-	✓	✓
Crea famiglie o librerie di sicurezza	-	-	-	-	-	-	-	✓
Elimina librerie o famiglie	-	-	-	-	-	-	✓	✓
Elimina famiglie o librerie di sicurezza	-	-	-	-	-	-	-	✓
Poni l'oggetto nella libreria	-	-	-	-	-	-	✓	✓
Poni l'oggetto nella libreria di sicurezza	-	-	-	-	-	-	-	✓
Elimina un oggetto dalla libreria	-	-	-	-	-	-	✓	✓
Elimina un oggetto dalla libreria di sicurezza	-	-	-	-	-	-	-	✓
Recupera oggetto da una libreria	-	-	-	-	-	-	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Recupera un oggetto dalla libreria di sicurezza	-	-	-	-	-	-	-	✓
✓ : Incluso - : Non incluso								

Modifica globale

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica documentazione	✓	✓	✓	✓	✓	✓	✓	✓
Modifica la vista funzionale	-	-	-	-	-	-	✓	✓
Modifica le tabelle di animazione	✓	✓	✓	✓	✓	✓	✓	✓
Modifica valore delle costanti	✓	-	✓	-	✓	-	✓	✓
Modifica valore delle costanti di sicurezza	-	✓	-	✓	-	✓	-	✓
Modifica la struttura del programma	-	-	-	-	-	-	✓	✓
Modifica la struttura del programma di sicurezza	-	-	-	-	-	-	-	✓
Modifica sezioni programma	-	-	-	-	-	-	✓	✓
Modifica sezioni programma di sicurezza	-	-	-	-	-	-	-	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica le impostazioni del progetto	-	-	-	-	-	-	✓	✓
✓ : Incluso - : Non incluso								

Modifica elementare di una variabile

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Rimozione/aggiunta variabile	-	-	-	-	-	-	✓	✓
Rimozione/aggiunta variabili di sicurezza	-	-	-	-	-	-	-	✓
Modifica attributi principali della variabile	-	-	-	-	-	-	✓	✓
Modifica attributi principali variabili di sicurezza	-	-	-	-	-	-	-	✓
Modifica attributi secondari della variabile	✓	-	✓	-	✓	-	✓	✓
Modifica attributi secondari variabili di sicurezza	-	✓	-	✓	-	✓	-	✓
✓ : Incluso - : Non incluso								

Modifica elementare di dati composti DDT

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regola- zione	Regola- zione_ Sicurez- za	Debug	Debug_ Sicurez- za	Operati- vo	Operati- vo_ Sicurez- za	Program- ma	Pro- gram- ma_ Sicurez- za
Rimozione/ aggiunta DDT	-	-	-	-	-	-	✓	✓
Modifiche DDT	-	-	-	-	-	-	✓	✓
✓ : Incluso - : Non incluso								

Modifica elementare di un tipo DFB

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regola- zione	Regola- zione_ Sicurez- za	Debug	Debug_ Sicurez- za	Operati- vo	Operati- vo_ Sicurez- za	Program- ma	Pro- gram- ma_ Sicurez- za
Rimozione/aggiunta tipo DFB	-	-	-	-	-	-	✓	✓
Rimozione/aggiunta tipo DFB di sicurezza	-	-	-	-	-	-	-	✓
Modifica struttura tipo DFB	-	-	-	-	-	-	✓	✓
Modifica struttura tipo DFB di sicurezza	-	-	-	-	-	-	-	✓
Modifica sezioni tipo DFB	-	-	-	-	-	-	✓	✓
Modifica sezioni tipo DFB di sicurezza	-	-	-	-	-	-	-	✓
✓ : Incluso - : Non incluso								

Modifica elementare di un'istanza DFB

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica istanza DFB	-	-	-	-	-	-	✓	✓
Modifica istanza DFB di sicurezza	-	-	-	-	-	-	-	✓
Modifica attributi secondari istanza DFB	✓	-	✓	-	✓	-	✓	✓
Modifica attributi secondari istanza DFB di sicurezza	-	✓	-	✓	-	✓	-	✓
✓ : Incluso - : Non incluso								

Editor di configurazione del bus

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica configurazione	-	-	-	-	-	-	✓	✓
Modifica la configurazione di sicurezza	-	-	-	-	-	-	-	✓
Rilevamento I/O	-	-	-	-	-	-	✓	✓
✓ : Incluso - : Non incluso								

Editor di configurazione degli I/O

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica configurazione I/O	-	-	-	-	-	-	✓	✓
Modifica la configurazione degli I/O di sicurezza	-	-	-	-	-	-	-	✓
Regola I/O	✓	-	✓	-	✓	-	✓	✓
Regola gli I/O di sicurezza	-	✓	-	✓	-	✓	-	✓
Salva_param	-	-	✓	-	-	-	✓	✓
Ripristina_param	-	-	✓	-	-	-	✓	✓
✓ : Incluso - : Non incluso								

Schermate di runtime

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica schermate	-	-	-	-	-	-	✓	✓
Modifica messaggi	-	-	-	-	-	-	✓	✓
Aggiungi/rimuovi schermate o famiglie	-	-	-	-	-	-	✓	✓
✓ : Incluso - : Non incluso								

Sicurezza informatica

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Crea o modifica password applicazione	-	-	-	-	-	-	✓	✓
Entra in modalità manutenzione	-	✓	-	✓	-	✓	-	✓
Adatta timeout blocco automatico	✓	✓	✓	✓	✓	✓	✓	✓
✓ : Incluso - : Non incluso								

Sicurezza

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Entra in modalità manutenzione	-	✓	-	✓	-	✓	-	✓
✓ : Incluso - : Non incluso								

Modifiche a Control Expert per il sistema di sicurezza M580

Introduzione

Questa sezione descrive la funzionalità Control Expert che è stata modificata o limitata per il sistema di sicurezza M580.

Trasferimento e importazione di codice e progetti di sicurezza M580 in Control Expert

Trasferimento di un progetto di sicurezza da Control Expert al PAC di sicurezza

È possibile utilizzare il comando **PLC > Trasferisci progetto al PLC** per trasferire il progetto da Control Expert al PAC quando:

- Control Expert è collegato in modalità di programmazione (vedi EcoStruxure™ Control Expert, Modalità operative) al PAC di sicurezza M580 e
- in Control Expert è aperto un progetto e
- tutti i task PAC sono in stato STOP.

NOTA: Un'applicazione di sicurezza può essere trasferita solo a un PAC di sicurezza. Non si può trasferire un'applicazione di sicurezza a un PAC non di sicurezza.

Trasferimento di un progetto di sicurezza dal PAC di sicurezza a Control Expert

Analogamente, è possibile utilizzare il comando **PLC > Trasferisci progetto dal PLC** per trasferire il progetto dal PAC a Control Expert quando:

- Control Expert è collegato in modalità di programmazione (vedi EcoStruxure™ Control Expert, Modalità operative) al PAC di sicurezza M580 e
- non vi sono progetti aperti in Control Expert.

È possibile trasferire il contenuto relativo a qualsiasi task (SAFE, MAST, FAST, AUX0 o AUX1) nella modalità operativa di sicurezza o di manutenzione.

Importazione di progetti e di sezioni di codice in Control Expert

Control Expert Safety supporta l'importazione sia di progetti interi (tramite **File > Apri**) sia di sezioni di codice (via **Task > Importa...** o **Sezioni > Importa...**), secondo le condizioni seguenti:

- Solo i tipi di funzioni o di blocchi funzione esistenti nella libreria di sicurezza (**Data Scope Editor > <Libset> > Safety**) oppure nella libreria personalizzata (**Data Scope Editor > <Libset> > Libreria personalizzata**), possono essere inclusi in una sezione di codice gestita dal task SAFE.
- Solo i tipi di funzioni o di blocchi funzione esistenti in librerie diverse dalla libreria di sicurezza possono essere inclusi in una sezione del codice non SAFE gestita da un task di processo (MAST, FAST, AUX0 o AUX1).

Salvataggio e ripristino di dati tra un file e il PAC

Funzioni di salvataggio e ripristino per i dati non di sicurezza

Control Expert supporta i comandi **PLC > Salva i dati dal PLC al file** e **PLC > Recupera i dati dal file al PLC** per i dati dell'area di processo e globali. Tuttavia, i dati salvati e ripristinati non includono le variabili e le istanze di blocchi funzione create nello spazio dei nomi sicuro.

Per informazioni su come utilizzare questi comandi per i dati non sicuri, vedere l'argomento *Salvataggio/ripristino di dati tra un file e il PLC* nel documento *EcoStruxure™ Control Expert - Modalità operative*.

CCOTF per un PAC di sicurezza M580

Modifica al volo della configurazione

La funzione di modifica al volo della configurazione (CCOTF) permette di modificare una configurazione di Control Expert mentre il PAC è in funzione. Le funzioni supportate possono includere:

- Aggiunta di una derivazione.
- Aggiunta di un modulo di I/O.
- Eliminazione di un modulo di I/O.

- Modifica della configurazione di un modulo di I/O, incluso:
 - Modifica di un'impostazione dei parametri.
 - Aggiunta di una funzione del canale.
 - Eliminazione di una funzione del canale.
 - Modifica di una funzione del canale.

NOTA: Le funzioni CCOTF non si applicano ai dispositivi CIP Safety.

La funzione CCOTF viene attivata selezionando **Modifica online in modalità RUN o STOP** nella scheda **Configurazione** del modulo CPU.

La funzionalità di base della funzione CCOTF è stata implementata nel PAC di sicurezza M580, con le limitazioni descritte sotto.

Per una descrizione completa della funzione CCOTF, vedere *Modicon M580 Modifica della configurazione al volo Guida utente*.

Limitazioni di CCOTF per un PAC di sicurezza M580

La funzione CCOTF è implementata nel PAC di sicurezza M580 con una serie di limitazioni legate alla funzione specifica e dal tipo di modulo di I/O, nel seguente modo:

Funzione CCOTF	Tipo di modulo di I/O e modalità operativa			
	I/O non interferenti		I/O di sicurezza SIL3	
	Modalità di manutenzione	Modalità di sicurezza	Modalità di manutenzione	Modalità di sicurezza
Aggiungi derivazione	✓	✓	✓ ¹	✓
Aggiungi modulo	✓	✓	✓ ¹	X
Elimina modulo	✓	✓	✓	X
Modifica configurazione modulo I/O	✓	✓	X	X
✓: Consentita X: Non consentita 1.Per aggiungere una derivazione e un modulo di sicurezza sono necessarie due sessioni CCOTF: una sessione CCOTF per aggiungere la derivazione e una seconda sessione CCOTF per aggiungere il modulo di sicurezza. Queste azioni non possono essere eseguite in una sola sessione CCOTF.				

NOTA: Le modifiche effettuate in una sola sessione CCOTF possono riferirsi solo a un singolo task (SAFE, MAST, FAST, AUX0 o AUX1).

Modifiche dei tool del PAC di sicurezza M580

Introduzione

Il PAC di sicurezza M580 supporta l'uso di vari tool correlati. Alcuni di questi tool sono stati modificati per essere utilizzati insieme al PAC di sicurezza M580. In questa sezione sono descritti alcuni di questi tool.

Uso della memoria

La schermata **Uso della memoria** contiene le seguenti informazioni:

- la distribuzione fisica del PAC (memoria iniziale e scheda di memoria)
- lo spazio di memoria utilizzato da un progetto (dati, programma, configurazione, sistema)

Per il PAC di sicurezza M580, questa schermata contiene due nuovi parametri specifici – **Dati di sicurezza dichiarati** e **Codice di sicurezza eseguibile** – che sono descritti di seguito.

NOTA: Si può anche usare il comando **Pack** in questa schermata per riorganizzare la memoria laddove possibile.

Per ulteriori informazioni vedere la sezione *Uso della memoria* nel manuale utente *EcoStruxure™ Control Expert, Modalità operative*.

Per il PAC di sicurezza M580 vengono visualizzati i seguenti parametri:

Parametro	Descrizione
Dati utente	<p>Questo campo indica lo spazio di memoria (in parole) occupato dai dati utente (oggetti relativi alla configurazione):</p> <ul style="list-style-type: none"> • Dati: dati identificati associati al processore (%M, %MW, %S, %SW, etc.) o ai moduli di ingresso/uscita. • Dati dichiarati: dati non localizzati (dichiarati nell'editor dati di processo) salvati dopo un'interruzione dell'alimentazione. • Dati dichiarati non salvati: dati non localizzati (dichiarati nell'editor dati di processo) non salvati dopo un'interruzione dell'alimentazione. • Dati di sicurezza dichiarati: dati non localizzati (dichiarati nell'editor dati di sicurezza) non salvati dopo un'interruzione dell'alimentazione.
Programma utente	<p>Questo campo indica lo spazio di memoria (in parole) occupato dal programma del progetto:</p> <ul style="list-style-type: none"> • Costanti: costanti statiche associate al processore (%KW) e ai moduli di ingresso/uscita; valori dati iniziali. • Codice eseguibile: codice eseguibile della parte area di processo del programma del progetto, tipi EF, EFB e DFB. • Informazioni di caricamento: informazioni per il caricamento di un progetto (codice grafico di linguaggi, simboli, ecc.).

Parametro	Descrizione
	<ul style="list-style-type: none"> • Codice di sicurezza eseguibile: codice eseguibile della parte area di sicurezza del programma del progetto, tipi EF, EFB e DFB.
Altro	<p>Questo campo indica lo spazio di memoria (in parole) occupato dagli altri dati relativi alla configurazione e alla struttura del progetto:</p> <ul style="list-style-type: none"> • Configurazione: altri dati relativi alla configurazione (hardware o software). • Sistema: dati utilizzati dal sistema operativo (stack di task, cataloghi, ecc.), • Diagnostica: informazioni relative alla diagnostica del processo o del sistema, buffer di diagnostica. • Dizionario dati: dizionario delle variabili simbolizzate con le rispettive caratteristiche (indirizzo, tipo, ecc.).
Memoria interna	<p>Questo campo mostra l'organizzazione della memoria PAC interna. Indica anche lo spazio di memoria disponibile (Totale), lo spazio di memoria contiguo più grande possibile (Valore più alto) e il livello di frammentazione (a causa delle modifiche online).</p>

Visualizzatore eventi

Visualizzatore eventi è una utility MS Windows che cattura gli eventi registrati da Control Expert. Si può usare *Visualizzatore eventi* per visualizzare una cronologia di eventi registrati.

Accedere a *Visualizzatore eventi* in MS Windows nella cartella *Strumenti di amministrazione* del *Pannello di controllo*. Quando si apre l'utility, selezionare **Mostra riquadro di azioni**, quindi fare clic su **Crea visualizzazione personalizzata** per aprire la finestra di dialogo. Qui si può creare una visualizzazione personalizzata per eventi Control Expert.

NOTA: Nella finestra di dialogo **Crea visualizzazione personalizzata**, selezionare prima **Per origine**, quindi selezionare **TraceServer** come origine per visualizzare eventi Control Expert.

CIP Safety

Contenuto del capitolo

Introduzione di CIP Safety per PAC Safety M580.....	346
Configurazione della CPU CIP Safety M580.....	350
Configurazione del dispositivo CIP Safety di destinazione.....	352
Configurazione dei DTM del dispositivo di sicurezza.....	356
Operazioni con CIP Safety.....	368
Diagnostica CIP Safety	378

Panoramica

Questo capitolo descrive le comunicazioni CIP Safety IEC 61784-3 supportate dalle CPU di sicurezza indipendenti BMEP58•040S M580.

Introduzione di CIP Safety per PAC Safety M580

Comunicazione CIP Safety

Introduzione

Le CPU di sicurezza indipendenti BM58•040S supportano la comunicazione CIP Safety (IEC 61784-3) e possono utilizzare questo protocollo per stabilire una connessione con un dispositivo CIP Safety su EtherNet/IP.

CIP Safety utilizza un meccanismo utilizzatore-produttore per lo scambio di dati tra nodi sicuri su EtherNet/IP (la comunicazione DeviceNet o Sercos III non è supportata). La CPU svolge un ruolo di origine che stabilisce una connessione EtherNet/IP Unicast (uno a uno) con ciascun dispositivo di sicurezza di destinazione. La CPU può stabilire una connessione CIP Safety con dispositivi di destinazione che supportano un protocollo CIP Safety e una connessione CIP (non di sicurezza) con i dispositivi di destinazione che supportano il protocollo CIP.

Siccome è il caso di tutti i PAC di sicurezza, la CPU CIP Safety e Copro eseguono due volte lo stack CIP Safety in parallelo e confrontano i risultati di esecuzione.

Architetture supportate

Le CPU di sicurezza indipendenti M580 supportano i dispositivi CIP Safety situati in cloud DIO.

NOTA: Al momento, non esiste un dispositivo CIP Safety in grado di supportare RSTP che possa essere installato su un rack eX80. Perciò, attualmente i dispositivi CIP Safety non possono essere collegati alle porte doppie della rete di dispositivi della CPU, ma possono essere collegati alla porta Service della CPU.

I cloud DIO richiedono solo una connessione unica (non ad anello) in rame e possono essere collegati a:

- un modulo di switch opzionale di rete BMENOS0300
- la porta service della CPU.
- la porta service del modulo adattatore Ethernet I/O eX80 BM•CRA312•0 su una derivazione RIO.
- una porta in rame di uno switch a doppio anello Ethernet.

