Modicon M580 Controller

Firmware History

Release Notes

Original instructions

02/2024

RN0000000110.02

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚡ The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

Document Scope

This document presents a history of Modicon M580 controller firmware releases, including a description of improvements made to each firmware release.

The firmware update procedure can be found in the *Modicon M580 - Update Procedure, User Guide*.

NOTE: Schneider Electric firmware is continuously reviewed and updated to maintain a high level of quality of our products.

Ensure your installation is up to date with the newest firmware versions, to help protect your infrastructure against cybersecurity threats and to experience improved quality performance.

For further information please visit the Schneider Electric Cybersecurity Support Portal: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Validity Note

This document is valid for Modicon M580 firmware versions up to and including version 4.20.

For product compliance and environmental information (RoHS, REACH, PEP, EOLI, etc.), go to www.se.com/ww/en/work/support/green-premium/.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

M580 Firmware Versions

M580 V04.20

Limitations

EADM is a common utility tool used for updating firmware in many Schneider Electric Industrial Automation products and can be downloaded here: https://www.se.com/ca/en/download/document/EADM/

Inoperable Equipment

- Do not upgrade with firmware version 4.01 or later any of the following Modicon M580 commercial references with a product version (PV) 3 or earlier: BMEP581020(H), BMEP582020(H), BMEP582040(H), BMEP583020, BMEP583040, BMEP584020, BMEP584040.
- If you intend to upgrade the M580 controller with a firmware version 4.01 or later, and you are using a Modicon M580 RTU module in association, first upgrade the RTU module to firmware version 03.02.02 or later and test your application.
- If you intend to upgrade the M580 controller with a firmware version 4.01 or later, and you are using a Modicon BMENOC0301 or BMENOC0311 module in association, first upgrade the BMENOC module to firmware version 02.20 or later and test your application.
- If you intend to upgrade the M580 controller with a firmware version equal to or greater than 4.01, and you are using a Modicon BMENOC0321 module in association, first upgrade the BMENOC module to firmware version 1.09 or later and test your application.

NOTE: Product version (PV) can be found on the product label. Current software version (firmware version) running on the product can only be found in connected mode with: *EcoStruxure Automation Device Maintenance* (EADM) or *EcoStruxure Control Expert*.

NOTE:

- A controller updated with software version (firmware version) 4.01 or later can be downgraded to earlier firmware versions using a specific downgrade tool. Contact your local Schneider Electric service representative.
- Updating from firmware version 3.20 or earlier to firmware version 4.01 or later must be done following a two-steps specific procedure. For instructions, refer to the M580 Firmware Installation Guide.
- Unity Loader cannot be used when using firmware version 4.01 or later. Instead, use of the EADM tool version 3 or later is necessary.
- Controllers with firmware version 4.01 and later can execute applications generated by earlier EcoStruxure Control Expert versions using earlier application versions. No modification or rebuild is needed.

Firmware Version 04.20 Improvements

Firmware Version	Publication Date	Internal Reference	Description
04.20	11/2023	N.A.	Improvement of Cybersecurity: New Secure Engineering link modes. Support of HTTPS communication between M580 controller and Control Expert.
		N.A.	Improvement of SYSLOG events recovery: The SYSLOG events are stored in the M580 non-volatile memory, they can be recovered and downloaded from the M580 webpage using an HTTPS connection.
		PEP0588260R PEP0588280R PEP1056784R	The following security vulnerability has been addressed in this release • CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel
		PEP0649547R	Bug fix of BMEP584040 I/O Scanner control bit (DIO_CTRL) that had been working incorrectly by resetting the bit repeatedly between 0 and 1 without effect.
		PEP1035211R	The following security vulnerability has been addressed in this release • CVE-2023-6408
		PEP1042827R	New Cybersecurity M580 V04.20 feature enabling external access to SYSLOG from web pages.
		PEP1052186R	The following security vulnerabilities have been addressed in this release • CVE-2018-7855
		PEP1056782R	The following security vulnerability has been addressed in this release • CVE-2022-45789
		PEP1058570R	Bug fix of Control Expert V15.2 & M580 Hot Standby v3.20, which were non-operational on application download.
		PEP1060888R	The following third-party components have been updated to address cybersecurity vulnerabilities. OpenSSL: • CVE-2023-0286 • CVE-2022-4304 • CVE-2023-0215 • CVE-2022-4450
		PEP1069770R	Bug fix of M580 V04.10 unable to connect via TFTP to EF OPCUA client

NOTE:

- EcoStruxure Control Expert V16.0 is required to use the new features of M580 controller Firmware version 4.20 (i.e., select M580 controller V04.20 as the application level).
- Firmware version 4.20 is compatible only with the Modicon M580 Standard offers (Standalone and Hot Standby controllers). The Modicon M580 Safety offer is not supported by this release.

V04.20 M580 Controller Firmware New Features

V04.20 new feature include:

- Secure Communication Drivers
- Engineering Link Modes
- Security Editor Whitelist, page 12
- Security Editor Password, page 12
- SYSLOG Events Recovery, page 12

Secure Communication Drivers

HTTPS and **HTTPS via USB** are new drivers that support secure engineering links.

> **NOTE:** For clarity, two pre-existing drivers have been renamed:
>
> - TCPIP is now *Modbus TCP*
> - USB is now *Modbus TCP via USB*

Engineering Link Modes

Depending on the level of targeted cybersecurity, you can select one of the following three **Engineering Link Modes**:

- **Full Access**:

  The controller behaves as in previous firmware versions. Secure and non-secure communications are accepted.

