Life Is On | Schneider Electric

# A bypass by any name is risky. Time for a rethink?

by Steve J Elliott
Schneider Electric Senior Director – Marketing

## Executive summary

Bypasses by any name are risky. The need to bypass hasn't changed, but the means to execute more efficiently and safely has grown by leaps and bounds. As have the international standards for safety and cybersecurity. In this paper we will explore how putting a renewed focus on operators doesn't mean we have to do things the same old way, and how new bypass methods bring opportunities to create new value.

## Introduction

Since the inception of the modern concept of safety instrumented systems there has always been the need to bypass for many reasons, such as during start up, during process transitions, for maintenance, testing, repair, or replacement of faulty instruments.

Bypasses are also referred to as inhibits, suppressions, forcing, impairments, or bridging, but regardless of the name, the process of enacting a bypass is risky. Why?

When Safety Instrumented Functions (SIF) are bypassed there is an increased risk to operating facilities associated with the loss of the specific safety function. The extent of the increased risk is dependent on the consequence of the hazard involved (e.g. rupture, explosion, toxic exposure) and the other protective layers that have been designed into the facility. Bypasses intentionally designed into an Emergency Shutdown System (ESD) must be strictly controlled to minimize the risk to people, production, the environment, and profits.

But the act of bypassing isn't new. Traditional bypassing methods vary, for example:

- Hardwired-initiated bypass:
  - Dedicated switches are connected to the inputs of the safety system to deactivate sensors and actuators, and then handled as part of the application program.
  - Sensors and actuators are electrically isolated (disconnected) from the PLC (e.g. using clamps) and checked manually by special measures.
- Software-initiated bypass:
  - Maintenance overrides initiated by serial communication to the safety system via an operator interface such as BPCS, DCS, SIS engineering tools or an independent HMI.

## Why are we talking about bypasses? And why now?

Bypasses have been around for decades, so why are we talking about this now?

A lot has changed in the last 24 months. The COVID pandemic amplified the already existing strain of safety expertise that was no longer available where or when needed. The old way of working was no longer fit for purpose, so things had to change, and quickly. This lifted the pace of change and investments in digital software solutions.

Then there was the "expertise drain" as companies reacted to the economic downturn and resized their workforce, causing an "expertise attrition". The experienced workforce with the legacy history and knowledge were no longer available. This "changing of the guard" brings a new workforce generation with an expectation of working with modern, easy to use tools that allow them to work differently, they ask "why would you use cumbersome hardwired switches when you can use modern software tools?"

**Figure 1**

*The aerospace industry has moved from lamps and switches to modern HMI interfaces*


No conversation would be complete without mentioning cybersecurity. In May of this year, Colonial Pipeline1 confirmed it paid $4.4M ransom to a hacker gang after a cyberattack, as the CEO authorized payment to restart the pipeline's systems quickly and safely. The industrial industry is facing unprecedented cybersecurity levels of complexity and quantity, so it is vital that whatever systems you rely on for bypasses, you don't leave them vulnerable.

This in turn brings a tightening attitude to corporate risk management. Many organizations are looking at the Total Cost of Risk (TCOR) and spreading their risk exposure by carrying third-party insurance.

However, the insurers are now more informed on what they are insuring (and their risk liability), so they are looking much harder at the safety systems and risk reduction measures in place to limit their own risk exposure.

All of this brings a renewed focus on bypass operation and performance.

## Operators are critical to safe and profitable operation

The control room is the heart of any manufacturing operation, and the role of a process operator is critical to both safe and profitable operation.

When a bypass is applied two things happen: (1) the risk reduction factors in place decrease, (2) the operational risk increases. During these elevated risk conditions, operators need maximum situational awareness of critical process conditions, so anything that can be done to help operators is a good thing.

This is reflected in the safety standards. For example, IEC61511-1 Edition 2 Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, section 16.2 provides guidance around bypasses:

**16.2.2** Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:
c) the measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional risk reduction needs to be implemented);

**16.2.3** Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

**16.2.4** Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

**16.2.6** Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure that they understand:

- the correct operation and management of all bypass/override switches and under what circumstances these bypasses are to be used;

## We have always done it this way, so what's the problem? Why change?

"We don't see the need to change. We can justify how things are." Sound familiar?

We know that change can be complex, challenging, time consuming, costly (emotionally as well as financially), and even a little scary. The general preference is to leave well alone, so it's all too easy to stand behind the adage "We have always done it this way." But this mindset is the enemy of safety improvements and curtails progress or gains.