NOTA: Quando un dispositivo CIP Safety è collegato alla porta service di un modulo adattatore Ethernet I/O eX80 BM•CRA312•0 su una derivazione RIO, il dispositivo CIP Safety di destinazione potrebbe non avviarsi automaticamente durante il caricamento della configurazione CRA. Per aprire nel modo previsto le connessioni CIP Safety, potrebbe essere necessario gestire il bit di controllo della connessione CIP Safety nel DDDT di destinazione (CTRL_IN o CTRL_OUT) commutandolo da False a True dopo il caricamento della configurazione di BM•CRA312•0.

Come per tutte le apparecchiature situate nel cloud DIO, i dispositivi CIP Safety non vengono analizzati come parte dell'anello principale RIO e il loro stato di connessione non viene mostrato dai LED della CPU.

Per maggiori informazioni sui cloud DIO, consultare *Guida di pianificazione del sistema Modicon M580 indipendente per le architetture utilizzate più di frequente* e *Guida di pianificazione del sistema Modicon M580 per le topologie complesse*.

Panoramica della configurazione

La configurazione delle comunicazioni CIP Safety comprende tre attività di configurazione distinte:

- Configurare la CPU indipendente M580 Safety con CIP Safety in Control Expert, pagina 350. Questo passaggio comprende anche la creazione di un Identificativo di rete univoco dell'origine (OUNID) che identifica in modo univoco la CPU. L'OUNID creato in Control Expert è formato dalla concatenazione di due elementi:
 - Numero di rete di sicurezza (SNN): Un identificativo della CPU creato in Control Expert.
 - L'indirizzo IP principale della CPU, immesso in Control Expert come parte delle impostazioni di indirizzo IP della CPU.

Schneider Electric suggerisce di configurare l'impostazione dell'OUNID della CPU una volta sola, durante la configurazione iniziale. Se in seguito venisse modificata l'impostazione OUNID, sarà necessario riconfigurare tutti i dispositivi CIP Safety collegati alla CPU.

- Configurare il dispositivo CIP Safety, pagina 354, utilizzando uno strumento di configurazione di rete di sicurezza (SNCT) offerto dal fornitore del dispositivo. Ciò comprende due attività:
 - Creazione di un identificativo di configurazione di sicurezza (SCID): noto anche come firma di configurazione, lo SCID viene creato nell'SNCT e utilizzato da Control Expert quando si configura la connessione CIP Safety tra origine (CPU) e destinazione (dispositivo CIP Safety).
 - Assegnazione di un numero di rete di sicurezza (SNN): l'SNN viene generalmente creato per il dispositivo CIP Safety da Control Expert e assegnato al dispositivo dall'SNCT.

- Configurare la connessione CIP tra la CPU e il dispositivo CIP Safety, pagina 356. La connessione viene identificata da un TUNID, creato utilizzando la connessione di dispositivo DTM in Control Expert e utilizzando un DTM CIP Safety, che può essere basato su un file EDS fornito dal produttore o utilizzato singolarmente se non sono disponibili file EDS.

Gestione delle connessioni di dispositivo CIP Safety

La CPU CIP Safety stabilisce una connessione tra un dispositivo CIP configurato e quindi gestisce il dispositivo collegato. Questo perché Control Expert supporta sia il protocollo CIP che il protocollo CIP Safety e può gestire le connessioni CIP verso:

- i dispositivi CIP, che implementano CIP, ma non CIP Safety, su EtherNet/IP.
- i dispositivi CIP Safety, che implementano CIP Safety, ma non CIP, su Ethernet/IP.
- i dispositivi ibridi CIP, che implementano sia CIP che CIP Safety su EtherNet/IP.

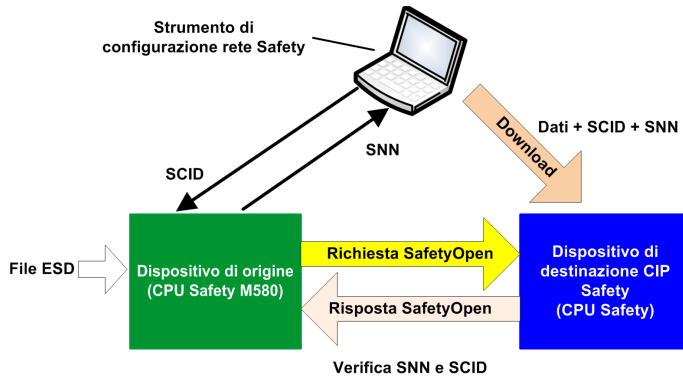
NOTA: Per la configurazione, i dispositivi CIP e CIP Safety necessitano ciascuno di un unico DTM. Un dispositivo ibrido CIP, che ingloba i protocolli CIP e CIP Safety, necessita di due DTM, uno configurato come dispositivo CIP, l'altro come dispositivo CIP Safety.

Come stabilire una connessione origine -> destinazione

Per stabilire la connessione con un dispositivo CIP Safety, la CPU indipendente M580 utilizza solo la richiesta apertura di sicurezza di tipo 2. Una connessione apertura di sicurezza di tipo 2 può essere stabilita verso un dispositivo di sicurezza solo dopo che il dispositivo sia stato configurato come SNCT. Ne caso in cui il dispositivo CIP Safety sia un prodotto di terze parti, Control Expert non possiede e non può scaricare un file di configurazione su un dispositivo CIP Safety e non può essere utilizzato come SNCT.

NOTA: Al contrario, una connessione apertura di sicurezza di tipo 1 può fornire al dispositivo di sicurezza le proprie impostazioni di configurazione e stabilire la connessione. Le CPU CIP Safety M580 non supportano la richiesta di connessione apertura di sicurezza di tipo 1.

Il diagramma seguente presenta una panoramica della modalità di creazione della connessione CIP Safety tra una CPU come origine di connessione e un dispositivo CIP Safety come destinazione:



In questo diagramma si verificano i seguenti eventi:

1. Control Expert utilizza un file EDS offerto dal fornitore come base per la creazione di un DTM per la connessione tra la CPU e un dispositivo CIP Safety.
2. Il dispositivo SNN viene creato in Control Expert, quindi immesso nell'SNCT.
3. L'SNCT crea lo SCID per il dispositivo, che viene inserito in Control Expert come parte della configurazione di connessione.
4. L'SNCT scarica sul dispositivo le proprie impostazioni di configurazione, lo SCID creato dall'SNCT e l'SNN creato da Control Expert per la connessione.
5. La CPU come origine invia al dispositivo una Richiesta apertura di sicurezza di tipo 2.
6. Il dispositivo CIP Safety invia una Risposta di apertura di sicurezza alla CPU.
7. Se il checksum corrisponde sia nella richiesta che nella risposta, la connessione viene stabilita.

Configurazione della CPU CIP Safety M580

Panoramica

Questa sezione descrive le modalità di configurazione della CPU indipendente CIP Safety come origine per le comunicazioni CIP Safety.

Configurazione dell'OUNID CPU

CPU come origine

Utilizzare la scheda **Sicurezza** della (vedi Modicon M580, Hardware, Manuale di riferimento) CPU di sicurezza indipendente M580 per configurare la CPU come CIP Safety origine, assegnandole un Identificativo di rete univoco di origine (OUNID).

Un OUNID è un valore esadecimale concatenato da 10 byte, composto da:

- Numero di rete di sicurezza (6 byte)
- Indirizzo IP (4 byte)

NOTA: Le modifiche all'OUNID possono essere effettuate solo offline. Dopo la creazione della configurazione modificata, l'applicazione può essere scaricata sul PAC.

Numero di rete di sicurezza

Il Numero di rete di sicurezza componente dell'OUNID può essere generato automaticamente da Control Expert, o generato dall'utente con immissione manuale. Creare l'SNN::

- Automaticamente, selezionando **Basato su tempo**, quindi facendo clic sul pulsante **Genera**. Il valore generato automaticamente viene visualizzato nel campo **Numero**.
- Manualmente, selezionando **Manuale**, quindi immettendo una stringa esadecimale da 6 byte nel campo **Numero**.

NOTA: È necessario che l'utente assegni un SNN univoco a ciascuna origine CPU M580 collegata alla stessa rete di sicurezza.

Indirizzo IP

L'impostazione di sola lettura viene inserita automaticamente, in base all'impostazione dell'**Indirizzo IP principale** della CPU nella scheda **IPConfig** Modicon M580, Hardware, Manuale di riferimento.

OUNID

Dopo la creazione, l'OUNID viene utilizzato come parametro nella Richiesta di apertura di sicurezza di tipo 2,, pagina 369 stabilendo una connessione tra la CPU come origine e il dispositivo CIP Safety come destinazione.

Configurazione del dispositivo CIP Safety di destinazione

Panoramica

Questa sezione descrive il processo di configurazione del dispositivo CIP Safety, compresa la sua configurazione con l'utilizzo di uno strumento di configurazione offerto dal fornitore.

Panoramica di configurazione del dispositivo CIP Safety

Introduzione

La configurazione del dispositivo CIP Safety di destinazione comprende due attività:

- Configurare le impostazioni del dispositivo di destinazione CIP Safety, pagina 354 utilizzando uno strumento di configurazione di rete di sicurezza (SNCT) offerto dal fornitore.
- Configurare la connessione tra l'origine della CPU CIP Safety e il dispositivo CIP di destinazione, utilizzando un DTM in Control Expert. Il DTM può essere:
 - basato su un file EDS offerto dal fornitore.
 - un DTM generico di Control Expert, se non sono disponibili file EDS.

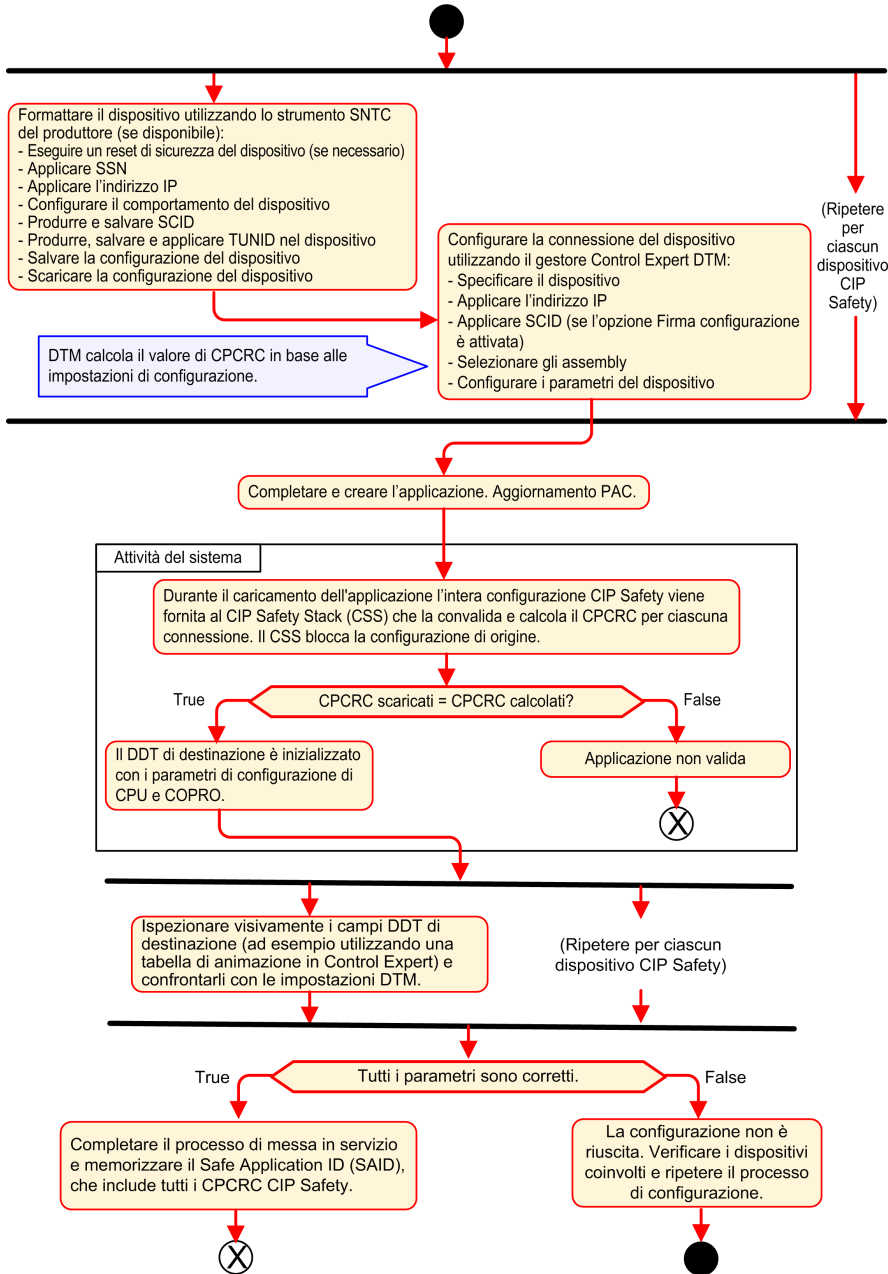
Verifica di configurazione doppia

I seguenti due processi, insieme, forniscono una conferma di integrità elevata che la configurazione creata con il software Control Expert è stata scaricata e salvata in modo corretto nella CPU CIP Safety M580 come origine:

- Un confronto visivo eseguito dall'utente (dopo il completamento dell'operazione) dei parametri di configurazione della connessione CIP Safety visualizzati nella destinazione DDDT rispetto agli stessi parametri visualizzati nel DTM di destinazione.
- Un confronto automatico, eseguito da CPU e Copro, del parametro di connessione CPCRC CRC calcolato dal DTM rispetto al CPCRC calcolato dallo stack CIP Safety (CSS) in esecuzione in CPU e Copro.

Panoramica del processo di configurazione

Il processo di configurazione e convalida del dispositivo CIP Safety:



Configurazione del dispositivo CIP Safety con l'utilizzo di uno strumento offerto dal fornitore

Introduzione

Il dispositivo di destinazione CIP Safety viene configurato utilizzando uno strumento di configurazione di rete di sicurezza (SNCT). Non è configurato con il software Control Expert. L'SNCT viene offerto dal fornitore del dispositivo CIP Safety, quindi è collegato al dispositivo.

Usare l'SNCT per:

- Configurare e scaricare sul dispositivo le impostazioni necessarie al suo funzionamento.
- Configurare, quindi copiare e trasferire al software Control Expert, un Identificativo di configurazione di sicurezza specifico per il dispositivo (SCID). Lo SCID viene denominato Firma di configurazione del dispositivo. Viene utilizzato in Control Expert per la configurazione della connessione Origine -> Destinazione., pagina 361
- Assegnare al dispositivo il TUNID univoco, composto da:
 - Numero di rete di sicurezza (SNN), pagina 360 e
 - Indirizzo IP univoco.

NOTA: L'SNN viene solitamente generato da un software di configurazione Control Expert (come parte della configurazione di connessione Origine -> Destinazione) e applicato al dispositivo. L'indirizzo IP viene immesso sia nell'SNCT che nel DTM di connessione del dispositivo in Control Expert.

Configurazione dello SCID

Lo SCID viene impostato nell'SNCT e svolge la funzione di identificativo univoco di configurazione esadecimale per il dispositivo di destinazione CIP Safety. È una concatenazione di:

- CRC di configurazione di sicurezza (SCCRC): un valore di controllo di ridondanza ciclico (CRC) delle impostazioni di configurazione del dispositivo CIP Safety, sotto forma di 4 ottetti.
- Un Time stamp di configurazione di sicurezza (SCTS): un valore time stamp esadecimale di data e ora formato da 6 ottetti.

AVVISO

RISCHIO DI FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Se la CPU M580 viene configurata come origine CIP Safety, prima di utilizzare la comunicazione CIP Safety verificare il comportamento funzionale di CIP Safety del sistema per controllare la funzione di sicurezza correlata. Dopo l'esito positivo della verifica, abilitare la firma di configurazione di destinazione di CIP Safety (se presente) nei DTM CIP Safety di Control Expert.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Dopo la creazione di uno SCID con SNCT, è possibile immettere gli elementi dello SCID nella scheda **Sicurezza** del DTM del dispositivo in Control Expert:

- **ID:** immettere il valore SCCRC.
- **Data:** immettere la data di creazione dello SCID (mm/gg/aaaa).
- **Ora:** immettere l'ora di creazione dello SCID (hh/mm/ss/ms).

Sequenza di configurazione del dispositivo CIP Safety

Questa sequenza descrive un tipico processo di configurazione del dispositivo CIP Safety:

1. Ottenere l'SNN del dispositivo (ricevuto da Control Expert).
2. Applicare l'SNN nell'SNCT del fornitore.
3. Eseguire un reset di sicurezza del dispositivo (opzionale: se l'OUNID di origine è cambiato dall'ultimo collegamento del dispositivo).
4. Applicare il TUNID nel dispositivo.
5. Determinare le impostazioni di configurazione che controllano il comportamento del dispositivo.
6. Configurare il dispositivo con l'SNCT del fornitore (strumento di configurazione di rete di sicurezza).
7. Bloccare la configurazione e verificarne l'accuratezza.
8. Registrare e salvare i parametri per un futuro utilizzo nella configurazione di origine (SCID, Numeri gruppo, indirizzo IP e così via).
9. Salvare una copia della configurazione del dispositivo per un futuro utilizzo (ad esempio, in caso il dispositivo debba essere sostituito).

Configurazione dei DTM del dispositivo di sicurezza

Panoramica

Questa sezione descrive la configurazione dei dispositivi di sicurezza di destinazione e la loro connessione alla CPU di origine, utilizzando i DTM in Control Expert.