  - For Control Expert communication, the controller accepts the non-secure drivers **Modbus TCP** and **Modbus TCP via USB** or secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) is accepted.

- **Filtered** (default):

  A hybrid mode you can use to apply cybersecurity on the engineering link, and non-secure connectivity on links to SCADA or other controllers.

  - For Control Expert communication, the controller accepts the secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) or **UMAS** (OFS) are accepted.

    NOTE: In **Filtered** mode, the controller accepts the unsecure drivers **Modbus TCP** and **Modbus TCP via USB** but only with **Connection mode** set to **monitoring** in the options of the project. Monitoring mode is a read only mode, where it is not possible to download an application to the controller or stop the controller.

- **Enforced**:

  This mode provides the highest level of security. Only secure protocols are accepted by the controller:

  - For Control Expert communication, the controller accepts only the secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) or **UMAS** (OFS) are **NOT** accepted.

Security Editor Whitelist

A **Certificate Whitelist** is introduced to the **Security Editor** and includes the following features:

- **Add**: Use this command to configure the IP address of the M580 controller on which you want to create a secure engineering link.
- **Get Certificate**: Use this command to retrieve HTTPS certificate from the device.
- A dialog where you can trust the certificate and add it to Windows certificate store.
- **View Certificate**: Use this command to display and verify the certificate.
- **Remove**: Use this command to remove a certificate from the whitelist.

Security Editor Password

A password expiration date can be configured in **Security Editor**.

The SecurityAdmin user now must configure a password at installation if security is enabled.

SYSLOG Events Recovery

SYSLOG events are stored in the M580 controller in non-volatile memory. They can be recovered and downloaded from the M580 web page using an HTTPS connection.

M580 V04.10

Firmware Version 04.10 Improvements

Firmware Version	Publication Date	Internal Reference	Description
04.10	02/2023	PEP0537170R	Improve M580 SD card diagnostic in %SW97 for application mismatch
		PEP0664538R	Improve M580 SD card diagnostic in %SW97 for missing SD card
		PEP1014002R	Fix M580 Forced bit counter decrement in %SW102 and %SW108 when over limit of 1024
		PEP0650241R	Add system time catchup bit status %SW73.4 in Time Stamping feature
		PEP1030630R	Improvement of robustness for some Modbus commands
		PEP1030267R VMT-7905	Improvement of cyber security protection (CVE-2022-45788)
		PEP1031147R	Restriction of “Initialize %MWi on cold start” option to not reset %SW138 and %SW141
		PEP1044835R	Fix a regression since 4.02 affecting reconfiguration of submodules with FDR and FTP
		PEP0541853R	Improvement of M580 diagnostics in DiagFiles
		PEP1051545R / PEP1051547R VMT–9330 / VMT–9331	Improvement of cyber security linked to UMAS protocol
		NA	M580 controller start-up time with firmware version 4.10 and later is increased by 50% compared to firmware version 3.20.

NOTE:

- Firmware version 4.10 replaces version 4.02, which is no longer available. EcoStruxure Automation Device Maintenance (EADM) version V3.1.147 or later is required to perform the firmware upgrade operation.
- EcoStruxure Control Expert V15.3 is required to use the new features introduced with the M580 controller Firmware version 4.10 (select M580 controller V4.10 as application level).
- Firmware version 4.10 is compatible only with the Modicon M580 Standard offer (Standalone and Hot Standby). The Modicon M580 Safety offer is not supported.

M580 V04.02

Firmware Version 04.02 Improvements

Firmware Version	Publication Date	Internal Reference	Description
04.02	09/2022	PEP1036111R	Fix a regression since 4.01. When using Modbus FC 15 to write multiple coils to M580 controller the result of the operation is not predictable.
		N.A.	Fix a regression since 4.01. It is not possible to update firmware of X-bus only in-Rack modules through the controller backplane: • X-bus modules with Ethernet front port access are not impacted. • For BMXNOM0200 module firmware update, M580 rack power supply must be reset manually after the operation.

NOTE:

- Firmware version 4.02 replaces version 4.01, which is no longer available. Use version 4.02 or later in place of version 4.01.
- EcoStruxure Control Expert V15.2 is required to use the new features introduced with M580 controller firmware version 4.01 (select M580 controller V4.00 as application level).
- Firmware version 4.02 is compatible only with the Modicon M580 Standard offer (Standalone and Hot Standby). The Modicon M580 Safety offer is not supported.

M580 V04.01

Firmware Version 04.01 Improvements

Firmware Version	Publication Date	Internal Reference	Description
04.01	07/2022	N.A.	Improvement of cybersecurity protection: secure firmware update with EcoStruxure Automation Device Maintenance
		N.A.	Improvement of cybersecurity protection: HTTPS for Data Storage, webpage access and firmware update (Self-Signed certificates)
		N.A	Implementation of a new feature: SNMPv 3 (NoAuthNoPriv only)
		N.A.	Implementation of a new feature: NTPv4 client/server and NTPv4 server only for better time precision and resiliency
		N.A.	Implementation of a new feature OPC UA Client as Elementary Function Blocks (EF) compliant to PLCopen Standard
		N.A.	Improvement of event log: update SYSLOG version RFC 3164 to RFC 5424
		N.A.	Implementation of a new feature: support BMENUA0100(H) Firmware version 2.01 for customized unique role name