However, that doesn't mean that traditional ways don't come with their own challenges, such as:

Hardwired-initiated bypasses:

**Dedicated Key Switches:**

- Require I/O and wiring
- Engineering, documentation, and testing required
- More space, weight, power, HVAC
- Difficult to expand / modify
- Higher installed cost
- Confusion of bypassing the wrong tag
- Anybody can change a switch
- Lack of auditability

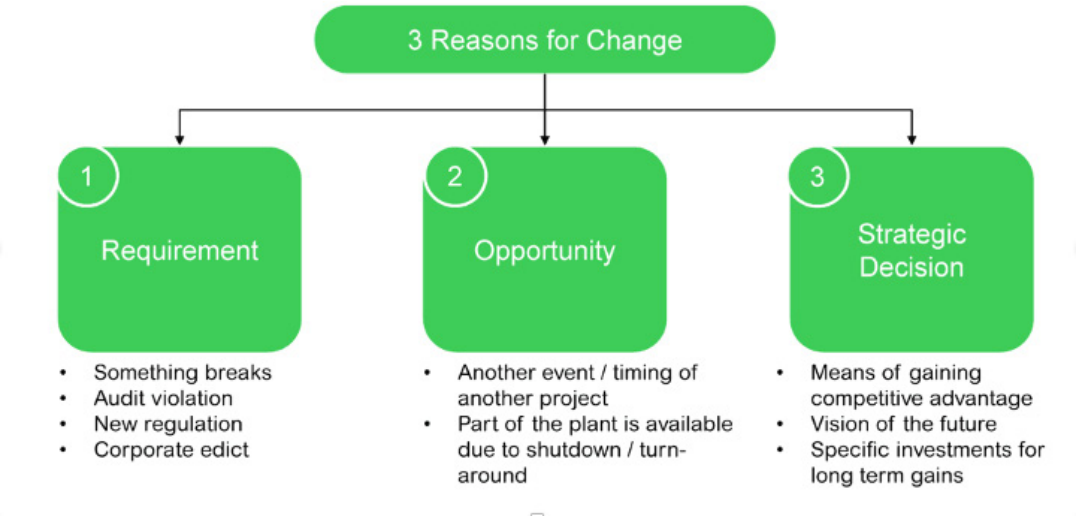
| Software-Initiated bypasses*: | |
|---|---|
|  | **BPCS / DCS:**<br>• Not certified for use in safety applications<br>• Critical alarms can easily get lost in a myriad of screens<br>• DCS is writing to the safety system so both the DCS and the SIS need to be configured for integrity checking<br>• Failure of the DCS results in the operators being "blind" to both process conditions and bypasses in place.<br>• Costly to implement<br>• Difficult to standardize and support |
|  | **SIS Engineering Tools:**<br>• Prone to error<br>• Need specialist safety system knowledge, access and privileges<br>• May need to understand the application logic<br>• Disallowed by industry safety standards<br>• May need to change safety system settings<br>• Not very friendly during shift hand over<br>• No traceability or audit trail of who / when bypasses applied / removed |
|  | **Independent HMI:**<br>• Often bespoke, every implementation is different, custom applications<br>• Difficult to maintain / update / keep cybersecure<br>• Difficult to standardize or scale up / deploy across multiple units / plants<br>• Both the HMI and the SIS need to be configured for integrity checking<br>• Redundancy often engineered in<br>• Require scripting / additional logic<br>• Not certified for use in safety applications<br>• Add up to higher implementation and total lifecycle costs |

**Important Note*: If you decide to go down the software bypass route, then it is mandated by industry standards that (1) the software used incorporates measurements to control random failures when the program is created or changed (2) incorporates measurements to control random data communication failures to the PLC (3) should ensure there are no common cause failures.

So why upset the status quo? After all, "if it aint broke, don't fix it." The requirement to change is primarily driven by three factors:

**Figure 2**

*Primary reasons to drive change*




Whatever the reason to change, the outcome from change needs to achieve tangible business goals, such as:

- improving safety performance
- reducing unplanned downtime
- mitigating cybersecurity threats
- reducing operational risk exposure
- driving efficiency or productivity gains
- reducing insurance premiums
- reducing lifecycle costs, support costs, etc.
- complying with company directives
- mitigating attrition of expertise

## Evolution is a fact of life; everything changes, nothing stays the same forever.

Just think about how the satellite navigation in your car has transformed getting from point A to point B (the job hasn't changed, you still need to get from A to B), but how you do it has been revolutionized. No more printing out maps, using highlighter pens to color the route, writing a list of road numbers, junction numbers, getting lost and wondering where you are, etc. As the technology evolved, a level of intelligence has been added. Now you have more information available so you can make informed choices i.e. take the most fuel-efficient route / the fastest route / avoid motorways / be able to adapt and change the route in the event of a major hold up or road closure etc.

The need to perform bypass and critical / priority alarm management hasn't changed, but the means to execute more efficiently and safely has grown leaps and bounds from traditional approaches. "Way back when", technology was the limiting factor; you had to use hardwired key switches for bypasses because there was no other way, there simply wasn't the choice that there is now.