Lavorare con i DTM

Lavorare con i DTM

La configurazione della connessione tra l'origine CPU e il dispositivo CIP Safety di destinazione viene effettuata utilizzando un DTM. Control Expert supporta l'utilizzo dei seguenti DTM, in base al profilo del dispositivo:

- DTM CIP Safety: per configurare una connessione a un dispositivo CIP Safety. Può essere effettuata con o senza un file EDS del fornitore.
- DTM generico: per configurare una connessione standard (ossia non di sicurezza) a un dispositivo, sulla base di un file EDS del fornitore.

Le impostazioni immesse con l'utilizzo di un DTM vengono archiviate nel DDDT, pagina 379 T_CIP_SAFETY_CONF e utilizzate dalla Richiesta di apertura di sicurezza di tipo 2, pagina 369 per stabilire una connessione tra la CPU origine e il dispositivo di destinazione.

Quando è disponibile un file EDS

Quando per un dispositivo è disponibile un file EDS del fornitore, è possibile utilizzarlo per creare un nuovo DTM e aggiungerlo al **Catalogo DTM** in Control Expert, procedendo come segue:

Pas-so	Azione
1	In Control Expert, selezionare Strumenti > Browser DTM .
2	In Browser DTM , fare clic con il pulsante destro del mouse su DTM CPU (BMEP58_ECPU_EXT) per aprire il menu contestuale.

Pas- so	Azione
3	Spostarsi fino a e selezionare il menu Dispositivo > Funzioni aggiuntive > Aggiungi EDS a libreria . Si apre la procedura guidata Aggiunta EDS .
4	Vedere l'argomento Aggiunta di un file EDS nel catalogo hardware (vedi EcoStruxure™ Control Expert, Modalità operative) per istruzioni passo passo su come completare il processo di aggiunta di un file EDS al Catalogo DTM.

Dopo aver aggiunto un DTM al **Catalogo DTM**, è possibile aggiungerlo al progetto Control Expert.

Quando un file EDS non è disponibile

Control Expert comprende un DTM di sicurezza generico nel **Catalogo DTM**. È possibile utilizzarlo per configurare un dispositivo CIP Safety quando non è disponibile un file EDS per quel dispositivo.

Dispositivi ibridi

Un dispositivo ibrido è un singolo dispositivo in grado di supportare sia connessioni di sicurezza che standard. Quando un dispositivo ibrido viene aggiunto al **Catalogo DTM** con il comando **Aggiungi EDS a libreria**, vengono creati due DTM nel **Catalogo DTM** per il dispositivo: un DTM standard e uno di sicurezza.

Quando un dispositivo ibrido viene aggiunto al progetto, è necessario configurare sia il DTM standard che quello di sicurezza per singolo dispositivo.

Aggiunta di un DTM al Progetto Control Expert

Per aggiungere un DTM al Progetto Control Expert:

Pas- so	Azione
1	Nel Browser DTM fare clic con il pulsante destro del mouse su DTM CPU (BMEP58_ECPU_EXT) e selezionare Aggiungi... Si apre la finestra di dialogo Aggiungi .
2	Selezionare il DTM da aggiungere. Può essere: <ul style="list-style-type: none"> • Un DTM CIP Safety creato da un file EDS del dispositivo CIP Safety del fornitore, o • Un DTM CIP Safety senza un file EDS del fornitore.

Pas- so	Azione
3	Fare clic su Aggiungi DTM . Il DTM selezionato compare nel Browse rDTM sotto DTM CPU.
4	Fare clic con il pulsante destro del mouse sul nuovo DTM selezionare Apri . Si apre la finestra di configurazione del DTM

Configurazione del DTM

Il DTM CIP Safety, creato con o senza file EDS del fornitore, presenta una serie di schermate di configurazione simili in Control Expert:

Struttura ad albero / Schede di configurazione	Tipo DTM	
	Con EDS del fornitore	Senza EDS del fornitore
<Nodo superiore>	✓	✓
Nodo generale		
Scheda dispositivo	✓	X
Scheda di sicurezza	✓	✓
<Conessioni>		
Scheda di connessione	✓	✓
Scheda Impostazioni di configurazione	✓	X
Scheda di verifica configurazione	✓	✓
< > indica il nome definito dall'utente. ✓ = incluso X = non incluso		

I seguenti argomenti descrivono diverse schede di configurazione presentate da Control Expert per ogni tipo di DTM.

DTM dispositivo di sicurezza - Informazioni su file e fornitore

Introduzione

Il DTM CIP Safety, creato o meno da file EDS, presenta una descrizione del file EDS di origine e del fornitore del dispositivo. Per un:

- DTM CIP Safety creato da file EDS del fornitore queste informazioni sono di sola lettura ed è possibile accedervi solo selezionando il <Nodo superiore> della struttura ad albero del DTM (pannello sinistro).
- DTM CIP Safety creato senza un file EDS queste informazioni sono visibili in due posizioni differenti:
 - con la selezione <Nodo superiore> vengono visualizzate le informazioni di sola lettura del file EDS.
NOTA: Il riferimento del file EDS è un file EDS di sicurezza generico interno con fornitore Schneider Electric, che viene utilizzato da Control Expert per creare il DTM CIP Safety.
 - Con la selezione della scheda **Generale > Dispositivo** vengono visualizzate le informazioni modificabili sul fornitore.

Informazioni sul file EDS

Le informazioni sul file EDS comprendono i seguenti dati di sola lettura:

- Descrizione
- Data creazione del file
- Ora creazione del file
- Data ultima modifica
- Ora ultima modifica
- Revisione EDS

Informazioni sul fornitore

Le seguenti informazioni sul fornitore sono di sola lettura per un DTM CIP Safety creato da un file EDS del fornitore:

- Nome del fornitore
- Tipo di dispositivo

- Revisione maggiore
- Revisione minore
- Nome prodotto

Le seguenti informazioni sul fornitore sono di lettura-scrittura per un DTM CIP Safety creato senza un file EDS del fornitore:

- ID fornitore
- Tipo prodotto
- Codice prodotto
- Revisione maggiore
- Revisione minore

NOTA: Per le configurazioni di DTM effettuate senza un file EDS, immettere le impostazioni del fornitore con le informazioni fornite da quest'ultimo. Per impostazione predefinita, i valori del fornitore DTM sono impostati su 0, quando i valori a 0 non sono supportati.

DTM del dispositivo di sicurezza - Numero di rete di sicurezza

Numero di rete di sicurezza

Utilizzare la scheda **Generale > Sicurezza** del DTM del dispositivo CIP Safety per configurare un Numero di rete di sicurezza (SNN) per il dispositivo di sicurezza. L'SNN viene utilizzato per impostare l'Identificativo univoco di rete di destinazione (TUNID). TUNID identifica il dispositivo CIP Safety ed è un componente essenziale della Richiesta di apertura di sicurezza di tipo 2, pagina 369 emessa dalla CPU di origine per iniziare una connessione CIP Safety.

Configurazione dell'SNN

L'SNN è un valore esadecimale che fa parte sia della configurazione di connessione CIP Safety (configurata utilizzando Control Expert) che della configurazione del dispositivo CIP Safety (configurato utilizzando un SNCT). Tipicamente, l'SNN viene creato in Control Expert, quindi copiato (o immesso nuovamente) nel SNCT. Quindi l'SNCT produce il TUNID sulla base di SNN e indirizzo IP e trasferisce tale valore CIP Safety.

È anche possibile inviare l'SNN direttamente dal DTM di connessione CIP Safety in Control Expert al dispositivo di destinazione, pagina 377.

Per configurare l'SNN:

Pas- so	Azione
1	Nella scheda Generale > Sicurezza , fare clic sul pulsante con i puntini di sospensione (...). Si apre la finestra di dialogo Numero di rete di sicurezza .
2	<p>Nella finestra di dialogo Numero di rete di sicurezza selezionare uno dei seguenti:</p> <ul style="list-style-type: none"> • Basato sul tempo: per generare un valore esadecimale basato su giorno, mese, anno, ora, minuto, secondo e millisecondo al momento della generazione. • Manuale: per generare un valore basato su un valore decimale immesso da 1 a 9999, concatenato con due valori esadecimali, come segue: <ul style="list-style-type: none"> ◦ parola 1: 0004 (fissa) ◦ parola 2: 0000 (fissa) ◦ parola 3: 0001...270F (il valore esadecimale del valore immesso da 1...9999) • Specifico del fornitore: un identificativo specifico del fornitore basato su 3 parole esadecimali di immissione: <ul style="list-style-type: none"> ◦ parola 1: 05B5...2DA7 (dal fornitore) ◦ parola 2: 0000 (fissa) ◦ parola 3: 0001...270F (dal fornitore) • Un valore esadecimale immesso direttamente (digitato o incollato), composto da: <ul style="list-style-type: none"> ◦ parola 1: 2DA8...FFFE ◦ parola 2 & 3: 00000000...05265BFF
3	Per un formato Basato sul tempo, Manuale o Specifico del fornitore, fare clic su Genera . Nel caso si sia immesso direttamente un valore esadecimale, fare clic su Imposta .
4	Fare clic su OK per salvare l'SNN e chiudere la finestra di dialogo. L'SNN compare nel campo Numero di rete di sicurezza .

Configurazione dello SCID

Lo SCID, chiamato anche Firma di configurazione, viene impostato nello strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e rappresenta l'identificativo di configurazione esadecimale univoco per il dispositivo CIP Safety. È composto da:

- CRC di configurazione di sicurezza (SCCRC), che è un valore di controllo di ridondanza ciclico (CRC) delle impostazioni di configurazione del dispositivo di sicurezza, sotto forma di un valore esadecimale formato da 4 ottetti.
- Time stamp di configurazione di sicurezza (SCTS), un valore time stamp esadecimale di data e ora formato da 6 ottetti.

Per inserire lo SCID:

Passo	Azione
1	Ottenere dal dispositivo che utilizza l'SNCT per la connessione i seguenti: <ul style="list-style-type: none"> • SCCRC • Data (mm/gg/aaaa) e ora (hh/mm/ss/ms) in cui è stata eseguita la configurazione SNCT.
2	Selezionare Firma di configurazione .
3	Immettere l'SCCRC nel campo ID .
4	Immettere i valori di data e ora nei campi Data e Ora .

NOTA: Se le connessioni di sicurezza vengono configurate con SCID = 0 ("configura SCID disabilitato), notare che si è responsabili della verifica della corretta configurazione dell'origine di sicurezza M580 e delle destinazioni CIP Safety.

DTM dispositivo di sicurezza - Verifica e convalida della configurazione

Verifica visiva della configurazione DTM

Utilizzare la scheda **Generale > Verifica configurazione** per il DTM CIP Safety, creato con o senza file EDS del fornitore, per confrontare i parametri definiti in questo DTM (e visualizzati in questa scheda) con quelli impostati nel dispositivo di destinazione DDDT. È anche possibile utilizzare la tabella di animazione in Control Expert, quando quest'ultimo è in modalità connesso ed è collegato a una CPU.

NOTA: Dopo aver scaricato un'applicazione, è necessario verificare visivamente per ciascuna destinazione CIP Safety che tutti i parametri di configurazione CIP Safety scaricati nell'origine M580 per una certa destinazione siano identici a quelli configurati nel DTM di destinazione. Ciò si realizza confrontando i parametri di configurazione visualizzati nella destinazione DDDT di CIP Safety (utilizzando una tabella di animazione con Control Expert in modalità connesso) con quelli configurati nel DTM e visualizzati nella scheda di verifica di configurazione.

Convalida della configurazione scaricata

Dopo aver scaricato tutte le configurazioni CIP Safety, la verifica utente è lo strumento per mezzo del quale vengono convalidati tutti i download. Una delle verifiche di convalida è un test delle configurazioni di connessione di sicurezza dopo il loro utilizzo in un'origine per confermare che la connessione di destinazione stia funzionando nel modo previsto.

DTM del dispositivo di sicurezza - Connessioni I/O

Introduzione

Il DTM CIP Safety, creato con o senza file EDS del fornitore, è dotato di nodi di connessione di sicurezza. Sia i nodi di ingresso che di uscita sono supportati, secondo le funzionalità, da un dispositivo specifico. La scheda **Connessione** presenta i parametri per la connessione di ingresso o di uscita selezionata.

Per i DTM creati con un file EDS del fornitore, le connessioni predefinite sono preselezionate. È possibile utilizzare i comandi **Rimuovi connessione** e **Aggiungi connessione** per adattare le impostazioni di connessione alle esigenze della propria applicazione.

Impostazioni di connessione dell'ingresso di sicurezza

Ciascuna connessione di ingresso di sicurezza presenta i seguenti parametri:

- **Dimensioni ingresso** (lettura-scrittura): la dimensione dei dati di ingresso configurati nel dispositivo CIP Safety, in byte. Impostate su 0 per impostazione predefinita.
NOTA: È necessario sostituire il valore predefinito con le impostazioni offerte dal fornitore. Il valore 0 non è supportato.
- **Intervallo pacchetto richiesto** (lettura-scrittura): RPI rappresenta il periodo di aggiornamento della connessione. Impostato nello stesso modo di (periodo di task SAFE)/2 per impostazione predefinita.
NOTA: È possibile impostare il periodo task SAFE (Tsafe) nella finestra di dialogo **Proprietà di SAFE (Browser di progetto > Task > SAFE > Proprietà)** in Control Expert.
- **Aspettativa tempo di rete** (lettura-scrittura): il tempo, in millisecondi, impiegato dalla comunicazione, pagina 163 CIP Safety. Se il valore è inferiore all'*Aspettativa tempo di rete minima* viene visualizzata una notifica di rilevamento di errore. Per impostazione predefinita, il valore dovrebbe essere pari a *Aspettativa tempo di rete minima* * 1,5.
- **Moltiplicatore timeout** (lettura-scrittura): componente del calcolo dell'*Aspettativa tempo di rete minima*, il suo valore deve essere pari a $\text{Aspettativa tempo di rete minima} = \text{RPI} * \text{Moltiplicatore timeout} + \text{Tsafe} + 40$. μSec .

- **Trasmissione_di_rete_max** (lettura-scrittura): l'età peggiore (più lontana, in ms) di data al momento del ricevimento del pacchetto da parte dell'utilizzatore. Questo parametro è utilizzato per il calcolo del valore minimo da immettere in *Aspettativa_tempo_di_rete* (come descritto sotto). Il parametro può essere perfezionato verificando il valore *Età_dati-max* nel dispositivo utilizzatore dopo l'esecuzione della comunicazione CIP Safety per un periodo di tempo significativo sulla rete.

Questo parametro è utilizzato per il calcolo del valore minimo del "*Aspettativa_tempo_di_rete*", come segue:

$$\text{Min (Aspettativa tempo di rete)} = \text{RPI} * \text{Moltiplicatore_timeout} + \text{Trasmissione_di_rete_max}$$

Quando viene modificato *Tsafe*, il valore di questo parametro deve cambiare e, di conseguenza, il valore minimo dell'*Aspettativa_tempo_di_rete* deve cambiare a sua volta.

A questo parametro si applicano i seguenti attributi:

- Valore minimo = 1 -ms
- Valore massimo = 5800 ms
- Valore predefinito = 40 + *Tsafe*

Il DTM di dispositivo utilizza queste impostazioni di ingresso per effettuare i seguenti calcoli:

Variabile	Valore		
	Predefinito	Minimo	Massimo
Safeperiod (ms)	20	10	255
Intervallo di pacchetti richiesti in ingresso (ms)	$\text{RPI} = \text{Tsafe} / 2$	5	500
Moltiplicatore timeout	2	1	255
Trasmissione_di_rete_max (ms)	$40 + 2 * \text{Tsafe}$	10	5800
Aspettativa tempo di rete	Aspettativa_tempo_di_rete valore minimo* 1.5	$\text{RPI} * \text{Moltiplicatore_timeout} + \text{Trasmissione_di_rete_max}$	5800

Impostazioni di connessione di uscita di sicurezza

Ciascuna uscita di sicurezza presenta i seguenti parametri:

- **Dimensioni uscita** (lettura-scrittura): la dimensione dei dati di uscita configurati nel dispositivo CIP Safety, in byte. Impostate su 0 per impostazione predefinita.

NOTA: È necessario sostituire il valore predefinito con le impostazioni offerte dal fornitore. Il valore 0 non è supportato.

- **Intervallo pacchetto richiesto** (sola lettura): RPI rappresenta il periodo di aggiornamento della connessione. Impostato nello stesso modo del periodo ask SAFE (Tsafe).
- **Aspettativa tempo di rete** (lettura-scrittura): il tempo, in millisecondi, impiegato dalla comunicazione, pagina 163 CIP Safety. Se il valore è inferiore all'*Aspettativa_tempo_di_rete_minima* viene visualizzata una notifica di rilevamento di errore. Per impostazione predefinita, il valore dovrebbe essere pari a *Aspettativa_tempo_di_rete_minima* * 1,5.
- **Moltiplicatore timeout** (lettura-scrittura): componente del calcolo dell'*Aspettativa_tempo_di_rete_minima*, il suo valore deve essere pari a $Aspettativa_tempo_di_rete / 128 \mu Sec$. $Aspettativa_tempo_di_rete_minima = RPI * Moltiplicatore_timeout + Tsafe + 40$.
- **Trasmissione di rete_max** (lettura-scrittura): l'età peggiore (più lontana, in ms) di data al momento del ricevimento del pacchetto da parte dell'utilizzatore. Questo parametro è utilizzato per il calcolo del valore minimo da immettere in *Aspettativa_tempo_di_rete* (come descritto sotto). Il parametro può essere perfezionato verificando il valore *Età_dati-max* nel dispositivo utilizzatore dopo l'esecuzione della comunicazione CIP Safety per un periodo di tempo significativo sulla rete.