Firmware Version	Publication Date	Internal Reference	Description
		N.A.	Implementation of a new feature: new Controller Device DDT type “T_BMEP58_ ECPU_EXT2” including NTPv4 diagnostics
		N.A.	Removed Controller Device DDT type “T_BMEP58_ECPUPRP_EXT” (only for application version >4.00)
		N.A.	Removed HTTP protocol
		N.A.	Removed FTP protocol for Data Storage and firmware upload
		N.A.	Removed: SNTP (only for application version >4.00)
		PEP0677514R VMT-4976	Improvement of cyber security protection. M580_CE v15 SP1 Denial of Service
		PEP0676721R VMT-4978	Improvement of cyber security protection. M580 Denial of Service
04.01	**07/2022**	PEP0670929R	Improvement of cyber security protection. M580 BadAlloc Multiple RTOS vulnerabilities Refer to CVE-2020-35198 - CVE-2020-28895 for more details
		PEP0660997R VMT-4659	Improvement of cyber security protection. M580_Integer Underflow Denial of Service
		PEP0636127R VMT-3285	Improvement of cyber security protection. M580 Denial of Service Refer to CVE-2021-22779 for more details
		PEP0635317R PEP0604347R VMT-2983	Improvement of cyber security protection. M580 information disclosure Refer to CVE-2021-22786 for more details
		PEP1005826R VMT-5538	Improvement of cyber security protection M580 XSS vulnerabilities contained in JQuery Refer to CVE-2020-11022 and CVE-2020-11023 for more details
		PEP0591421R	Improvement: new SYSLOG event, Hot Standby system states (Primary/ Standby/Wait)
		PEP0667293R	Fix: M580 controller receiving zone disorder for multiple READ_VAR calling
		N.A.	Increases robustness of controller: new diagnostic mechanism (history traceability) with essential system word information for better support purpose from Schneider Electric
		PEP0647567R	Fix: Cold start (instead of warm start) on power up issue with BMEP5820X0 PV15 FW3.20
		PEP0667554R	Fix: M580 Hot Standby losing CRA Drops on swap from Prim->Stby when performing online change on an application using more than 70 EDS files.
		PEP0669774R	Fix: a M580 DIO_CTRL bit not working as expected for the Modbus TCP IO Scanner
		N.A.	Fix: After a Power ON, the standby has MS and NS LED steady red
		PEP1013234R	Fix: %SW49 freezes and was not updated as expected.
04.01	07/2022	N.A.	Fix: String_to_real conversion when ‘generate with LD link animation’ option unchecked
		PEP1009430R	Fix regression from 2.90 to 3.20 in BMEP582040 - IO SCANNING, missing devices in the IO scanner
		N.A.	Fix: Write Only IO Scanning function between 2 NOCs giving bad status in DDT SCANNER_OK variable and DIO_Health[x] variable
		N.A.	Fix regression from 3.10 to 3.20 in BMEH6040, BMENUA0100 is abnormally disconnected after each swap by application.
		N.A.	Fix: Drop loss after drop power cycle
		PEP1025228R	Fix: M580 - crashes in 0xEC10 due to EtherNet/IP stack

NOTE:

- Firmware version 4.01 replaces version 3.30, which is no longer available for non-safety-related controllers. Use version 4.01 or later in place of version 3.30.
- EcoStruxure Control Expert V15.3 is required to use the new features introduced with M580 controller firmware version 4.01 (select M580 controller V4.00 as application level).
- Firmware version 4.01 is compatible only with the Modicon M580 Standard offer (Standalone and Hot Standby). The Modicon M580 Safety offer is not supported.

M580 V03.30

Firmware Version 03.30 Improvements

Firmware Version	Publication Date	Internal Reference	Description
03.30	12/2021	N.A.	Improvement: support of the Modicon M580 Safety commercial reference BMEP586040S

NOTE: Firmware version 3.30 is only available for safety processor BMEP586040S.

M580 V03.22

Firmware Version 03.22 Improvements

Firmware Version	Publication Date	Internal Reference	Description
03.22	05/2022	N.A.	Manufacturing tests support for new hardware PV25.
		PEP0647567R	Fix unexpected "Cold start" at power up issue for BMEP582020 and BMEP582040.

NOTE:

- Firmware version 3.22 is not available in se.com.
- In Modicon M580 Hot-Standby systems, level of Firmware version in both controller “A” and “B” must be equal. Controller PV 25 with Firmware version 3.22 can be downgraded to earlier software versions (Firmware version).

M580 V03.20

Firmware Version 03.20 Improvements

Firmware Version	Publication Date	Internal Reference	Description
03.20	11/2020	PEP0531707R	Implementation of a new feature: data memory protect settings in the variable editors
		PEP0546432R VMT-1385	Improvement of cyber security protection. Refer to CVE-2019-6848 for more details

Firmware Version	Publication Date	Internal Reference	Description
		PEP0546433R VMT-1386	Improvement of cyber security protection. Refer to CVE-2019-6849 for more details
		PEP0575205R	Improvement of cyber security Increases robustness of controller on access to the webserver
		PEP0536845R	Fix a SNMP answer data regression since 2.80
		PEP0574971R VMT-1950	Resolved a remote Denial Of Service while using a specific Python script; controller went into an stop managed exception. refer to CVE-2020-7543 for more details
		PEP0573933R	Increases robustness of controller communication EF on big number of simultaneous connections.
		N.A.	CFB: error when reading a TOD variable (Error when retrieving local variable type despite variable well declared)
		N.A.	Increases robustness of controller for SFC section on warmstart
		PEP0569506R / VMT-1705	Corrected a stop managed exception vulnerability of the controller caused by a specific UMAS command. Refer to CVE-2020-7537 for further details.
		N.A.	Increases robustness of Hot Standby system, in case of very long task period (to prevent de-synchronization)
		N.A.	Improvement of the reliability of the controller workload diagnostic value
		PEP0558372R	Increases robustness of controller against memory leak issue, on some types of LLDP frames occurrence.
03.20	11/2020	PEP0556173R	Increases robustness of controller against removal of a device accessible through a gateway.
		PEP0591264R	Removed wrong diagviewer message "HSBY: Degraded hsby data transfer"
		PEP0539539R	Implementation of the "monotonic time" black channel for safety systems.
		PEP0593227R	Remove the 6 extension racks unexpected limitation.
		PEP0558717R	Correction to align the SYSLOG events messages text with online documentation.
		N.A.	Enhancement of the performance when in parallel branches in SFC language.
		N.A.	Fix a bad display of the links in FBD section on the program viewer using the webserver.
		PEP0572529R	Improvement of cyber security protection on webserver
		N.A.	Implement new version of safety coprocessor.
		N.A.	Restored the error reporting service of the send_email function block.
		PEP0547752R	Fix a Hot Standby device_ddt EIO_ERROR status that was toggling.
		PEP0582003R	Implementation of the capability to recover from a long catchup state without stopping the process
		PEP0547404R	Implementation of the safety monotonic time principle
		N.A.	Implementation of a new feature: SFC “final scan”
		PEP0611715R	Improvement of cyber security memory read protection
03.20	11/2020	PEP0537170R	Improvement of controller device DDT about SD Card diagnostics
		N.A.	Increases robustness of heavy safety systems (managed exception after few hours running)
		PEP0563955R	Enhancement of the reliability of the Hot Standby device_DDT "SYNC" diagnostic for BMEH586040 controllers.
		PEP0595913R	Fix a NOC disconnection (IP lost) on app transfer following several online modifications
		PEP0531779R	Fix variable initialization issue after init on SFC

M580 V03.10

Firmware Version 03.10 Improvements

Firmware Version	Publication Date	Internal Reference	Description
03.10	11/2019	N.A.	Improvement: support of the CIP Safety protocol for the standalone Safety controllers BMEP582040S and BMEP584040S
		PEP0536229R PEP0536224R PEP0549596R PEP0535816R	Improvement of cyber security protection: Denial of service on invalid inputs on firmware upgrade
		PEP0545693R	Improvement of cyber security protection: Denial of service: Operating System reinforcement
		N.A.	Improvement: optimization of the max start-up delay between wait and run-primary state on Hot Standby controller when no peer controller is connected
		N.A.	Improvement: safety controller NTP time update via BMENOC0301.4 or BMENOC0311.4
		PEP0546973R	Improvement of cyber security protection: Denial of Service on invalid inputs

M580 V02.90

Firmware Version 02.90 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.90	07/2019	PEP0532740R PEP0533497R PEP0448402R PEP0518846R PEP0518847R PEP0518848R PEP0515689R PEP0527486R	Improvement of cyber security protection: Denial of service on invalid inputs
		PEP0532557R	Fixes a byte swap issue following Modbus I/O scanning modification. When the I/O scanner of the controller writes data to any devices, swap of byte might appear in specific conditions. This issue was present on legacy versions.
		PEP0533499R	Improvement of cyber security protection: Unauthenticated write data request
		PEP0435529R PEP0454883R	Enhancement: The controller informs the NOR that it's in summer time. %S58.
		PEP0454883R	Adjust the behavior of the controller in case of data checksum error (reboot instead of exception stop).
		PEP0504969R	Harmonizes the behavior of the variables initialization on all controller ranges.
		PEP0535827R	Increases robustness of controller when loading an application level V1.10 in controller with V2.8
02.90	07/2019	N.A.	Improvement of the robustness on swap on Safety Hot Standby controller.
		PEP0527907R	Improves the behavior of I/O scanner lines control bits when the M580 scans a Schneider M221 controller.
		PEP0448852R	Improves the readability of the RIO diagnostics

Firmware Version	Publication Date	Internal Reference	Description
		PEP0448852R	Improves the robustness of the Standby Safety controller following CCOTF and application transfer from Primary to Standby.
		PEP0530147R	The wrong cabling on the coax side of the 140CRA31908 was not detected. The fix of this issue requires a 140CRA firmware V2.40 and the OS V2.90
		N.A.	New feature to prevent downgrade firmware. Firmware version<2.90 in the controllers with PV referenced below.
		PEP0515685R	Improvement of cyber security protection: Denial of service on invalid application transfer
		PEP0530708R N.A.	Improves the robustness following modification online. (when replacing wire between 2 FBs by variable)
		PEP0534509R	Improvement of cyber security protection: Denial of service on HTTP request
		N.A.	Improves the firmware upgrade robustness with Unity Loader
		PEP0532226R	Fixes M580 - %SW87 - the Number of Queries not matching between client and server
		PEP0450104R	Improvement of cyber security protection: Buffer overflow in FTP service
		PEP0426709R	Fixes that backup LED is reported incorrectly in web page.
		PEP0505171R PEP0505170R	Improvement of cyber security protection: Unauthenticated modification of application
		PEP0505165R	Improvement of cyber security protection: Denial of Service on controller reservation
02.90	07/2019	PEP0515694R	Improvement of cyber security protection: Unauthenticated application transfer
		N.A.	Improves robustness during big amount of project downloads
		N.A.	Enriches the event log (SYSLOG protocol) when the firmware of the controller has been upgraded

NOTE: To be able to select the M580 V2.90 controller and its features in Control Expert V14.0 applications, installation of the following hot fix for Control Expert V14.0 is required: “ControlExpert_V140_HF_PMEPXM0100_HF0312169E”

NOTE:

- The following table lists the controller PV references that cannot be downgraded to Firmware versions earlier than V2.90 (due to new hardware). Unity Loader will not perform such a downgrade.
- Controllers with PV later than the ones referenced below need to be upgraded to Firmware version 2.90 or later.
- Like any new firmware, a program generated by versions earlier than V14 of Unity Pro / Control Expert will be accepted.