Questo parametro è utilizzato per il calcolo del valore minimo del "Aspettativa_tempo_di_rete", come segue:

$$\text{Min (Aspettativa tempo di rete)} = RPI * \text{Moltiplicatore_timeout} + \text{Trasmissione_di_rete_max}$$

Quando viene modificato Tsafe, il valore di questo parametro deve cambiare e, di conseguenza, il valore minimo dell'*Aspettativa_tempo_di_rete* deve cambiare a sua volta.

A questo parametro si applicano i seguenti attributi:

- Valore minimo = 1 -ms
- Valore massimo = 5800 ms
- Valore predefinito = $40 + 2 * Tsafe$

Il DTM di dispositivo utilizza queste impostazioni di uscita per effettuare i seguenti calcoli:

Variabile	Valore		
	Predefinito	Minimo	Massimo
Safeperiod (ms)	20	10	255
Intervallo di pacchetti richiesti in ingresso (ms)	$RPI = Tsafe$	10	255
Moltiplicatore timeout	2	1	255
Trasmissione_di_rete_max (ms)	$40 + 2 * Tsafe$	10	5800
Aspettativa tempo di rete	Aspettativa_tempo_di_rete valore minimo* 1.5	$RPI * Moltiplicatore_timeout + Trasmissione_di_rete_max$	5800

DTM del dispositivo di sicurezza - Impostazioni di connessione I/O

Introduzione

Il DTM CIP Safety, se creato senza un file EDS del fornitore, comprende la scheda **Impostazioni di configurazione** del nodo di connessione.

Utilizzare la scheda **Impostazioni di configurazione** per completare la configurazione della connessione tra la CPU e il dispositivo remoto.

Parametri

La scheda **Impostazioni di configurazione** include i seguenti parametri:

- **Istanza d'ingresso:** il numero gruppo specifico del gruppo dispositivo associato con le trasmissioni di ingresso (T→O).
- **Istanza di uscita:** il numero gruppo specifico del dispositivo associato con le trasmissioni di uscita (O→T).
- **Istanza di configurazione:** il numero gruppo specifico del dispositivo associato con le impostazioni di configurazione del dispositivo.

Impostazioni dell'indirizzo IP del dispositivo di sicurezza

Modiche del DTM master della CPU M580

Le impostazioni dell'indirizzo IP e DHCP per un dispositivo CIP Safety sono configurabili in DTM Master della CPU M580.

NOTA: Diversamente dalle altre impostazioni di configurazione della connessione per i dispositivi di destinazione, l'indirizzo IP del dispositivo non è impostato nel DTM di connessione del dispositivo.

Accesso alle impostazioni dell'indirizzo IP del dispositivo di sicurezza

Eeguire questa sequenza di passaggi per modificare l'indirizzo IP e i parametri DHCP del dispositivo CIP Safety:

Pas- so	Azione
1	Disconnettere Control Expert dal dispositivo di destinazione ed eseguire le seguenti modifiche offline.
2	Nel Browser DTM di Control Expert, fare doppio clic su DTM Master della CPU M580 (BMEP58_ECPU_EXT) per aprire la sua configurazione.
3	Nella struttura di navigazione, espandere l'Elenco dispositivi per visualizzare le istanze degli slave associate.
4	Selezionare il dispositivo che corrisponde al dispositivo CIP Safety.
5	Selezionare la scheda Impostazione indirizzo .

Configurazione delle impostazioni dell'indirizzo IP del dispositivo di sicurezza

Nella scheda **Impostazione indirizzo**, modificare questi parametri per il dispositivo di sicurezza selezionato:

Campo	Parametro	Descrizione
Configurazione IP	Indirizzo IP	Immettere l'indirizzo IP del dispositivo selezionato.
	Maschera di sottorete	La maschera di sottorete del dispositivo. NOTA: Impostare la subnet mask in modo tale che l'indirizzo IP del dispositivo risieda nella stessa subnet dell'indirizzo IP principale della CPU di origine.
	Gateway	L'indirizzo gateway utilizzato per raggiungere questo dispositivo. Il valore predefinito 0.0.0.0 indica che il dispositivo si trova sulla stessa subnet della CPU di origine.
Server di indirizzi	DHCP per questo dispositivo	<ul style="list-style-type: none"> • Disattivato (predefinito) disattiva il client DHCP per il dispositivo. • Attivato attiva il client DHCP in questo dispositivo.
	Identificato da	Se il servizio DHCP per questo dispositivo è Attivato, selezionare il tipo di identificativo del dispositivo: <ul style="list-style-type: none"> • Indirizzo MAC. • Nome dispositivo.
	Identificativo	Se il DHCP è Attivato e il Nome dispositivo selezionato, immettere il valore del nome dispositivo.

Per maggiori informazioni sulla configurazione dei parametri del dispositivo DTM Master della CPU M580, vedere l'argomento Parametri elenco dispositivi (vedi Modicon M580, Hardware, Manuale di riferimento).

Operazioni con CIP Safety

Panoramica

Questa sezione descrive le operazioni con CIP Safety.

Trasferimento di un'applicazione CIP Safety da Control Expert al PAC

Iniziare il download dell'applicazione

Utilizzare il comando **PLC > Trasferisci progetto a PLC** per iniziare il download.

Se il PLC è configurato con un'applicazione preesistente (la "vecchia applicazione"), viene invalidato all'inizio del download della nuova applicazione. Se la vecchia applicazione comprende dispositivi configurati, il PAC chiude le connessioni con tali dispositivi.

Fine del download dell'applicazione

La configurazione CIP Safety viene scritta nel CIP Safety Stack (CSS) della CPU, che calcola un parametro di connessione CRC (CPCRC) per ciascuna connessione. Quindi, ciascun CPCRC calcolato da CSS viene confrontato con il CPCRC corrispondente archiviato nella configurazione e calcolato dal DTM di destinazione. In caso di:

- Non corrispondenza di CPCRC, il CSS rifiuta l'applicazione e il PAC resta in stato NOCONF.
- Uguaglianza:
 - Il CPCRC e i valori dei parametri di connessione vengono copiati nel DDDT di destinazione, pagina 378 corrispondente.
 - Il parametro CSIO_HEALTH, pagina 385 all'interno del DDDT della CPU (T_BMEP58_ECPU_EXT) è impostato su 0.
 - I bit DDDT HEALTH del dispositivo, pagina 378 di destinazione CIP Safety sono impostati su 0.
 - Il PAC apre le connessioni dei dispositivi configurati tramite le Richieste di apertura di sicurezza di tipo 2, pagina 369

Nel caso di non corrispondenza di CPCRC, il CSS rifiuta l'applicazione e il PAC resta in stato NOCONF.

Ricalcolo dell'ID dell'applicazione di sicurezza

L'ID dell'applicazione di sicurezza (SAId) è una firma della parte sicura dell'applicazione Control Expert. È archiviata come parola di sistema %SW169, pagina 401. Il CSS calcola un CRC su tutte le istanze di CPCRC. Questo CRC viene aggiunto al calcolo del SAId. Quindi, una modifica alla configurazione della destinazione CIP Safety modifica il valore SAId.

Struttura della richiesta di apertura di sicurezza di tipo 2

Struttura del frame di connessione di apertura di sicurezza di tipo 2 CIP

Le CPU di sicurezza indipendenti M580 supportano le connessioni CIP Safety create da richieste di connessione di apertura di sicurezza di tipo 2 La struttura della richiesta di connessione è descritta di seguito:

Nome parametro		Descrizione
Moltiplicatore timeout di connessione		Per l'utilizzatore di una connessione, è utile a determinare se una delle tre connessioni standard debba essere in timeout. Il valore di timeout per la connessione è definito come segue: RPI di connessione * (CTM+1) * 4
O_to_T RPI		Intervallo pacchetto richiesto da origine a destinazione.
T_to_O RPI		Intervallo pacchetto richiesto da destinazione a origine.
Electronic Key.Vendor ID		Identificativo del fornitore
Electronic Key.Prod Type		Tipo di dispositivo
Electronic Key.Prod Code		Codice prodotto dispositivo
Electronic Key.Compatible/Major Rev		Revisione maggiore
Electronic Key.Minor Rev		Revisione minore
SCID	Configurazione di sicurezza CRC	Identificativo configurazione di sicurezza: fornito dallo strumento di configurazione di rete di sicurezza (SNCT), viene utilizzato durante la messa in servizio, la formazione di una connessione e la sostituzione del dispositivo.
	Data configurazione	
	Ora di configurazione	
TUNID	Data TUNID	Identificativo di rete univoco di destinazione: identifica la destinazione della richiesta di apertura di sicurezza.
	Ora TUNID	
	ID del nodo di destinazione	

Nome parametro		Descrizione
OUNID	Data OUNID	Identificativo di rete univoco di origine: identifica l'origine della richiesta di apertura di sicurezza.
	Ora OUNID	
	ID del nodo di origine	
Moltiplicatore_EPI_Intervallo_ping		Definisce l'Intervallo_conteggio_ping per la connessione.
Moltiplicatore_min_Msg_Coord_Tempo		Il numero minimo di incrementi di 128 μ S necessari al Messaggio di coordinamento di tempo per passare dall'utilizzatore al produttore.
Moltiplicatore_Aspettativa_tempo_rete		L'età massima dei dati di sicurezza, misurata con incrementi di 128 μ S, consentita da un utilizzatore.
Moltiplicatore_Timeout		Il numero di tentativi di produzione dati da includere nell'equazione per il rilevamento di connessioni fallite.
Numero_errore_max		Il numero di pacchetti errati che può essere derivato prima della chiusura della connessione.
CRC parametri di connessione (CPCRC)		CRC parametri di connessione. Un CRC-S32 di parametri di connessione di destinazione contenuti nella richiesta di apertura di sicurezza di tipo 2.

Operazioni del dispositivo CIP Safety

Introduzione

Questo argomento descrive le operazioni del dispositivo CIP Safety, compresi il sistema di rilevazione degli errori, i meccanismi di risposta e lo stato di funzionamento del dispositivo:

- Autotest all'accensione
- Risposta a errore non reversibile rilevato
- Errore reversibile rilevato
- Gestione dello stato di connessione destinazione
- Stato Run / Inattivo del dispositivo CIP Safety

Autotest all'accensione dell'origine e della destinazione CIP Safety

All'accensione, e ogni qualvolta viene caricata una nuova applicazione, il sistema CIP Safety esegue le seguenti operazioni:

- La CPU trasferisce i parametri di configurazione allo Stack CIP Safety (CSS) sia a CPU che a Copro.
- Il CSS, sia in CPU che in Copro, valuta il CPCRC per ciascuna connessione.
- Per ogni connessione, il sistema CIP Safety confronta il CPCRC (calcolato dall'origine DTM) con quelli calcolati da CPU e Copro.
- Il CSS blocca la configurazione di origine.
- L'applicazione lancia le richieste di connessione di apertura di sicurezza di tipo 2 ad ogni dispositivo CIP Safety.
- Ciascun dispositivo CIP Safety:
 - Calcola il proprio CPCRC e lo confronta con quello ricevuto dall'origine.
 - Confronta lo SCID ricevuto con quello archiviato internamente (Nota: questa verifica si applica solo ai dispositivi configurabili).

Gli scambi di I/O tra dispositivi di origine e di destinazione iniziano solo se tutte le verifiche hanno esito positivo.

NOTA: Oltre agli autotest all'accensione descritti in precedenza, il sistema esegue tutti gli autotest di runtime richiesti dagli standard CIP di sicurezza IEC 61784-3.

Risposta a errore non reversibile rilevato

Se la CPU o la diagnostica I/O rileva un errore non reversibile, il sistema di sicurezza pone la parte di sistema coinvolta in uno stato sicuro. La parte coinvolta del sistema viene spenta e non alimentata, con gli ingressi di sicurezza impostati su 0. Tutte le uscite di sicurezza coinvolte sono portate nello stato di posizionamento di sicurezza configurato.

Risposta a errore reversibile rilevato

Gli errori reversibili rilevati tipicamente comprendono eventi quali la perdita di connessione di un modulo e così via. Tali errori sono riportati nei bit Stato del DDDT del dispositivo (T_CIP_SAFETY_IO, pagina 378), che contiene il valore logico AND dei bit Status_IN e Status_OUT. Nel caso di un errore reversibile rilevato per un ingresso, il valore di quest'ultimo viene forzato in stato sicuro e impostato su 0.

Gestione dello stato di connessione destinazione

Lo stato di una connessione verso una destinazione CIP Safety è riportato nel bit Stato dei parametri Status_IN e Status_OUT come descritti nel tipo dati T_CIP_SAFETY_STATUS, pagina 379. Lo stato della destinazione può essere aperto, operativo o di errore rilevato.

Per gli ingressi, lo stato di connessione viene fornito dal convalidatore di sicurezza del server, per le uscite, lo stato di connessione viene fornito dal convalidatore di sicurezza del client.

Run / Inattivo

Lo stato operativo di un dispositivo CIP Safety, run o inattivo, è riportato nel bit Run_Inattivo del parametro Status_IN o Status_OUT come descritto nel tipo dati T_CIP_SAFETY_STATUS, pagina 379.

Per un dispositivo di ingresso:

Quando viene stabilita una connessione con un modulo di ingresso, il bit Run_Inattivo viene impostato su Inattivo (0) dal produttore (ingresso) fino a quando la sequenza di coordinamento di tempo iniziale viene completata. Dopodiché, il valore del bit può essere 1 (stato Run) o 0 (stato Inattivo). Se il bit Run_Inattivo viene impostato su 0 (stato Inattivo), i valori dei dati di ingresso vengono forzati su 0 (stato Sicuro).

Per un dispositivo di uscita:

Il bit Run_Inattivo per le uscite viene impostato su 1 dall'origine (CPU) quando il PAC è in stato Run e la sequenza di coordinamento di tempo iniziale viene completata. Lo stato Run/Inattivo per le uscite viene impostato su 0 dall'origine (CPU) quando il PAC è in stato Stop o Halt, o quando la sequenza di coordinamento di tempo iniziale non è stata completata o la connessione chiusa. Se il bit Run_Inattivo viene impostato su 0 (stato Inattivo), il dispositivo di uscita deve impostare le proprie uscite sul loro stato di posizionamento di sicurezza.

Interazioni tra le operazioni del PAC di sicurezza e la connessione di destinazione

Introduzione

Questo argomento tratta delle interazioni tra i seguenti stati/operazioni dell'origine CPU di sicurezza e la connessione del dispositivo di destinazione:

- Tempo di reazione del sistema
- Stato Run
- Stato Stop / Halt
- Ciclo accen/spegn / Riavvio
- Comando Iniz SAFE
- Modalità di manutenzione
- CCOTF

- Connessione / Disconnessione / sostituzione di un dispositivo

Tempo di reazione del sistema

Il tempo impiegato dalla comunicazione CIP Safety, chiamato *aspettativa tempo di rete*, viene aggiunto al e fa parte del *tempo di reazione del sistema* M580. Per maggiori informazioni, vedere l'argomento *Impatto delle comunicazioni CIP Safety* sul tempo di reazione del sistema di sicurezza

Stato Run

Quando il sistema CIP Safety sta funzionando in stato Run:

- I bit di stato nel DDDT, pagina 378 di comunicazione del dispositivo CIP Safety vengono aggiornati all'inizio del ciclo task SAFE.
- I valori di ingresso vengono aggiornati all'inizio del ciclo task SAFE, sulla base del valore ricevuto più recentemente.
- Dopo l'esecuzione del programma task SAFE i valori di uscita sono aggiornati e trasmessi.
- Il bit Run_Inattivo per le uscite nel DDDT di comunicazione del dispositivo CIP Safety viene impostato su 1.
- I bit di stato nel DDDT di comunicazione del dispositivo CIP Safety vengono aggiornati.

Stato Stop

Quando il task SAFE entra nello stato Stop, ad esempio se il task SAFE viene arrestato o ha raggiunto il punto di interruzione:

- La connessione da origine a destinazione resta aperta.
- Gli scambi di dati tra CPU e dispositivi CIP Safety vengono eseguiti.
- I bit di stato nel DDDT, pagina 378 di comunicazione del dispositivo CIP Safety continuano ad essere aggiornati.
- Il bit Run_Inattivo per le uscite nel DDDT di comunicazione del dispositivo CIP Safety viene impostato su 0 e i dispositivi di uscita applicano l'impostazione di posizionamento di sicurezza configurata.

Stato Halt

Nello stato Halt, i valori di uscita non sono inviati dalla CPU al dispositivo CIP Safety e i bit di stato di quest'ultimo sono impostati su 0.

Ciclo accen/spegn o Reset

In un ciclo accen/spegn o reset:

- La parte di sicurezza dell'applicazione esegue un riavvio a freddo, pagina 270.
- Il PAC esegue la stessa sequenza di operazioni che viene eseguita per il download dell'applicazione, pagina 368.

Comando Iniz SAFE

L'esecuzione del comando **PLC > Iniz Safety** in Control Expert inizializza i valori del DDDT di comunicazione del dispositivo CIP Safety, pagina 378, impostandoli sui valori predefiniti di fabbrica.