Commercial Reference	Short Description	New Product Version	New Software Version
BMEH582040	M580 HSBY CPU LEVEL 2 FOR R IO	11	2.90
BMEH582040C	C M580 HSBY CPU LEVEL 2 FOR R IO	10	2.90
BMEH582040K	M580 LEVEL 2 HSBY CPU KIT	10	2.90
BMEH584040	M580 HSBY CPU LEVEL 4 FOR R IO	11	2.90
BMEH584040C	C M580 HSBY CPU LEVEL 4 FOR R IO	10	2.90
BMEH584040K	M580 LEVEL 4 HSBY CPU KIT	10	2.90
BMEH586040	M580 HSBY CPU LEVEL 6 FOR R IO	11	2.90
BMEH586040C	C M580 HSBY CPU LEVEL 6 FOR R IO	10	2.90
BMEP581020	M580 processor level 1 for D IO	14	2.90
BMEP581020H	M580 hardened processor level 1 for D IO	14	2.90
BMEP582020	M580 processor level 2 for D IO	14	2.90
BMEP582020H	M580 hardened processor level 2 for D IO	14	2.90
BMEP582040	M580 processor level 2 for D & R IO	14	2.90
BMEP582040H	M580 hardened processor level 2 for D & R IO	14	2.90
BMEP583020	M580 processor level 3 for D IO	14	2.90
BMEP583040	M580 processor level 3 for D & R IO	15	2.90
BMEP584020	M580 processor level 4 for D IO	15	2.90
BMEP584040	M580 processor level 4for D & R IO	14	2.90
BMEP585040	M580 processor level 5 for R IO	9	2.90
BMEP585040C	C M580 processor level 5 for R IO	8	2.90
BMEP586040	M580 processor level 6 for R IO	8	2.90
BMEP586040C	C M580 processor level 6 for R IO	8	2.90

M580 V02.80

Firmware Version 02.80 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.80	02/2019	PEP0477261R	LED ERR blinks in storm condition
		PEP0448055R	Controller Device DDT Network Health bit now returns to 1 when issue of Storm/Network disappears
		PEP0481942R	BME*58*0*0 controllers do not lose anymore I/O scanning tick
		PEP0437710R	BME*58*0*0 controllers - enable CIP requests when sender / receiver is a controller
		PEP0472830R PEP0475431R PEP0441086R	Improvement of cyber security protection.

Firmware Version	Publication Date	Internal Reference	Description
		PEP0433539R PEP0456402R	
		PEP0478160R	Prevent a controller firmware to be loaded in a BMXNOR module (destructive)
		PEP0423915R	New feature: force eRIO drops outputs to fallback state (like %S9 for local I/0s)
		PEP0423150R	Diagnostic Viewer improvement
		PEP0495030R	Improvement of the safe communication avoiding I/O fallbacks
		N.A.	Improvement of the safe communication avoiding I/O fallbacks on %SW128 usage
		N.A.	Avoid having a possible Safe task Halt (%SW125=5AF3) following an Init safe
		N.A.	Improvement of the startup sequence if the Hot Standby link is not healthy (damaged, broken or unplugged…): if controller B is controlling the I/Os (Primary), then at startup, controller A might take the Primary role with a NULL context instead of starting in Standby mode.
		PEP0496873R	Improvement of the startup sequence with "auto start in run" and reset from the power supply, to avoid a possible 3 red LEDs managed exception.
		PEP0500049R	Correction of a network redundancy diagnostic issue (in the controller DDDT) when the controller is connected to an STB DIO loop.

NOTE: For Firmware version 2.80 and later, the Unity Pro offer is re-named EcoStruxure Control Expert.

M580 V02.70

Firmware Version 02.70 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.70	07/2018	PE-P0300614R	New feature: manage time stamped events on user defined trigger (external sources such as power breaker…)
		PE-P0337045R	Addition of 2 diagnostic messages in the primary diagnostic viewer concerning counterpart controller: “becomes standby” & “no more standby”
		PE-P0411281R	Improve SD Card driver robustness
		PE-P0439440R	Enhance cybersecurity features regarding Run/Stop input and reservation mechanism management
		PE-P0440866R	Enhance cybersecurity features regarding buffer overflow in TFTP service
		PE-P0441146R	Enhance cybersecurity coding rules on instruction “STRNCPY”
		PE-P0441227R	Enhance cybersecurity coding rules for Software Development Lifecycle
		PE-P0447659R	Enhance cybersecurity regarding controller memory robustness
		PE-P0329819R	Enhance “READ_VAR” robustness against multiple fast disconnection / reconnections of Ethernet cable on NOC module
		PE-P0434129R	Improve NTP service to fix the “RTC = 2085+” issue
		PE-P0471161R	When using NTP service, the controller now displays correct information in the % SW53
		PE-P0434129R	When using NTP service, the controller now always keeps RTC updated on power cycle
		PE-P0432934R	Enhance robustness regarding FTP access to SD card (could lead to HALT)