Modalità di manutenzione

Il funzionamento della CPU di sicurezza M580 in modalità manutenzione, pagina 258 non ha impatti sul funzionamento del dispositivo CIP Safety. La CPU continua a confrontare i calcoli eseguiti separatamente da CPU e Copro. Tuttavia, non vi saranno confronti aggiuntivi ai valori nel DDDT di destinazione. Quindi, il funzionamento del PAC in modalità manutenzione non si può considerare sicuro.

CCOTF

La funzione di modifica della configurazione in corso d'opera (CCOTF) non è supportata dai dispositivi CIP Safety. Poiché un dispositivo CIP Safety ottiene le impostazioni di configurazione da uno strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e non dalla CPU di origine, le modifiche alle impostazioni del dispositivo non possono essere effettuate dalla CPU.

Connessione / Disconnessione / sostituzione di un dispositivo CIP Safety

Per impostazione predefinita, sulla base dell'avvio dell'applicazione o l'esecuzione di un comando **PLC > Iniz Safety**, i bit CTRL_IN e CTRL_OUT in DDDT, pagina 378 sono impostati su Attivato (1). Quando un dispositivo viene collegato a un PAC in modalità Stop o Run e i bit CTRL_IN o CTRL_OUT del dispositivo sono impostati su Attivato (1), il dispositivo inizia automaticamente gli scambi di dati.

NOTA: Siccome i bit CTRL_IN e CTRL_OUT sono impostati su Attivato in un ciclo di accensione/spengimento, è necessario adottare misure adeguate nell'applicazione SAFE per evitare funzionamenti non previsti quando viene eseguito un ciclo accensione/spengimento.

⚠ AVVERTIMENTO

RISCHIO DI FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Non utilizzare i bit CTRL_IN e CTRL_OUT come misure di sicurezza per impostare i dati di destinazione in uno stato sicuro.

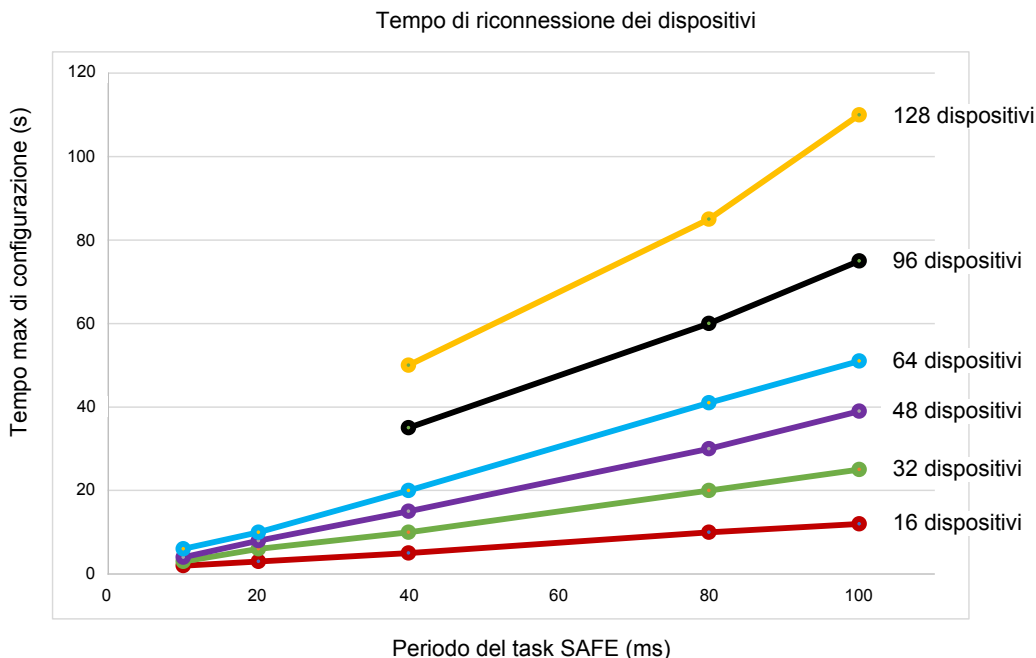
Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Quando il PAC rileva un errore che necessita della chiusura di una connessione del dispositivo, il PAC imposta il bit CTRL_IN o CTRL_OUT corrispondente su Disattivato (0). Il dispositivo resta in stato disabilitato e ritorna nello stato Attivato (1) se la transizione è stata prevista. Ad esempio, se l'errore viene azzerato e viene eseguita una richiesta di riapertura di connessione.

È possibile eseguire una richiesta di riapertura di connessione reimpostando il bit di controllo corrispondente (CTRL_IN o CTRL_OUT) da Disattivato (0) a Attivato (1) nel DDDT.

Quando un dispositivo viene nuovamente connesso, il tempo di connessione dipende dal periodo task SAFE e il numero di dispositivi connessi:

- Per un dispositivo singolo con un periodo task SAFE inferiore a 100 ms, il tempo stimato per la connessione è inferiore a 2 secondi.
- Per dispositivi multipli, vedere il grafico seguente per i tempi di connessione stimati.



Il PAC CIP Safety tratta la sostituzione di un dispositivo allo stesso modo di una disconnessione e successiva connessione. Le operazioni per riconfigurare il nuovo dispositivo con le stesse impostazioni di quello sostituito sono locali per il dispositivo e non coinvolgono il PAC.

Comandi DTM CIP Safety

Introduzione

Il DTM CIP Safety comprende la scheda **Sicurezza**, che presenta i seguenti comandi:

- **RESET proprietà**
- **Mettere TUNID**

È possibile accedere a questi comandi selezionando una connessione nella struttura ad albero del DTM, quindi vengono abilitati soltanto quando il DTM collegato al dispositivo CIP Safety è in funzione online.

Proprietà RESET

utilizzare il comando **Proprietà RESET** per eseguire un reset delle impostazioni di configurazione del dispositivo CIP Safety ai valori out-of-the-box predefiniti di fabbrica. Un reset può essere eseguito solo se:

- Il comando viene eseguito dalla CPU di origine identificata con l'OUNID archiviato nel dispositivo.
- Le impostazioni di configurazione del modulo non sono bloccate.

Dopo il reset, il modulo non ha proprietario e può essere configurato da un'altra origine.

NOTA: Se viene eseguito un reset su un modulo con connessioni operative, il comando reset non avrà efficacia.

Mettere TUNID

Utilizzare il comando **Mettere TUNID** per impostare il Numero di rete di sicurezza (SNN) nel dispositivo CIP Safety di destinazione. In esecuzione, il Numero di rete di sicurezza, pagina 360 archiviato nella configurazione del DTM del dispositivo CIP Safety viene trasferito al dispositivo di destinazione e sovrascrive il valore SNN già esistente nel dispositivo.

NOTA: Prima di eseguire questo comando, confermare che si è identificato il dispositivo corretto per la ricezione dell'SNN che si intende trasferire.

Diagnostica CIP Safety

Panoramica

Questa sezione presenta gli strumenti di diagnostica per il dispositivo CIP Safety, la connessione tra il dispositivo e la CPU indipendente Safety M580.

DDDT del dispositivo CIP Safety

T_CIP_SAFETY_IO DDDT

Ciascuna istanza al dispositivo CIP Safety è descritta da T_CIP_SAFETY_IO DDDT, composto dai seguenti parametri:

Parametro	Tipo di dati	Descrizione
Stato	BOOL	Stato globale = AND logico di <ul style="list-style-type: none"> • Status_IN.Health • Status_OUT.Health Consultare i tipi di dati T_CIP_SAFETY_STATUS, pagina 379 per una descrizione di queste parti di stato.
Status_IN	T_CIP_SAFETY_STATUS	Stato ingresso.
Status_OUT	T_CIP_SAFETY_STATUS	Stato uscita.
CTRL_IN	BOOL	Attivare/disattivare la connessione di ingresso.
CTRL_OUT	BOOL	Attivare/disattivare la connessione di uscita.
Conf_In	T_CIP_SAFETY_CONF	Le firme e i parametri CIP per la connessione di ingresso.
Conf_Out	T_CIP_SAFETY_CONF	Le firme e i parametri CIP per la connessione di uscita.
Ingresso	Array[0...n] di BYTE	Valori di ingresso, la dimensione dipende dal tipo di dispositivo. Modulo allineato da 4 byte con dimensione configurata all'interno del DTM.
Uscita	Array[0...m] di BYTE	Valori di uscita, la dimensione dipende dal tipo di dispositivo. Modulo allineato da 4 byte con dimensione configurata all'interno del DTM.

I tipi di dati CIP Safety a cui si è fatto riferimento sopra sono descritti di seguito.

T_CIP_SAFETY_STATUS

Il tipo di dati T_CIP_SAFETY_SATATUS è composto dai seguenti parametri:

Parametro	Tipo di dati	Descrizione
Stato operativo	BOOL	Stato ingresso o uscita: <ul style="list-style-type: none"> • Per ingresso: <ul style="list-style-type: none"> ◦ 1: la comunicazione in ingresso è aperta e funzionante. ◦ 0: errore rilevato per la comunicazione in ingresso dal convalidatore di sicurezza del server. • Per uscita: <ul style="list-style-type: none"> ◦ 1: la comunicazione in uscita è aperta e funzionante. ◦ 0: errore rilevato per la comunicazione in uscita dal convalidatore di sicurezza del client.
Run_Inattivo	BOOL	Stato degli ingressi o delle uscite del dispositivo CIP Safety: <ul style="list-style-type: none"> • Per gli ingressi, è impostato dal produttore (ingresso): <ul style="list-style-type: none"> ◦ 1: se l'ingresso è in stato Run. ◦ 0: se l'ingresso è in stato Inattivo, o fino al corretto completamento della sequenza di coordinamento di tempo iniziale. • Per le uscite, è impostato dall'origine (CPU): <ul style="list-style-type: none"> ◦ 1: se il PAC è in stato Run, o dopo il corretto completamento della sequenza di coordinamento di tempo iniziale. ◦ 0: se il PAC è in stato Stop o Halt, se la connessione è chiusa, o se la sequenza di coordinamento di tempo iniziale non è stata completata.
Codice_errore	WORD	Vedere l'elenco dei codici di errore individuati, pagina 381.
Sottocodice_errore	WORD	Vedere l'elenco dei sottocodici di errore individuati, pagina 382.

T_CIP_SAFETY_CONF

Il tipo di dati T_CIP_SAFETY_CONF è composto dai seguenti parametri, che vengono trasmessi nella Richiesta di apertura di sicurezza di tipo 2, pagina 369:

Parametro	Tipo di dati	Descrizione
TO_MULTIPLIER	BYTE	Moltiplicatore timeout. Per l'utilizzatore di una connessione, è utile a determinare se una delle tre connessioni standard debba essere in timeout. Il valore di timeout per la connessione è definito come segue: RPI di connessione * (CTM+1) * 4
RPI_uscita	UDINT	Intervallo pacchetto richiesto della connessione O→T.
RPI_ingresso	UDINT	Intervallo pacchetto richiesto della connessione T→O.
ID_fornitore_dispositivo	UINT	Identificativo del fornitore ODVA.
Tipo_dispositivo	UINT	Raggruppamento ODVA a cui appartiene il dispositivo.
Codice_prodotto_dispositivo	UINT	Codice prodotto assegnato da ODVA.
Revisione_maggiore	BYTE	Numero della revisione maggiore del firmware del dispositivo.
Revisione_minore	BYTE	Numero della revisione minore del firmware del dispositivo.
Nb_assembly_configurazione	UINT	Il numero gruppo specifico del dispositivo associato con le impostazioni di configurazione del dispositivo.
Nb_assembly_uscita	UINT	Il numero gruppo specifico del dispositivo associato con le trasmissioni di uscita (O→T).
Nb_assembly_ingresso	UINT	Il numero gruppo specifico del dispositivo associato con le trasmissioni di ingresso (T→O).
CRC_SC	UDINT	Configurazione di sicurezza CRC. Un controllo di ridondanza ciclico (CRC) della configurazione del dispositivo CIP Safety.
Data_configurazione	UINT	Mese, giorno e anno della creazione della configurazione.
Ora_configurazione	UDINT	Ora, minuto, secondo e millisecondo della creazione della configurazione.
Ora_TUNID	UDINT	Mese, giorno e anno in cui è stato generato l'identificativo univoco di rete di destinazione.
Data_TUNID	UINT	Ora, minuto, secondo e millisecondo in cui è stato generato l'identificativo univoco di rete di destinazione.
IDnodo_TUNID	UDINT	Un identificativo univoco di rete per il dispositivo di destinazione.
Ora_OUNID	UDINT	Mese, giorno e anno in cui è stato generato l'identificativo univoco di rete dell'origine.
Data_OUNID	UINT	Ora, minuto, secondo e millisecondo in cui è stato generato l'identificativo univoco di rete dell'origine.

Parametro	Tipo di dati	Descrizione
IDnodo_OUID	UDINT	Un identificativo univoco di rete per il dispositivo di origine.
Moltiplicatore_EPI_Intervallo_ping	UINT	Definisce l'Intervallo_conteggio_ping per la connessione.
Moltip_min_mess_coordinamento_tempo	UINT	Il numero minimo di incrementi di 128 μ S necessari al Messaggio di coordinamento di tempo per passare dall'utilizzatore al produttore.
Moltip_aspettative_tempo_rete	UINT	L'età massima dei dati di sicurezza, misurata con incrementi di 128 μ S, consentita da un utilizzatore.
Moltiplicatore_Timeout	BYTE	Il numero di tentativi di produzione dati da includere nell'equazione per il rilevamento di connessioni fallite.
Numero_errore_max	UDINT	Il numero di pacchetti errati che può essere derivato prima della chiusura della connessione.
CPCRC	UDINT	CRC parametri di connessione. Un CRC-S32 di parametri di connessione di destinazione contenuto nella richiesta di apertura di sicurezza di tipo 2.

Codici di errore del dispositivo CIP Safety

Codici di errore rilevato

I seguenti codici e sottocodici di errore rilevato si applicano al tipo di dati T_CIP_SAFETY_STATUS e sono compresi nei parametri Status_IN e Status_OUT del DDDT del dispositivo CIP Safety.

Codici di errore rilevato

Codice errore rilevato	Significato
0001	Connessione aperta, nessuna risposta.
0002	Connessione aperta, rilevato errore di risposta dal dispositivo.
0003	Connessione aperta, risposta non valida dal dispositivo.
0004	Il server (utilizzatore) non è in funzione.
0005	Il client (produttore) non è in funzione.

Sottocodici di errore rilevato

NOTA: Tutti i sottocodici di errore rilevato diversi da quelli elencati di seguito sono previsti per il solo utilizzo interno di Schnieder Electric. In tal caso, è necessario riferire il sottocodice di errore rilevato al personale di Schnieder Electric.

Sottocodici di errore rilevato per connessioni aperte:

Sottocodice di errore rilevato (hex)	Significato
0100	Connessione in uso o Forward_Open doppio.
0103	Classe di trasporto e combinazione di trigger non supportate.
0105	La configurazione appartiene già ad un'altra origine.
0106	L'uscita appartiene già ad un'altra origine.
0107	Connessione di destinazione non trovata (Invia_Chiusura).
0108	Parametro di connessione di rete non valido.
0109	Dimensioni connessione non valide.
0110	Dispositivo non configurato.
0111	O->T RPI, T->O RPI o RPI correzione di tempo non supportata.
0113	Tutte le Istanze del convalidatore di sicurezza sono in uso.
0114	ID_fornitore_dispositivo o Codice_prodotto_dispositivo specificati nella chiave elettronica non corrispondono.
0115	Il Tipo_dispositivo specificato nella chiave elettronica non corrisponde.
0116	Revisione_maggiore o Revisione_minore specificate nella chiave elettronica non corrispondono.
0117	Percorso applicazione prodotta o utilizzata non valido.
0118	Percorso applicazione configurazione non valido o incoerente.
011 A	Oggetto destinazione fuori da connessioni.
011B	RPI inferiore a tempo inibizione produzione.
011C	Classe di trasporto non supportata.
011D	Trigger di produzione non supportato.
011E	Direzione non supportata.
0123	Tipo di connessione di rete da origine a destinazione non valido.
0124	Tipo di connessione di rete da destinazione a origine non valido.
0126	Dimensione configurazione non valida.

Sottocodice di errore rilevato (hex)	Significato
0127	Dimensione da origine a destinazione non valida.
0128	Dimensione da destinazione a origine non valida.
0129	Percorso applicazione configurazione non valido.
012A	Percorso applicazione utilizzatrice non valido.
012B	Percorso applicazione produttrice non valido.
012C	Il simbolo di configurazione è inesistente.
012D	Il simbolo di utilizzo è inesistente.
012E	Il simbolo di produzione è inesistente.
012F	Combinazione percorso dell'applicazione incoerente.
0130	Formato data di utilizzo incoerente.
0131	Formato data di produzione incoerente.
0203	Timeout connessione.
0204	La destinazione non risponde a richieste non collegate.
0205	Errore rilevato parametro in richiesta di apertura di sicurezza.
0207	Riconoscimento non collegato senza risposta.
0315	Tipo di segmento non valido in percorso connessione.
031B	Connessione modulo già stabilita.
031C	Non può essere applicato nessun altro codice di stato esteso.
031F	Nel modulo di produzione non sono più disponibili i collegamenti configurabili alle risorse per l'utilizzatore.
0801	Moltiplicatore_EIP_Intervallo_Ping o Numero_consumatore_max non valido per unione multicast.
0802	Dimensione di connessione di sicurezza non valida.
0803	Formato di connessione di sicurezza non valido.
0804	Parametri di connessione correzione di tempo non validi.
0805	Moltiplicatore_EIP_intervallo_ping non valido.
0806	Moltiplicatore_min_Msg_coordinamento_tempo non valido.
0807	Moltiplicatore_aspettativa_tempo_rete non valido.
0808	Moltiplicatore timeout non valido.
0809	Numero max utilizzatore non valido.