Firmware Version	Publication Date	Internal Reference	Description
		PE-P0439586R	Enhance robustness regarding Modbus server on reception of partial request
		PE-P0439147R	Enhance memory robustness when Magelis HMI configured by Vijeo Designer writes to unlocated variable
		PE-P0428446R	Correct IP address assignment to a BMEAHI0812 after a controller power cycle if one or both of the ETH ports on the controller are disabled
		PE-P0461343R PE-P0460854R	Correct FDR synchronization on Hot Standby controller switchover: could lead to Hot Standby synchronization status to “OFF”, PMESWT0100 not restarting after controller switchover

M580 V02.60

Firmware Version 02.60 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.60	05/2018	N.A.	Improvement: support of the reference BMEP582040S

NOTE:

- Firmware version 2.60 is only available for safety processors BMEP584040S.
- Downgrading the BMEP584040S can only be executed by Schneider Electric support services.

NOTICE

INOPERABLE EQUIPMENT

Do not downgrade a BMEP584040S to the Firmware version 2.40.

Failure to follow these instructions can result in equipment damage.

M580 V02.50

Firmware Version 02.50 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.50	04/2018	PEP0314683R	Correction of a problem related to frozen variables that might happened after a SFC initialization in seldom cases
		PEP0428256R	Internal Modbus server robustness enhancement against malformed Frame
		PEP0412883R	ECC activation (Error Correcting Code) – see notes
		PEP0422526R	Fix of i/o scan that didn't work due to an RST_ACQ
		PEP0431488R	Internal HTTP server robustness enhancement against malformed Frame
		PEP0419392R	Restore SYSLOG function that was not available anymore since v2.30
		PEP0434189R	Increase of backup application speed
		N.A.	Update processor settings based on the latest manufacturer recommendations

Firmware Version	Publication Date	Internal Reference	Description
		N.A.	Enrich the diagnostic file information to ease and make more efficient problem resolution by R&D
		N.A.	Fixes seldom "3 red LEDs" behavior on rack reset (CPS button)

NOTE: An Error Correcting Code mechanism improves the robustness of the controller against memory bit flips (soft errors) during its lifetime. This feature allows the controller to reach a level of robustness that exceeds the quality standard and might also impact the cycle time of the controller. It is recommended to check that the application cycle time after upgrade conforms with application requirements.

NOTICE

INOPERABLE EQUIPMENT

Do not power off the controller when upgrading the controller to 2.50 or later from an earlier version (or vice versa).

Failure to follow these instructions can result in equipment damage.

M580 V02.41

Firmware Version 02.41 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.41	10/2017	N.A.	Improvement: support of the CCOTF (Configuration Changes On The Fly) function in S908 drops behind a 140CRA31908. The minimum requirements for this function are: • Unity Pro v12.0 Hot Fix or Unity Pro v13.1 or later (Unity Pro v13 does not support CCOTF on S908) • 140CRA31908 FW version 2.30 or later • 140CRP93xxx FW version 2.10 or later • 140CRA93xxx FW version 2.03 or later • BMEx584040 or BMEP585040 or BMEx586040 FW version 2.41 or later
		PE-P0358607R	Improve robustness on power cycle when tasks cycle periods are close to 1ms
		PE-P0423246R	Improve the robustness of cancelling a communication function block when used in a FAST task. Reminder: it is not recommended to use communication function block in FAST tasks.
		PE-P0341973R	Improve robustness of the system when 2 breakpoints are used consecutively within the same ST section
		PE-P0418125R	Evolution of "device DDT" mode behavior, so that the I/O power supply validity is evaluated before the logic (like in "topological" mode).
		PE-P0391470R	Fixes the incorrect information displayed in the webpage concerning the DHCP feature: even if enabled, the webpage was displaying it disabled.
		PE-P0314563R	Prevent the system to go to HALT when large number of communication function blocks are used (80 or more per cycle) and when the execution cycle duration is close to the configured period.
		PE-P0358247R	Optimize the performances when %SW90 is used to expand the default number of communication requests possible per cycle
		PE-P0427510R	Avoid a rare situation where the controller might go to the NO CONF state upon power cycle in case of very large application (memory close to be full)
		PE-P0428228R	Robustness improvement of the communication system in case of heavy loads

NOTE: Firmware version 2.41 is available only for processors level 40 and later. The impact of performances introduced in v2.30 has been resolved and is back to normal.

M580 V02.30

Firmware Version 02.30 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.30	04/2017	PEP0348778-R	Improve the robustness of the redundant system to avoid a very seldom case where the RIO bumped on 1 cycle after a controller switchover triggered by a complete loss of visibility the RIO network by the primary (both the 2 controller ETH ports disconnected)
		PEP0348925-R	Prevent any RIO drop disconnection in rare cases of a misformed DHCP telegram
		PEP0333697-R	Change the behavior of the NTP management in order to avoid the system time to shift one hour less when BMXNOR0200H is set as NTP client.
		PEP0337384-R	Improve robustness on proprietary FC90 Modbus server in controller
		PEP0339111-R	Implement a new algorithm against TCP sequence number vulnerability giving now unpredictable random TCP sequence numbers
		PEP0348361-R	Change the behavior of the SCHEDULE function block to be aligned with the user documentation: Sunday was assign to bit 7 in WEEK instead of 0
		PEP0350099-R	Improve SYSLOG system where some events described in user manual were not recorded (Application and configuration upload / download)
		PEP0358247-R	Improve robustness of the internal communication system to avoid it being overloaded by too many requests that resulted into diminished communication performances
		PEP0387751-R	Improve robustness of the system against very seldom cases where specific DTM files loaded into the controller lead to a controlled stop unexpectedly.
		UNI-TY00081595	Increase robustness of the system when sending communication FC90 requests via WRITE_CMD_MX that could lead to a controlled stop unexpectedly
		UNI-TY00083596	Increase the robustness of the web server (rack viewer part) to avoid, in very seldom case, to trigger a controlled stop of the controller unexpectedly
		UNI-TY00084328	Increase the robustness of the redundant system related to Ethernet IP scanner & adapter services that might stop after intensive controller swaps
		UNI-TY00084413	Fix a seldom behavior in the firmware download processing that could lead to the following error message “Flash upgrade error: S_False”
		UNI-TY00084448	Fix a very seldom case of system-controlled stop (managed exception state EC10) when downloading a new firmware in the controller
		UNI-TY00084826	Fix a seldom issue that lead to a unexpected state in the module re-configuration after a hot swap due to high frequency of explicit communication EF activation (READ_VAR, WRITE_VAR…) – typically less than 50ms.

NOTE: Firmware version 2.30 is available only for processors level 40 and later. It may impact performances under specific operating conditions (up to +30% of scan time measured) due to enhancements concerning operating system cybersecurity.

After updating the processor version from an existing application, check if this impact appears and study the potential consequences in the system.

M580 V02.20

Firmware Version 02.20 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.20	09/2016	N.A.	Fix a communication server issue when many communication EFs are started at the same time, could lead to error code 7.
		N.A.	Fix a communication EF operating mode issue in redundant configuration: Controller waits now until its IP address is correctly set after a controller swap (Hot Standby) before executing communication EF. Wrong IP address could previously be used by Modbus EF during first Mast cycle after a swap that leads to communication errors.
		N.A.	Improvement: Enhance diagnostic for redundant system: %SW61.5 support to get access by program to the information of controller A and controller B
		N.A.	Fix a real time issue on Ethernet IP system when processing arpResolv request: task could be interrupted during up to 600ms, that could lead to a bump on CRA.
		N.A.	Fix a seldom issue that lead to a controller stop (error code EC04) after around 20 000 swaps on redundant system. (robustness of tDiagMgrPoll system task).
		N.A.	Fix a seldom issue that lead to a controller stop (error code EC04) after application swaps on redundant system. (robustness of tLLDP system task).
		N.A.	Improvement: Enhance diagnostic in case of unexpected system stop thank to a new file /usr/diag/crash.txt generated. It includes the complete VxWorks call stack of the faulty task.
		N.A.	Fix an issue on software upload when password activated.
		PE-P0342179R	Fix a robustness issue that could lead to a controlled stop of the controller after receiving PTP Ethernet packets.
		PE-P0343987R	Fix an issue on %S94 operating mode that caused the BMENOC falling in "No Conf" state.
		PE-P0328060R	Improvement: Enhance application upload operating mode to block the upload when controller is not reserved to increase the security.
		UNI-T-Y00079914	Fix an issue on SET_FILE_ATTRIBUTES EF that didn't change the file attributes successfully on M580.
		UNI-T-Y00080213	Fix a diagnostic issue on RIO DDT heartbeat (trigger too sensible)
		UNI-T-Y00081354	Fix an issue on the redundant M580 controller to make the redundant link more robust to avoid seldom cases of controller B in "Wait" state after several power cuts
		UNI-T-Y00082078	Fix an issue regarding auto-negotiation feature of the wired Hot Standby high speed link.
		UNI-T-Y00082487	Fix an issue that leads to system stop (error code EC10) of redundant M580 controller when performing operating modes on both %S94 and %S66
		UNI-T-Y00082337	Fix an issue that leads to a controller stop (root cause was a watchdog overflow on EtherNet/IP) when disconnecting the Ethernet link connected with many scanned devices
		UNI-T-Y00082350	Fix an issue that leads to a controller stop (root cause was a watchdog overflow on EIP - %SW124=0x001F) when controller alternative power cycles
		N.A.	Fix an issue on the SFP after restarting the system that could lead to have a Hot Standby Link Down.
		N.A.	Improvement of robustness on hardware watchdog by changing internal system timeout values of MAC2.

M580 V02.13

Firmware Version 02.13 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.13	09/2016	PEP0333578R	Fix the issue introduced with v2.12 where the controller does not boot after power cycle

M580 V02.12

Firmware Version 02.12 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.12	04/2016	PEP0314608R	Improvement: change the management of closing TCP connection (to be aligned as M340)
		N.A.	Improvement: miscellaneous robustness improvements
		N.A.	Improvement: support BMENOC IO Scanning upgrade (from 1.8KW to 3.7 KW)
		N.A.	Improvement: support of the Redundant Power Supplies (BMXCPS4002) advanced diagnostic function blocks
		N.A.	Improvement: support of the Global Data Module (NGD)
		PEP0309455R	Fix the 10 years offset issue if time reference for NTP is coming from BMXNOR0200
		PEP0286728R	Fix the wrong display in millisecond of value coming from R_NTPC() function.
		PEP0286728R	Fix the arithmetic error wrongly generated when using FFB R_N NTPC function block
		PEP0328302R	Fix the offset issue when M580 answering to Modbus FC02 and FC04 requests from SCADA (same mapping than Quantum now)
		PRB 192406	(Hot Standby only): Fix the wrong behavior of remote IO frozen if remaining Hot Standby controller goes into HALT state
		PEP0322001R	Fix the wrong behavior of the %S9 not working properly at first controller cycle

NOTE: Firmware version 2.12 is no longer available. Use version 2.13 or later in its place.