Sottocodice di errore rilevato (hex)	Significato
080A	CPCRC non valido.
080B	ID di connessione di correzione di tempo non valido.
080C	SCID non corrispondente.
080D	TUNID non impostato.
080E	TUNID non corrispondente.
080F	Funzionamento di configurazione non consentito.

Sottocodici di errore rilevato per server o client:

Sottocodice di errore rilevato (hex)	Significato
271D	Il Messaggio di coordinamento di tempo è stato ricevuto con un bit Risposta_ping non impostato.
2730	Messaggio di coordinamento di tempo non ricevuto nel tempo assegnato.
2732	Verifica messaggio di coordinamento di tempo: messaggio con stesso time stamp già ricevuto da questo utilizzatore.
2733	Verifica messaggio coordinamento di tempo: controllo parità errore rilevato.
2734	Verifica messaggio coordinamento di tempo: verifica Ack_Byte_2 errore rilevato.
2735	Verifica messaggio di coordinamento di tempo: non ricevuto entro il limite di circa 5 secondi.
2736	Verifica messaggio di coordinamento di tempo: non ricevuto entro lo stesso o il successivo intervallo di ping.
2738	Verifica messaggio coordinamento di tempo: CRC non corrispondente.
2820	CRC di time stamp non corrispondente.
2821	Delta di time stamp pari a zero.
2822	Delta di time stamp maggiore dell'Aspettativa tempo di rete.
2823	Età dei dati di un messaggio errato maggiore dell'Aspettativa tempo di rete.
2824	Età dei dati di un messaggio valido sotto altri aspetti maggiore dell'Aspettativa tempo di rete.
2825	CRC dati effettivi non corrispondente.
2826	CRC dati complementari non corrispondente.
282E	CRC dati effettivi non corrispondente (nessuna chiusura della connessione).

Sottocodice di errore rilevato (hex)	Significato
282F	CRC dati complementari non corrispondente (nessuna chiusura della connessione).
2832	Timeout del monitor di attività dell'utilizzatore.

DDDT CPU indipendente CIP Safety

Aggiunte CIP Safety a T_BMEP58_ECPU_EXT

Il DDDT CPU di sicurezza indipendente M580 (T_BMEP58_ECPU_EXT) comprende due variabili CIP Safety:

- CSIO_SCANNER: lo stato del bit di controllo dello scanner I/O CIP Safety. Questo campo Booleano può essere:
 - 1: il servizio funziona correttamente.
 - 0: il servizio non funziona correttamente.

Per ulteriori informazioni, vedere l'elenco dei parametri di ingresso (vedere Modicon M580, Hardware, Manuale di riferimento) SERVER_STATUS2 DDDT.

- CSIO_HEALTH: lo stato dei dispositivi CIP Safety collegati. Questa variabile è un array di 128 valori Booleani, in cui ciascun bit indica lo stato di un singolo dispositivo collegato:
 - 1: il servizio funziona correttamente.
 - 0: il servizio non funziona correttamente.

Per ulteriori informazioni, vedere l'argomento Stato dispositivo (vedere Modicon M580, Hardware, Manuale di riferimento).

Diagnostica DTM CPU

Diagnostica mediante DTM CPU M580

Il DTM CPU M580 fornisce i seguenti servizi di diagnostica:

- Rilevamento dispositivo
- Stato del dispositivo I/O CIP Safety

Rilevamento dispositivo di sicurezza CIP



Quando Control Expert funziona online, è possibile utilizzare il suo servizio di rilevamento bus di campo per individuare i dispositivi CIP Safety di primo livello, ossia i dispositivi collegati direttamente alla CPU presenti nella propria rete. Sono individuabili solo i dispositivi con un DTM che corrisponde al DTM registrato nel **Catalogo DTM** del PC host.

Il rilevamento del dispositivo viene eseguito facendo clic con il pulsante destro del mouse sul DTM CPU (BMEP58_ECPU_EXT) in **Browser DTM**, quindi selezionando **Rilevamento bus di campo** per aprire una finestra di dialogo con lo stesso nome, che permette di visualizzare i dispositivi individuati. È possibile utilizzare gli strumenti di questa finestra di dialogo per aggiungere i DTM dispositivo al proprio progetto. I dispositivi aggiunti vengono visualizzati sotto la CPU sia in **Browser DTM** sia nella struttura ad albero del DTM CPU.

Per ulteriori informazioni su come utilizzare questo servizio, vedere l'argomento Servizio di rilevamento del bus di campo (vedere l'argomento [™]EcoStruxure Control Expert, Modalità operative).

Stato connessione dispositivo CIP Safety

Quando Control Expert è in funzione online, la struttura ad albero del DTM CPU visualizza un'icona che indica lo stato di ciascuna connessione per i dispositivi di I/O CIP Safety aggiunti al progetto:

-  indica che la CPU è in stato RUN.
-  indica che la connessione è in stato STOP, o non connesso, o sconosciuto.

Per ulteriori informazioni su come utilizzare questa funzione, consultare l'argomento Introduzione della diagnostica nel DTM Control Expert (vedere Modicon M580, Hardware, Manuale di riferimento).

Diagnostica di connessione del dispositivo CIP Safety

Introduzione

I nodi di connessione del DTM CIP Safety comprendono due schede utilizzabili per identificare e diagnosticare la connessione del dispositivo:

- Informazioni modulo
- Informazioni stato

Scheda Informazioni del modulo

Il DTM CIP Safety presenta la scheda **Informazioni del modulo**, che fornisce valori statici per i seguenti parametri di identificazione del modulo:

- ID fornitore
- Tipo prodotto
- Codice prodotto
- Revisione software
- Numero di serie
- Nome prodotto
- Indirizzo Mac

Scheda Informazioni di stato

Il DTM CIP Safety presenta la scheda **Informazioni di stato**, che fornisce valori dinamici per la connessione da CPU a dispositivo CIP Safety:

Stato	Descrizione
Stato CIP Safety	<p>Lo stato attuale del dispositivo, come definito dalla sezione 5-4.2.1.5 "Stato dispositivo" dello standard CIP Safety:</p> <ul style="list-style-type: none"> • 0: non definito • 1: verifica automatica • 2: inattivo • 3: eccezione verifica automatica • 4: in esecuzione • 5: interrotto • 6: errore critico • 7: configurazione • 8 = in attesa TUNID • 9...50: riservati • 51: in attesa TUNID con coppia consentita <small>Vedere NOTA</small> • 52: in esecuzione con coppia consentita <small>Vedere NOTA</small> • 53...99: specifiche dispositivo • 100...255: specifiche fornitore <p>NOTA: Consentiti e definiti solo nei profili del Dispositivo movimento di sicurezza: 0x2E, 0x2F.</p>
Stati di eccezione	<p>Un attributo a byte singolo il cui valore indica lo stato degli allarmi e avvisi per il dispositivo. Può essere fornito come metodo di base o espanso. Per maggiori dettagli, vedere la sezione 5-4.2.1.6 "Stati di eccezione" dello standard CIP Safety.</p>

Stato	Descrizione
Errore maggiore	Condizione specifica del dispositivo. Per maggiori dettagli, vedere il Manuale dispositivo.
Errore minore	Condizione specifica del dispositivo. Per maggiori dettagli, vedere il Manuale dispositivo.
Indirizzo IP	Indirizzo IP del dispositivo CIP Safety, impostato nel DTM di CPU, pagina 366 M580.
TUNID	Identificativo di rete univoco di destinazione
OUNID	Identificativo di rete univoco di origine, pagina 350
Stato di blocco	Lo stato della configurazione del dispositivo, come configurato utilizzando uno strumento di configurazione di rete di sicurezza (SNCT): <ul style="list-style-type: none">• Bloccato: configurazione di sola lettura.• Sbloccato: configurazione lettura-scrittura.
Firma configurazione	La connessione del dispositivo di destinazione Identificativo di configurazione di sicurezza (SCID, pagina 361).

Appendici

Contenuto della sezione

IEC 61508	390
Oggetti di sistema	398
Riferimenti SRAC.....	404

Introduzione

Le appendici contengono informazioni su IEC 61508 e la relativa policy SIL. Inoltre, sono forniti i dati tecnici dei moduli di sicurezza e non interferenti con esecuzione di calcoli di esempio.

IEC 61508

Contenuto del capitolo

Informazioni generali su IEC 61508	391
Policy SIL	393

Introduzione

Questo capitolo fornisce informazioni sui concetti Safety del IEC 61508 in generale e sulla relativa policy SIL in particolare.

Informazioni generali su IEC 61508

Introduzione

I sistemi correlati alla sicurezza sono sviluppati per l'uso nei processi in cui i rischi per le persone, l'ambiente, l'apparecchiatura e la produzione devono essere tenuti a un livello accettabile. Il rischio dipende dalla gravità e dalla probabilità, quindi definendo le necessarie misure di protezione.

Per quanto riguarda la sicurezza dei processi, occorre considerare due aspetti:

- le normative e i requisiti definiti dagli enti ufficiali per la protezione di persone, ambiente, apparecchiatura e produzione
- le misure per cui tali normative e requisiti vengono soddisfatti

Descrizione di IEC 61508

Lo standard tecnico che definisce i requisiti per i sistemi correlati alla sicurezza è

- l'IEC 61508.

Il suo scopo è la sicurezza funzionale di sistemi correlati alla sicurezza elettrici, elettronici o elettronici programmabili. Un sistema di sicurezza è un sistema che deve eseguire una o più funzioni specifiche per garantire che i rischi siano mantenuti a un livello accettabile. Queste funzioni sono definite funzioni di sicurezza (Safety Functions). Un sistema viene definito sicuro dal punto di vista funzionale se guasti casuali, sistematici o di causa comune non inducono un malfunzionamento del sistema e non provocano lesioni o morte delle persone, danni ambientali e perdite di apparecchiature e di produzione.

Lo standard definisce un approccio generico a tutte le attività nel ciclo di vita dei sistemi utilizzati per eseguire funzioni di sicurezza. È costituito dalle procedure da utilizzare per la progettazione, lo sviluppo e la convalida di hardware e software applicati nei sistemi correlati alla sicurezza. Inoltre, determina le regole che riguardano la gestione della sicurezza funzionale e la documentazione.

Descrizione di IEC 61511

I requisiti di sicurezza funzionale definiti nella IEC 61508 sono perfezionati appositamente per l'industria di processo nei seguenti standard tecnici:

- IEC 61511: sicurezza funzionale - sistemi strumentali di sicurezza per l'industria di processo

Questo standard guida l'utente nell'applicazione di un sistema correlato alla sicurezza, a partire dalla fase iniziale di un progetto, proseguendo con l'avvio, contemplando modifiche ed eventuali attività di dismissione dal servizio. Riepilogando, si occupa del ciclo di vita di sicurezza di tutti i componenti di un sistema correlato alla sicurezza utilizzato nell'industria di processo.

Descrizione dei rischi

IEC 61508 si basa sui concetti di analisi del rischio e funzione di sicurezza. Il rischio dipende da gravità e probabilità: Può essere ridotto a un livello tollerabile applicando una funzione di sicurezza che consiste di un sistema elettrico, elettronico o elettronico programmabile. Inoltre, deve essere ridotto a un livello che sia il più basso ragionevolmente praticabile.

Riepilogando, IEC 61508 vede i rischi come segue:

- Il rischio zero non è mai raggiungibile.
- La sicurezza deve essere considerata fin dall'inizio.
- I rischi intollerabili devono essere ridotti.

Policy SIL

Introduzione

Il valore SIL valuta la robustezza di un'applicazione rispetto ai guasti, indicando perciò la capacità di un sistema di eseguire una funzione di sicurezza in una probabilità definita. La IEC 61508 specifica 4 livelli di prestazioni di sicurezza che dipendono dal rischio o impatti causati dal processo per cui si utilizza il sistema correlato alla sicurezza. Più pericolosi sono i possibili impatti su comunità e ambiente, maggiori sono i requisiti di sicurezza per ridurre il rischio.

Descrizione valore SIL

Livello discreto (1 su 4) per la specifica dei requisiti di integrità di sicurezza delle funzioni di sicurezza che deve essere assegnato ai sistemi, dove il livello di integrità di sicurezza 4 è il più alto e il livello 1 il più basso, vedere SIL per bassa richiesta, pagina 395.

Descrizione dei requisiti SIL

Per raggiungere la sicurezza funzionale, sono necessari due tipi di requisiti:

- Requisiti della funzione di sicurezza, che definiscono quali funzioni di sicurezza devono essere eseguite
- Requisiti di integrità di sicurezza, che definiscono il grado di certezza necessario di esecuzione delle funzioni di sicurezza

I requisiti della funzione di sicurezza derivano dall'analisi del pericolo e quelli dell'integrità di sicurezza dalla valutazione del rischio.

Consistono delle seguenti quantità:

- Tempo medio tra i guasti
- Probabilità di guasto
- Frequenza di guasto
- Copertura diagnostica
- Frazione di guasti di sicurezza
- Tolleranza di errore hardware

In base al livello di integrità di sicurezza, queste quantità devono essere comprese tra limiti definiti.

NOTA: La combinazione di dispositivi con livelli di integrità di sicurezza differenti su una rete o una funzione di sicurezza richiede un elevato livello di attenzione relativamente ai requisiti di IEC 61508 e genera implicazioni progettuali e operative.

Descrizione della classificazione SIL

Come definito nella IEC 61508, il valore SIL è limitato dalla Frazione di guasti sicurezza (SFF) e dalla Tolleranza di errore hardware (HFT) del sottosistema che esegue la funzione di sicurezza. Un HFT pari a n significa che $n+1$ errori possono provocare una perdita della funzione di sicurezza, non è possibile accedere allo stato di sicurezza. SFF dipende dalla frequenza guasti e dalla copertura diagnostica.

La tabella seguente mostra la relazione tra SFF, HFT e SIL per sottosistemi correlati alla sicurezza complessi in base a IEC 61508-2, in cui le modalità di guasto di tutti i componenti non possono essere completamente definite:

SFF	HFT = 0	HFT = 1	HFT = 2
$SFF \leq 60\%$	-	SIL 1	SIL 2
$60\% < SFF \leq 90\%$	SIL 1	SIL 2	SIL 3
$90\% < SFF \leq 99\%$	SIL 2	SIL 3	SIL 4
$SFF > 99\%$	SIL 3	SIL 4	SIL 4

Vi sono due modi per raggiungere un determinato livello di integrità di sicurezza:

- aumentando HFT fornendo ulteriori percorsi di arresto indipendenti
- aumentando SFF tramite ulteriore diagnostica

Descrizione della relazione a richiesta SIL

La IEC 61508 distingue tra modalità a bassa richiesta e modalità ad alta richiesta (o continua) di funzionamento.

Nella modalità a bassa richiesta, la frequenza della richiesta per il funzionamento fatta su un sistema correlato alla sicurezza non è maggiore di 1 all'anno e non maggiore del doppio della frequenza di test di tenuta. Il valore SIL per un sistema correlato alla sicurezza a bassa richiesta è legato direttamente alla probabilità media dell'impossibilità di eseguire la propria funzione di sicurezza su richiesta oppure, semplicemente, alla probabilità di guasto su richiesta (PFD).

Nella modalità ad alta richiesta o continua, la frequenza di richiesta di operatività fatta su un sistema correlato alla sicurezza è maggiore di 1 all'anno e maggiore del doppio della frequenza di test di tenuta. Il valore SIL per un sistema correlato alla sicurezza ad alta

richiesta è direttamente legato alla probabilità che si verifichi un guasto pericoloso all'ora oppure, semplicemente, alla probabilità di guasto all'ora (PFH).

SIL per bassa richiesta

La tabella seguente elenca i requisiti per un sistema nella modalità di funzionamento a bassa richiesta:

Livello di integrità della sicurezza	Probabilità di guasto su richiesta
4	$\geq 10^{-5} - < 10^{-4}$
3	$\geq 10^{-4} - < 10^{-3}$
2	$\geq 10^{-3} - < 10^{-2}$
1	$\geq 10^{-2} - < 10^{-1}$

SIL per alta richiesta

La tabella seguente elenca i requisiti per un sistema nella modalità di funzionamento ad alta richiesta:

Livello di integrità della sicurezza	Probabilità di guasto/ora
4	$\geq 10^{-9} - < 10^{-8}$
3	$\geq 10^{-8} - < 10^{-7}$
2	$\geq 10^{-7} - < 10^{-6}$
1	$\geq 10^{-6} - < 10^{-5}$

Per SIL3, le probabilità richieste di guasto per il sistema integrato di sicurezza completo sono:

- PFD $\geq 10^{-4} - < 10^{-3}$ per bassa richiesta
- PFH $\geq 10^{-8} - < 10^{-7}$ per alta richiesta

Descrizione del loop di sicurezza

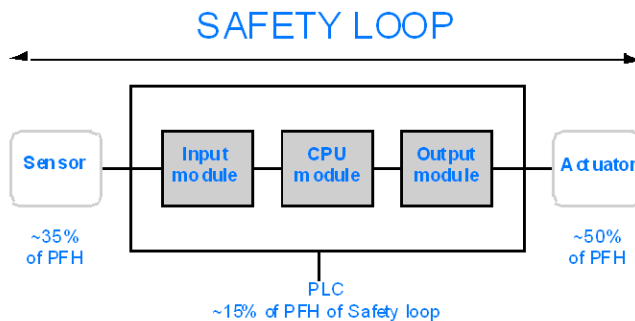
Il loop di sicurezza con il PAC M580 Safety è composto dalle seguenti 3 parti:

- Sensori

- PAC M580 Safety con alimentatore di sicurezza, CPU di sicurezza, coprocessore di sicurezza e moduli I/O di sicurezza
- Attuatori

Un backplane o una connessione remota comprendente uno switch o un CRA non distrugge un loop di sicurezza. I backplane, gli switch e i moduli CRA sono parte di un canale nero. Questo significa che lo scambio di dati tra gli I/O e il PAC non può danneggiarsi senza alcun rilevamento da parte del ricevente.