M580 V02.10

Firmware Version 02.10 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.10	01/2016	PEP0299575R	Fixed an alignment issue in IO Scanner when a sequence of specific manipulations is done related to adding / modifying and removing line upon several build
		PEP0287801R	Fixed potential loss of signature of an SD Card upon power cycle
		PEP0311101R	Improvement: animation enabled on function REF_TO_ANYBOOL when mapped on extracted bit
		UNITY00079055	Improvement of data_exch CIP address input parameter in order to avoid having to write it in the DFB at each cycle.

Firmware Version	Publication Date	Internal Reference	Description
		UNITY00078119 UNITY00078306 UNITY00076741 UNITY00076742	Improvement of cybersecurity robustness against: • Periodic configuration change at each cycle using ETH_PORT_CTRL block (ex: enable / disable FTP) • FTP session still active when FTP is disabled using ETH_PORT_CTRL block • Controller SYSLOG events recording improvement in case of FW update or controller reboot
		UNITY00078670	Fixed EIP communication issues between M580 and M340 BMXNOC0401 in Ethernet / IP (it was OK for Modbus TCP)
		N.A.	Improvement: support of State RAM for BMEP584040
		N.A.	Improvement: support of Quantum Ethernet drops (140CRA31200) for BMEP584040
		N.A.	Improvement: support of some Quantum function blocks for BMEP584040
		N.A.	Improvement: support of Rack Viewer for BMEP584040
		N.A.	Improvement: All controllers: support of Redundant Power Supplies BXCPS4002 (status and function blocks)

NOTE: Firmware version 2.10 does not support, and cannot be use on, M580 Hot Standby controllers (BME H 58xxxx).

M580 V02.01

Firmware Version 02.01 Improvements

Firmware Version	Publication Date	Internal Reference	Description
02.01	07/2015	N.A.	Scanner controller DDDT evolution to simplify user interface (new health bit and control bit per device...)
		N.A.	Numbering schema change: Device ID, Connection ID, Object ID, Compatibility to simplify user interface
		N.A.	ANYBOOL support for online animation
		N.A.	Time stamping support for local variables of the controller
		N.A.	Enhance cybersecurity features: Enable/Disable unused services, support EtherNet/IP, DHCP, BOOTP services, Hardening Access Control (ACL), Disable FTP on Ethernet when in NOCONF mode, Event Logging
		N.A.	Device Integration: support of ‘R’ Ready devices
		N.A.	Support of CCOTF on Local IO
		PEP0293564R	Fix a potential issue where an undesirable output was one during the first controller cycle after start-up
		PEP0291328R	When the controller is HALTed, the DIO outputs keep the last values -> the fix is to stop the IO scanner to activate the fallback values
		PEP0281260R	No Ethernet IP connection (with drive Danfoss FC102)
		PEP0250301R	Enhance DIO management for class 1 CIP connections (controller DIO connection internal time-outs)
		PEP0275023R	FTP password for firmware upload must be configurable
		PEP0280264R	DEVICE_CNX_CTRL bits management is not correct on M580 controller Device DDT for STB
		PEP0250299R	M580 data Freshness bits management do not behave as described in the documentation
		PEP0275021R	Enhance FTP robustness against too long login names
		PEP0275017R	Increase the reliability of the firmware integrity self-test

Firmware Version	Publication Date	Internal Reference	Description
		PEP0261831R	Regression vs M340: implement NOR0200 NTP Client feature to update the controller RTC
		PEP0267189R	Enhance existing password protection mechanism to reserve controller

M580 V01.13

Firmware Version 01.13 Improvements

Firmware Version	Publication Date	Internal Reference	Description
01.13		N.A.	Unity Loader being connected to a BMXEHCxxx via a controller, the controller may go in "NO CONF" state OR Module LEDs blinking (RUN, ERR, I/O, DL) OR "system stop" state (%SW124=EC00) during the upgrade of the EHC.
		N.A.	The webpage fails after a long period of time with the popup message: "communication timeout occurred, please check the connection"
		N.A.	During CNM Network discovery (Auto Topology using SNMP features) the controller seems not being connected to the correct port
		N.A.	In M580 controller web page, the module name is followed by "Pr"
		PEP0267431R	Controller goes in "system stop" state when an unexpected CIP frame targets the controller (this issue only occurs on BMEP58x020 controller versions)
		PEP0266012R	When connected indirectly to the controller (e.g., through a NOC), the communication to the controller fails while performing heavy actions (like storing actual values in init values)
		PEP0250302R	The Control bits of the DIO scanner stops working after a while
		PEP0250296R	Controller may go in "system stop" state after an Online Modification with High communication traffic
		PEP0273207R	Cybersecurity: impossible to disable the ports 2 and 3 of the controller whereas the option is checked in Unity Pro (only concerns BMEP58x020 controller versions)
		N.A.	Improves Ethernet backplane communication management for large configurations.

M580 V01.04

Firmware Version 01.04 Improvements

Firmware Version	Publication Date	Internal Reference	Description
01.04	12/2014	N.A.	Launch version

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.