La seguente figura mostra un loop di sicurezza tipico:



Come mostrato nella figura precedente, il contributo del PAC è solo del 10-20% in quanto la probabilità di guasto di sensori e attuatori è in genere più alta.

Un presupposto conservativo del 10% per la contribuzione del PAC di sicurezza sulla probabilità globale lascia maggiore margine per l'utente e determina le seguenti probabilità richieste di guasto per il PAC di sicurezza:

- $\text{PFD} \geq 10^{-5}$ - $< 10^{-4}$ per bassa richiesta
- $\text{PFH} \geq 10^{-9}$ - $< 10^{-8}$ per alta richiesta

Descrizione dell'equazione PFD

La IEC 61508 presume che metà dei guasti finisca in uno stato di sicurezza. Perciò, la frequenza di guasto λ viene divisa in

- λ_S - il guasto di sicurezza e
- λ_D - l'avaria, composta da
 - λ_{DD} - avaria rilevata dalla diagnostica interna
 - λ_{DU} - avaria non rilevata.

La frequenza di guasto può essere calcolata mediante il tempo medio tra guasti (MTBF), un valore specifico del modulo, come segue:

$$\lambda = 1/\text{MTBF}$$

L'equazione per calcolare la probabilità di guasto su richiesta è:

$$\text{PFD}(t) = \lambda_{\text{DU}} \times t$$

t rappresenta il tempo tra 2 test di tenuta.

La probabilità di guasto/ora implica un intervallo di tempo di 1 ora. Quindi, l'equazione PFD si riduce a quella seguente:

$$\text{PFH} = \lambda_{\text{DU}}$$

Oggetti di sistema

Contenuto del capitolo

Bit di sistema M580 Safety	399
Parole di sistema M580 Safety	401

Introduzione

Questo capitolo descrive i bit e le parole di sistema del PAC M580 Safety.

NOTA: i simboli associati a ciascun oggetto bit o parola di sistema menzionati nelle tabelle descrittive di questi oggetti non sono implementati come standard nel software, ma possono essere immessi con l'ausilio dell'editor di dati.

Bit di sistema M580 Safety

Bit di sistema per esecuzione task SAFE

I seguenti bit di sistema si applicano al PAC M580 Safety. Per una descrizione dei bit di sistema validi per PAC M580 Safety e PAC M580 non di sicurezza, consultare la presentazione di *Bit di sistema in EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento*.

Tali bit di sistema sono correlati all'esecuzione del task SAFE, ma non sono direttamente accessibili nel codice del programma di sicurezza. È possibile accedervi solo tramite i blocchi `S_SYST_READ_TASK_BIT_MX` e `S_SYST_RESET_TASK_BIT_MX`.

Bit Simbolo	Funzione	Descrizione	Stato iniziale	Tipo
%S17 CARRY	Uscita rotazione	Durante un'operazione di rotazione, questo bit assumerà lo stato del bit in uscita.	0	R/W
%S18 OVERFLOW	Errore aritmetico o di superamento del limite rilevato	Normalmente impostato a 0, questo bit viene impostato a 1 nel caso in cui si verifichi un superamento della capacità: <ul style="list-style-type: none"> Un risultato maggiore di + 32 767 o minore di - 32 768, in lunghezza singola. Un risultato maggiore di + 65 535, in intero senza segno. Un risultato maggiore di + 2 147 483 647 o minore di - 2 147 483 648, in lunghezza doppia Un risultato maggiore di +4 294 967 296, in lunghezza doppia o intero senza segno. Divisione per 0. Radice di un numero negativo. Forzatura a un passo inesistente su un tamburo. Riempimento di un registro già completo, svuotamento di un registro già vuoto. 	0	R/W
%S21 1RSTTASKRUN	Prima scansione task SAFE in RUN	Provato nel task SAFE, questo bit indica il primo ciclo di questo task. Viene impostato a 1 all'inizio del ciclo e azzerato alla fine. <p>NOTA:</p> <ul style="list-style-type: none"> Il primo ciclo dello stato del task può essere letto mediante l'uscita <code>SCOLD</code> del blocco funzione di sistema <code>S_SYST_STAT_MX</code>. Questo bit non è efficace per sistemi M580 Safety Hot Standby. 	0	R/W

Note relative ai bit di sistema specifici non di sicurezza

Bit di sistema	Descrizione	Note
%S0	avvio a freddo	Può essere utilizzato solo nei task di processo (non SAFE) e non influisce sul task SAFE.
%S9	uscite impostate su posizionamento di sicurezza	Non influisce sui moduli di uscita Safety.
%S10	Errore globale rilevato su I/O	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S11	overflow del watchdog	Prende in considerazione un overrun su task SAFE.
%S16	errore task rilevato su I/O	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S19	overrun del periodo di task	Informazioni per overrun task SAFE non disponibili.
%S40...47	errore rilevato su I/O rack <i>n</i>	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S78	STOP su errore rilevato	Si applica ai task di processo e al task SAFE. Se è impostato il bit, se ad esempio si verifica un errore di overflow %S18, il task SAFE entra in stato HALT.
%S94	salva i valori regolati	Non si applica alle variabili SAFE. I valori iniziali SAFE non sono modificabili dall'attivazione di questo bit.
%S117	Errore rilevato RIO sulla rete I/O Ethernet	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S119	generale nell'errore rack rilevato	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.

Parole di sistema M580 Safety

Parole di sistema per PAC M580 Safety

Le seguenti parole di sistema si applicano al PAC M580 Safety. Per una descrizione delle parole di sistema valide per PAC M580 di sicurezza e PAC M580 non di sicurezza, consultare la presentazione di *Parole di sistema in EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento*.

Questi valori e parole di sistema sono correlati al task SAFE. È possibile accedervi dal codice del programma applicativo nelle sezioni non di sicurezza (MAST, FAST, AUX0 o AUX1), ma non dal codice nella sezione del task SAFE.

Parola	Funzione	Tipo
%SW4	Periodo del task SAFE definito nella configurazione. Il periodo non è modificabile dall'operatore.	R
%SW12	Indica la modalità operativa del modulo Copro: <ul style="list-style-type: none"> 16#A501 = modalità di manutenzione 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	R
%SW13	Indica la modalità operativa della CPU: <ul style="list-style-type: none"> 16#501A = modalità di manutenzione 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	R
%SW42	Ora corrente task SAFE. Indica il tempo di esecuzione dell'ultimo ciclo del task SAFE (in ms).	R
%SW43	Durata max. task SAFE. Indica il tempo di esecuzione del task SAFE più lungo dall'ultimo avvio a freddo (in ms).	R
%SW44	Durata min. task SAFE. Indica il tempo di esecuzione del task SAFE più breve dall'ultimo avvio a freddo (in ms).	R
%SW110	Percentuale del carico della CPU di sistema utilizzato dal sistema per servizi interni.	R
%SW111	Percentuale del carico della CPU di sistema utilizzato dal task MAST.	R
%SW112	Percentuale del carico della CPU di sistema utilizzato dal task FAST.	R
%SW113	Percentuale del carico della CPU di sistema utilizzato dal task SAFE.	R
%SW114	Percentuale del carico della CPU di sistema utilizzato dal task AUX0.	R
%SW115	Percentuale del carico della CPU di sistema utilizzato dal task AUX1.	R
%SW116	Carico totale della CPU di sistema.	R

Parola	Funzione	Tipo
%SW124	<p>Contiene la causa dell'errore irreversibile rilevato quando il PAC M580 Safety è in stato Halt:</p> <ul style="list-style-type: none"> • 0x5AF2: errore rilevato RAM nel controllo memoria. • 0x5AFB: errore codice firmware di sicurezza rilevato. • 0x5AF6: errore di overrun watchdog di sicurezza rilevato sulla CPU. • 0x5AFF: errore di overrun watchdog di sicurezza rilevato sul coprocessore. • 0x5B01: coprocessore non rilevato all'avvio. • 0x5AC03: errore irreversibile CIP di sicurezza rilevato dalla CPU. • 0x5AC04: errore irreversibile CIP di sicurezza rilevato dal coprocessore. <p>NOTA: Quanto indicato sopra non costituisce un elenco completo. Per ulteriori informazioni, consultare <i>EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento</i>.</p>	R
%SW125	<p>Contiene la causa dell'errore reversibile rilevato nel PAC M580 Safety:</p> <ul style="list-style-type: none"> • 0x5AC0: la configurazione del CIP di sicurezza non è corretta (rilevata dalla CPU). • 0x5AC1: la configurazione del CIP di sicurezza non è corretta (rilevata dal coprocessore). • 0x5AF3: errore di confronto rilevato dalla CPU principale. • 0x5AFC: errore di confronto rilevato dal coprocessore. • 0x5AFD: errore interno rilevato dal coprocessore. • 0x5AFE: errore di sincronizzazione rilevato tra CPU e coprocessore. • 0x9690: errore checksum programma applicativo rilevato. <p>NOTA: Quanto indicato sopra non costituisce un elenco completo. Per ulteriori informazioni, consultare <i>EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento</i>.</p>	R
%SW126	<p>Queste due parole di sistema contengono informazioni per uso interno Schneider Electric per consentire di analizzare nei dettagli un errore rilevato.</p>	R
%SW127		
%SW128	<p>Con firmware della CPU 3.10 o precedenti, forzare la sincronizzazione dell'ora tra ora NTP e ora Safe negli stessi moduli IO di sicurezza e il task CPU Safe:</p> <ul style="list-style-type: none"> • Il cambiamento di valore da 16#1AE5 a 16#E51A forza la sincronizzazione. Consultare l'argomento <i>Procedura per sincronizzare le impostazioni dell'ora NTP</i>, pagina 179. • Altre sequenze e valori non forzano la sincronizzazione. 	R/W
%SW142	<p>Contiene la versione del firmware COPRO di sicurezza in 4 cifre BCD: ad esempio la versione firmware 21.42 corrisponde a %SW142 = 16#2142.</p>	R
%SW148	<p>Conteggio degli errori ECC (codice correzione errore) rilevati dalla CPU.</p>	R
%SW152	<p>Stato dell'ora della CPU NTP aggiornato dal modulo di comunicazione Ethernet (ad esempio BMENOC0301/11) sul backplane X Bus tramite funzionalità di sincronizzazione dell'ora forzata opzionale:</p> <ul style="list-style-type: none"> • 0: l'ora della CPU non è aggiornata dal modulo di comunicazione Ethernet. • 1: l'ora della CPU è aggiornata dal modulo di comunicazione Ethernet. 	R

Parola	Funzione	Tipo
%SW169	<p>ID applicazione di sicurezza: contiene un ID della parte codice di sicurezza dell'applicazione. L'ID viene modificato automaticamente quando si modifica il codice applicazione sicuro.</p> <p>NOTA:</p> <ul style="list-style-type: none"> Se il codice di sicurezza è stato modificato ed è stato eseguito un comando Crea modifiche dal precedente comando Ricrea tutto (cambiando perciò l'ID applicazione di sicurezza), l'esecuzione di un comando Ricrea tutto può di nuovo cambiare l'ID applicazione di sicurezza. L'identificativo univoco del programma SAFE può essere letto mediante l'uscita SAID del blocco funzione di sistema S_SYST_STAT_MX. 	R
%SW171	<p>Stato dei task FAST:</p> <ul style="list-style-type: none"> 0: Non esistono task FAST 1: Stop 2: Run 3: Breakpoint 4: Pausa 	R
%SW172	<p>Stato del task SAFE:</p> <ul style="list-style-type: none"> 0: nessun task SAFE 1: Stop 2: Run 3: Breakpoint 4: Pausa 	R
%SW173	<p>Stato del task MAST:</p> <ul style="list-style-type: none"> 0: nessun task MAST 1: Stop 2: Run 3: Breakpoint 4: Pausa 	R
%SW174	<p>Stato del task AUX0:</p> <ul style="list-style-type: none"> 0: nessun task AUX0 1: Stop 2: Run 3: Breakpoint 4: Pausa 	R
%SW175	<p>Stato del task AUX1:</p> <ul style="list-style-type: none"> 0: nessun task AUX1 1: Stop 2: Run 3: Breakpoint 4: Pausa 	R

Riferimenti SRAC

Il piano di verifica delle condizioni di applicazione relative alla sicurezza (SRAC) fornisce un quadro generico per giustificare il rispetto delle istruzioni del manuale di installazione e sicurezza associato. Queste istruzioni nella documentazione *Modicon M580, Manuale di sicurezza* sono elencate come requisiti.

La tabella seguente fornisce il titolo del paragrafo dove è possibile trovare il requisito relativo al ciclo di vita dell'applicazione:

Requisito del ciclo di vita dell'applicazione	
Id	In questa posizione
LC #1	Passaggio 9: Specifica dei requisiti di sicurezza del sistema E/E/PE, pagina 37
LC #2	Passaggio 9: Specifica dei requisiti di sicurezza del sistema E/E/PE, pagina 37
LC #3	Passaggio 10: Realizzazione dei sistemi di sicurezza E/E/PE, pagina 37
LC #4	Passaggio 12: Installazione e messa in servizio globali, pagina 41
LC #5	Passaggio 12: Installazione e messa in servizio globali, pagina 41
LC #6	Passaggio 13: Convalida sicurezza globale, pagina 42
LC #7	Passaggio 14: Funzionamento, manutenzione e riparazione globali, pagina 43
LC #8	Passaggio 15: Modifica e retrofit globale, pagina 43

La tabella seguente fornisce il titolo del paragrafo dove è possibile trovare i requisiti relativi al Messaggio informativo di sicurezza:

Requisito del messaggio informativo di sicurezza	
Id	In questa posizione
SM #1	Prima di iniziare, pagina 10
SM #2	Avviamento e verifica, pagina 11
SM #3	Loop di sicurezza, pagina 17
SM #4	Moduli non interferenti, pagina 29

Requisito del messaggio informativo di sicurezza	
Id	In questa posizione
SM #5	Alimentazione esterna utilizzata con gli I/O di sicurezza digitali, pagina 47
SM #6	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, Introduzione, pagina 54
SM #7	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, SIL3 Cat2/PLd, pagina 56
SM #8	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, SIL3 Cat2/PLd con alta disponibilità, pagina 57
SM #9	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, SIL3 Cat4/PLe, pagina 58
SM #10	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, SIL3 Cat4/PLe con alta disponibilità, pagina 59
SM #11	Connettore di cablaggio BMXSDI1602, alimentazione processo, pagina 67
SM #12	Connettore di cablaggio BMXSDI1602, fusibile, pagina 67
SM #13	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Introduzione, pagina 73
SM #14	Diagnostica cablaggio configurabile in Control Expert, pagina 74
SM #15	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 75
SM #16	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 75
SM #17	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 75
SM #18	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 77
SM #19	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 77
SM #20	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 77
SM #21	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 77
SM #22	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 77
SM #23	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81

Requisito del messaggio informativo di sicurezza	
Id	In questa posizione
SM #24	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #25	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #26	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #27	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #28	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #29	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #30	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 81
SM #31	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #32	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #33	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #34	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #35	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #36	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 88
SM #37	Connettore di cablaggio BMXSDO0802, fusibile, pagina 100
SM #38	Esempi di cablaggio dell'applicazione di uscita BMXSDO0802, Introduzione, pagina 102
SM #39	Esempi di cablaggio dell'applicazione di uscita BMXSDO0802, Introduzione, pagina 102
SM #40	Diagnostica cablaggio configurabile in Control Expert, pagina 103
SM #41	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106
SM #42	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106

Requisito del messaggio informativo di sicurezza	
Id	In questa posizione
SM #43	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106
SM #44	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106
SM #45	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106
SM #46	Riepilogo della diagnostica del cablaggio delle uscite, pagina 106
SM #47	Connettore di cablaggio BMXSRA0405, fusibile, pagina 114
SM #48	Applicazione_1: 4 uscite, SIL2 / Cat2 / PLc, stato non alimentato, nessun test automatico del segnale, pagina 117
SM #49	Applicazione_3: 4 uscite, SIL2 / Cat2 / PLc, stato non alimentato, nessun test automatico del segnale, pagina 118
SM #50	Applicazione_5: 2 uscite, SIL3 / Cat4 / PLc, stato non alimentato, nessun test automatico del segnale, pagina 119
SM #51	Applicazione_7: 2 uscite, SIL3 / Cat4 / PLc, stato alimentato, nessun test automatico del segnale, pagina 120
SM #52	Alimentatori M580 Safety, Introduzione, pagina 131
SM #53	Descrizione del tempo per moduli di uscita, pagina 157
SM #54	Configurazione dei periodi massimi dei task SAFE e FAST della CPU, pagina 161
SM #55	Funzioni e blocchi funzione di sicurezza certificati, pagina 166
SM #56	Configurazione della sincronizzazione dell'ora con firmware della CPU 3.10 o precedente, Introduzione, pagina 177
SM #57	Modifica dell'impostazione dell'ora NTP durante il funzionamento, pagina 178
SM #58	Procedura per sincronizzare le impostazioni dell'ora NTP, pagina 179
SM #59	Procedura per sincronizzare le impostazioni dell'ora NTP, pagina 179
SM #60	Configurazione del DFB S_WR_ETH_MX, pagina 191
SM #61	Configurazione del DFB S_RD_ETH_MX, pagina 193

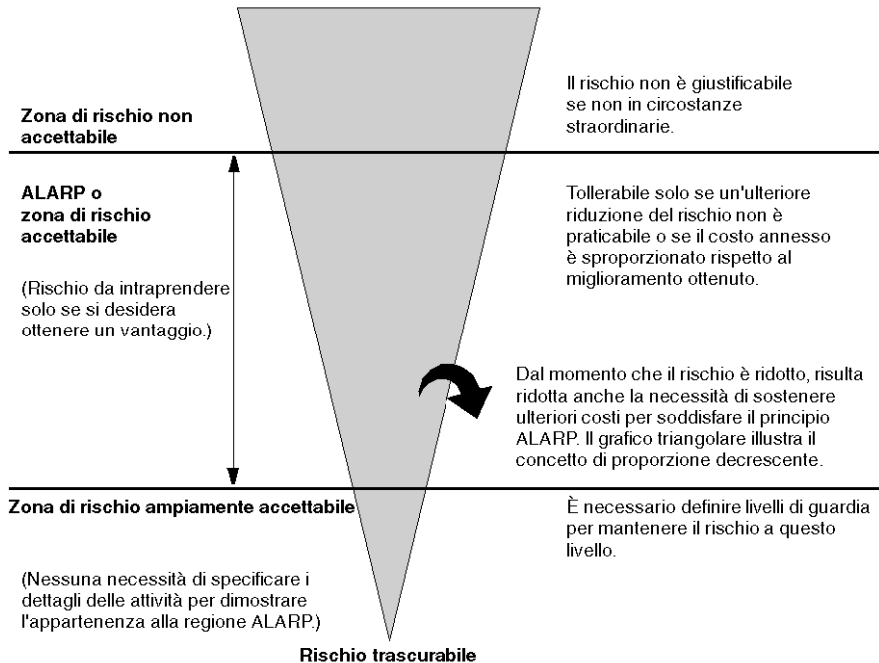
Requisito del messaggio informativo di sicurezza	
Id	In questa posizione
SM #62	Configurazione del DFB S_WR_ETH_MX2, pagina 204
SM #63	Configurazione del DFB S_RD_ETH_MX2, pagina 207
SM #64	Comunicazioni black channel M580, pagina 210
SM #65	Comunicazioni black channel M580, pagina 210
SM #66	Diagnostica LED CPU M580 Safety, pagina 221
SM #67	Funzionalità della modalità di manutenzione, pagina 258
SM #68	Sequenze di avvio, avvio a caldo, pagina 270
SM #69	Blocco della configurazione del modulo I/O di sicurezza, pagina 283
SM #70	Visualizzazione dei dati sulle schermate operatore, pagina 290
SM #71	Configurazione del dispositivo CIP Safety con l'utilizzo di uno strumento offerto dal fornitore, pagina 354
SM #72	Interazioni tra le operazioni del PAC di sicurezza e la connessione di destinazione, pagina 375

Glossario

A

ALARP:

(il più basso prevedibile) (Definizione di IEC 61508)



C

CCF:

(*Common cause failure, guasto da causa comune*) Guasto risultante da uno o più eventi che causano guasti concomitanti su due o più canali separati in un sistema a più canali, provocando un guasto del sistema. (Definizione di IEC 61508) La causa comune in un sistema a due canali è un fattore cruciale per la probabilità di guasto su domanda (PFD, probability of failure on demand) per l'intero sistema.

CPCRC:

(*controllo di ridondanza ciclica del parametro di connessione*) Un CRC-S32 dei parametri di connessione di destinazione prodotto dal CSS per ciascuna connessione CIP Safety e contenuto nella richiesta di apertura di sicurezza di tipo 2.

D**DDDT:**

(*Device derived data type, tipo dati derivati dispositivo*) Un DDT predefinito dal produttore e non modificabile dall'utente. Contiene gli elementi di linguaggio di I/O di un modulo di I/O.

Derivazione RIO:

Un rack di moduli I/O Ethernet, gestito da un adattatore RIO, con ingressi e uscite inclusi nella scansione RIO della CPU. Una derivazione può essere un rack singolo o un rack principale con un rack esteso.

DRS:

(*switch a doppio anello*) Uno switch a gestione estesa ConneXium configurato per il funzionamento su una rete Ethernet. I file di configurazione predefinita sono forniti da Schneider Electric per lo scaricamento su un DRS per supportare funzionalità speciali dell'architettura dell'anello principale / del sotto-anello.

DTM:

(*Device Type Manager*) Un DTM è un driver del dispositivo eseguito sul PC host. Fornisce una struttura unificata per l'accesso ai parametri, la configurazione e il funzionamento dei dispositivi e la diagnostica dei problemi. I DTM possono essere una semplice interfaccia utente grafica (Graphical User Interface, GUI) per l'impostazione dei parametri dei dispositivi su un'applicazione altamente sofisticata che supporta l'esecuzione di calcoli complessi in tempo reale a scopo di diagnostica e manutenzione. Nel contesto di un DTM, un dispositivo può essere un modulo di comunicazione o un sistema di rete remoto.

Vedere FDT.

E**EDS:**

(*Electronic Data Sheet*) Gli EDS sono semplici file di testo che descrivono le capacità di configurazione di un dispositivo. I file EDS sono elaborati e forniti dal costruttore del dispositivo.

EUC:

(Equipment under control, apparecchiatura sotto controllo) (Definizione IEC 61508) Questo termine indica apparecchiature, macchine, sistemi o impianti utilizzati per attività di produzione, elaborazione, trasporto, medicali o di altro tipo.

H**HFT:**

(Hardware Fault Tolerance, tolleranza degli errori hardware) (Definizione IEC 61508)

Una tolleranza degli errori hardware pari a N significa che N + 1 errori potrebbero provocare la perdita delle funzioni di sicurezza, ad esempio:

- HFT = 0: il primo errore può causare la perdita della funzione di sicurezza.
- HFT = 1: 2 errori combinati potrebbero causare la perdita della funzione di sicurezza. (Vi sono due percorsi possibili per passare a uno stato di sicurezza. Perdita della funzione di sicurezza significa che non è stato possibile passare a uno stato di sicurezza.)

O**OUNID:**

(identificativo di rete univoco dell'origine) Un valore che identifica in modo univoco il dispositivo da cui ha origine la connessione (tipicamente una CPU) su una rete CIP Safety. OUNID consiste in:

- un numero di rete di sicurezza (SNN), che può essere un Time stamp o un altro valore definito dall'utente.
- un indirizzo di nodo (per reti EtherNet/IP, l'indirizzo IP).

P**PST:**

(Process safety time, tempo di sicurezza processo) Il tempo di sicurezza del processo è il periodo di tempo che intercorre tra un errore verificatosi in un EUC o nel sistema di controllo dell'EUC (potenzialmente in grado di provocare un evento pericoloso) e il verificarsi dell'evento pericoloso qualora non venga eseguita la funzione di sicurezza. (Definizione IEC 61508)

R

Rete DIO:

Una rete contenente apparecchiature distribuite nella quale la scansione I/O viene eseguita da una CPUDIO con servizio di scansione sul rack locale. Il traffico di rete DIO è fornito dopo il traffico RIO, che ha la priorità in una rete di dispositivi.

S

SAId:

(identificativo dell'applicazione di sicurezza) Una firma calcolata con un algoritmo della parte sicura dell'applicazione Control Expert, archiviata in %SW169.

SCID:

(identificativo di configurazione di sicurezza) Vedere TUNID.

SFF:

(Safe Failure Fraction, frazione di guasti di sicurezza)

SNCT:

(strumento di configurazione di rete di sicurezza) Uno strumento offerto dal fornitore per la configurazione dei dispositivi CIP Safety. Vedere TUNID.

SRAC:

(Safety Related Application Condition, condizione dell'applicazione di sicurezza)

SRT:

(System reaction time, tempo di reazione del sistema) Il tempo di reazione del sistema è il periodo di tempo tra il rilevamento di un segnale al terminale del modulo di ingresso e la reazione di impostazione di un'uscita al terminale del modulo di uscita.

T

TFFR:

(tolerable functional failure rate, tasso guasti funzionali tollerabili) Un tasso orario secondo le norme EN 5012x per il settore ferroviario.

TUNID:

(identificativo di rete univoco della destinazione) Un valore che identifica in modo univoco il dispositivo di destinazione della connessione su una rete CIP Safety. TUNID consiste in:

- un numero di rete di sicurezza (SNN), che può essere un Time stamp o un altro valore definito dall'utente.
- un identificativo di configurazione di sicurezza (SCID), anche detto firma di configurazione, creato con uno strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e che consiste in:
 - un CRC di configurazione di sicurezza (SCCRC), che è un valore CRC delle impostazioni di configurazione del dispositivo di sicurezza, sotto forma di un valore esadecimale formato da 4 byte.
 - Un Time stamp di configurazione di sicurezza (SCTS), un valore time stamp esadecimale di data e ora formato da 6 byte.

Indice

61508	
IEC	391
61511	
IEC	391

A

A caldo, avvio	270
A freddo, avvio	270
Alimentatore	
diagnostica	229
diagnostica contatti relè di allarme	135
Alimentatore M580	
diagnostica mediante LED	229
Alimentazione	
diagnostica tensione backplane	134
alloggiamento	46
Altitudine	47
Ambito dei dati	171
Animazione, tabelle	287
applicazione	320
protezione	302
applicazione, ciclo di vita	35
Architettura	
BMEP58•040S CPU	139
BMXSAI0410	143
BMXSDI1602	144
BMXSDO0802	145
BMXSRA0405	146
coprocessore BMEP58CPROS3	139
Area dati	
di processo	172
globale	172
sicura	172
Aspettativa tempo di rete	163
Avvio	267
avvio a caldo	270
avvio a freddo	270
dopo interruzione alimentazione	268
iniziale	268

B

Black channel	210
---------------------	-----

Blocco configurazione I/O	283
BMEP58•040S	
architettura	139
BMEP58•040S CPU	
LED di diagnostica	221
BMEP58CPROS3	
architettura	139
BMEP58CPROS3 coprocessore	
Diagnostica LED	224
BMXSAI0410	50
applicazioni	54
architettura	143
connettore di cablaggio	52
DDDT	61
diagnostica DDDT	231
Diagnostica LED	232
BMXSDI1602	65
applicazioni	73
architettura	144
connettore di cablaggio	67
DDDT	94
diagnostica DDDT	235
Diagnostica LED	237
BMXSDO0802	98
applicazioni	102
architettura	145
connettore di cablaggio	100
DDDT	108
Diagnostica DDDT	241
BMXSRA0405	113
applicazioni	116
architettura	146
connettore di cablaggio	113
DDDT	125
Diagnostica DDDT	247
Diagnostica LED	248

C

cablaggio, connettore	
BMXSDI1602	67
BMXSDO0802	100
CCOTF	
limitazioni in un progetto di sicurezza	341
certificazioni	
PAC	21
Certificazioni	25

ciclo di vita	
applicazione	35
codici di errore	381
Comunicazione	
PAC-PAC	183
Condizioni bloccanti	216
Condizioni non bloccanti	219
Connettore di cablaggio	
BMXSAI0410	52
BMXSRA0405	113
Control Expert	
editor sicurezza	330
gestione accesso a	327
importazione di un progetto di	
sicurezza	340
profili utente predefiniti	330
ripristino di dati non sicuri	341
salvataggio di dati non sicuri	341
separazione dati	253
trasferimento di un progetto di	
sicurezza	340
uso della memoria	343
visualizzatore eventi	344
Control Expert Safety	
libreria di sicurezza	166
CPU	
comunicazioni con i moduli I/O di	
sicurezza	47
SNN	350
Crea, comando	
Crea modifiche	275
Ricrea tutto il progetto	275
Rinnova ID e Ricrea tutto	275
crittografia	
file	302
cybersicurezza	34

D

Dati, comando inizializzazione	
Init	286
Init Safety	286
dati, memorizzazione	
protezione	318
Dati, separazione in Control Expert	253
Dati, trasferimento tra spazi dei nomi	
procedura	175

DDDT	
BMXSAI0410	61
BMXSDI1602	94
BMXSDO0802	108
BMXSRA0405	125
diagnostica	
CIP Safety	378
LED BMXSAI0410	232
LED BMXSDI1602	237
LED BMXSRA0405	248
LED del coprocessore	
BMEP58CPROS3	224
Diagnostica	
alimentatore	229
BMXSAI0410 DDDT	231
BMXSDI1602 DDDT	235
BMXSDO0802 DDDT	241
BMXSRA0405 DDDT	247
condizioni bloccanti	216
condizioni non bloccanti	219
LED alimentatore di sicurezza M580	229
LED CPU BMEP58•040S	221
moduli di I/O di sicurezza	48
relè di allarme alimentatore	135
scheda di memoria	226
tensione backplane	134
dimenticare	
password	320
dispositivo, stato connessione	386

F

file	
crittografia	302
Firma di origini SAFE	275
firma sicura	275
firmware	320
protezione	316
Frazione di guasti sicurezza (SFF)	394

G

Guasto, frequenza	396
-------------------------	-----

H		O	
HFT (Tolleranza di errore hardware)	394	Operativa, modalità	257
HMI	290	Operativi, stati	262
I		OUNID	350
intervallo test di tenuta (PTI)	153	P	
I/O, configurazione		PAC a PAC, comunicazione	
blocco	283	ricevitore DFB PAC	206
IEC 61508		PAC e I/O, comunicazione	213
sicurezza funzionale	391	PAC-PAC, comunicazione	183
IEC 61511		architettura	184, 196
sicurezza funzionale per l'industria di		configurazione	185, 197
processo	391	DFB OAC ricevente	193
Inizializzazione dati	286	DFB PAC mittente	191, 204
L		trasmissione dati	190, 203
Livello di integrità di sicurezza (SIL)	393	password	
Loop di sicurezza	17	dimenticare	320
M		perdita	320
M580 Safety I/O	213	Password	
Manutenzione, ingresso	261	sezione	310
Manutenzione, modalità operativa	258	perdita	
memorizzazione dati	320	password	320
Mettere TUNID	377	PFD (Probabilità di guasto su richiesta)	394
moduli		PFD (probability of failure on demand,	
certificato	27	probabilità di guasto su richiesta)	147, 150
non interferenti	29	PFH (Probabilità di guasto all'ora)	394
tipo 1 non interferente	30	PFH (probability of failure per hour,	
tipo 2 non interferente	32	probabilità di guasto all'ora)	147, 150
Moduli di I/O di sicurezza		probabilità di guasto all'ora (PFH,	
diagnostica comune	48	probability of failure per hour)	147, 150
funzioni comuni	46	Probabilità di guasto all'ora (PFH)	394
MTBF (tempo medio tra guasti)	396	probabilità di guasto su richiesta (PFD,	
N		probability of failure on demand)	147, 150
network time protocol (NTP)	177	Probabilità di guasto su richiesta (PFD)	394
NTP (Network Time Protocol)	177	Programma, unità	
		protezione	314
		Proprietà RESET	377
		protezione	
		applicazione	302
		firmware	316
		memorizzazione dati	318
		Protezione	
		sezione	314
		Unità programma	314
		PTI (intervallo test di tenuta)	153

R

richiesta di apertura di sicurezza	
struttura frame	369
rilevamento dispositivi	386
RIO	46, 213

S

Safety, bit di sistema	399
Safety, I/O	46
SCCRC	354
Scheda di memoria	
diagnostica	226
SCID	354, 361
SCTS	354
Separazione dei dati	171
Sezione	
protezione	314
SFF (Frazione di guasti sicurezza)	394
Sicura, area	
password	310
Sicurezza, editor	327
Sicurezza, funzione	16
sicurezza, libreria	
Control Expert Safety	166
Sicurezza, loop	395
Sicurezza, modalità operativa	257
sicurezza, moduli I/O	
comunicazioni con la CPU	47
Sicurezza, parole di sistema	401
SIL (Livello di integrità di sicurezza)	393
Sistema	
bit	399
parole	401
SNCT	354
SNN	
dispositivo	360
Spazio dei nomi	
di processo	171
sicuro	171
trasferimento dati	174
Standard	25

T

task	292
------------	-----

Task	271
configurazione	272
Task SAFE	
configurazione	292
Tempo di sicurezza del processo	154
Tempo medio tra guasti (MTBF)	396
Tolleranza di errore hardware (HFT)	394
Trasferimento dati tra gli spazi dei nomi	174
Trending, strumento	291

U

Uso della memoria	343
-------------------------	-----

V

Visualizzatore eventi	344
-----------------------------	-----

Schneider Electric

35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

© 2021 **Schneider Electric**. Tutti i diritti sono riservati.

QGH46985.05