So not only **what** you use has changed, but also **how** you use it. The user interface is easier to use, more user friendly, interactive, intuitive. This means you can not only make the job easier, more efficient, more effective, but you can create new value and improve top line / bottom line performance. For example, using a certified software-initiated bypass system such as EcoStruxure™ Triconex™ Safety View you can:

- Streamline shift hand over by reactivating bypass indicators so the new operator knows what's in bypass and why, what risk he must manage, and eliminating the possibility of unknowingly leaving bypasses enabled.
- Prohibit a bypass from being removed if the process is in a potential trip condition, preventing the operator from inadvertently tripping the unit or plant.
- Have a clear audit trail of when bypasses were applied and by who.
- Optimize obligatory reporting on bypass quantity, duration, etc. for those important Key Performance Indicators (KPIs) or target-based performance.
- Identify potential improvement areas e.g. identify potential design problems, operational problems, maintenance problems.

## What do the safety standards say?

As bypasses impact the safeguards and levels of risk reduction and are considered as safety-related, they fall under the purview of the safety standards. For example, the international safety standard IEC61511-1 Edition 2 Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements states:

**Section 11.7.2. – Operator Interface Requirements**

**11.7.2.1** Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

*NOTE* This can include preparing plans to enable an orderly safe shutdown in the event of total failure of the operational displays.

**11.7.2.2** The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

*NOTE* If the operator has to select a particular option, there can be a confirmation step.

**11.7.2.3** Bypass switches or means shall be protected to prevent unauthorized use (e.g., by key locks or passwords in conjunction with effective management controls).

*NOTE* Consideration can be given to enforcing time limits on bypass operation and to limiting the number of bypasses that can be active at any one time.

**11.7.2.4** The SIS status information that is critical to maintaining the SIF shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;
- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

**11.7.2.5** The SIS operator interface design (see 11.7.2.7) shall be such as to prevent changes to the SIS application program.

**11.7.2.6** Where information is transferred from the BPCS to the SIS, systems, equipment or procedures shall be applied to confirm that the correct information has been transferred and that the safety integrity of the SIS is not compromised.

*NOTE* The systems, equipment or procedures used can include control over selective writing from the BPCS to specific SIS variables.

**11.7.2.7** The design of the SIS operator interface via the BPCS operator interface shall be such that provision of incorrect information or data from the BPCS to the SIS shall not compromise safety.

**11.7.3 Maintenance / engineering interface requirements:**

**11.7.3.3** The maintenance/engineering interface shall not be used as the operator interface.

**11.7.4 Communication interface requirements**

**11.7.4.1** The design of any SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to achieve or maintain a safe state of the process.

**11.7.4.2** When the SIS is able to communicate with the BPCS and peripherals, the communication interface, BPCS, or peripherals shall not adversely impact any of the SIFs within the SIS.

*Important Note*: If you are considering using any software-initiated tool or application, and you reference IEC61511 in your codes and standards, then you should:

1. Consider credible failures of the operator interface.
2. Include facilities for protection against operator error.
3. Provide clear indication that a protective function is impaired or bypassed.
4. Confirm that the correct information is transferred between the operator interface and the safety system.
5. Confirm that the safety integrity of the SIS is not compromised.

## TÜV Guidance

We strongly recommend to keep the tools for programming and debugging separate from the tools used for maintenance override.

The engineering workstation, which is used for programming, should not be used for maintenance.

6. Avoid using the maintenance / engineering tools.
7. Ensure that any failure of the communication interface does not affect the ability of the SIS to achieve or maintain a safe state of the process.
8. Not adversely impact any of the SIFs within the SIS.

## Why is safety-certified software important?

The need to have hardware platforms which perform safety-related functions be safety-certified is no longer debateable. If software tools directly or indirectly impact these same safety functions, then why would we not expect the same level of rigor?

The integrity of software used in safety-related applications is extremely important, as you need to know that it will **work when needed** and **won't introduce any adverse effects**. For example, when applying a software-initiated bypass, the software is writing to the Safety System and will directly impact a specific SIF (with a specific SIL1, 2 or 3 rating). So, you had better be sure that you don't get any nasty surprises.

One way to do this is to ensure the software application you use is TÜV-certified to **Systematic Capability SC3** according to IEC61508, for specific use in safety-related applications up to SIL 3.

The best way to think of systematic capability is as a confidence level and a measure of the integrity of the software being used i.e. procedures, methods, tools, testing, validation, documentation, etc. that proves its effectiveness. Per IEC61511-1 Edition 2, systematic capability is defined as:

**3.2.80 systematic capability**

Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual.

*Note 1 to entry*: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults in IEC 61508-2:2010 and IEC 61508-3:2010.

*Note 2 to entry*: The systematic failure mechanism depends on the nature of the device. For a device comprised solely of hardware, only hardware failure mechanisms are considered. For a device comprised of hardware and software, it is necessary to consider the interactions between hardware and software failure mechanisms.

*Note 3 to entry*: A systematic capability of SC N for a device means that the systematic safety integrity of SC N has been met when the device is applied in accordance with the instructions specified in the device safety manual for SC N.

Systematic Capability is achieved when the equipment used to implement any safety function is designed using procedures intended to prevent systematic design errors. The rigor of the procedures is a function of a Safety Integrity Level (SIL).

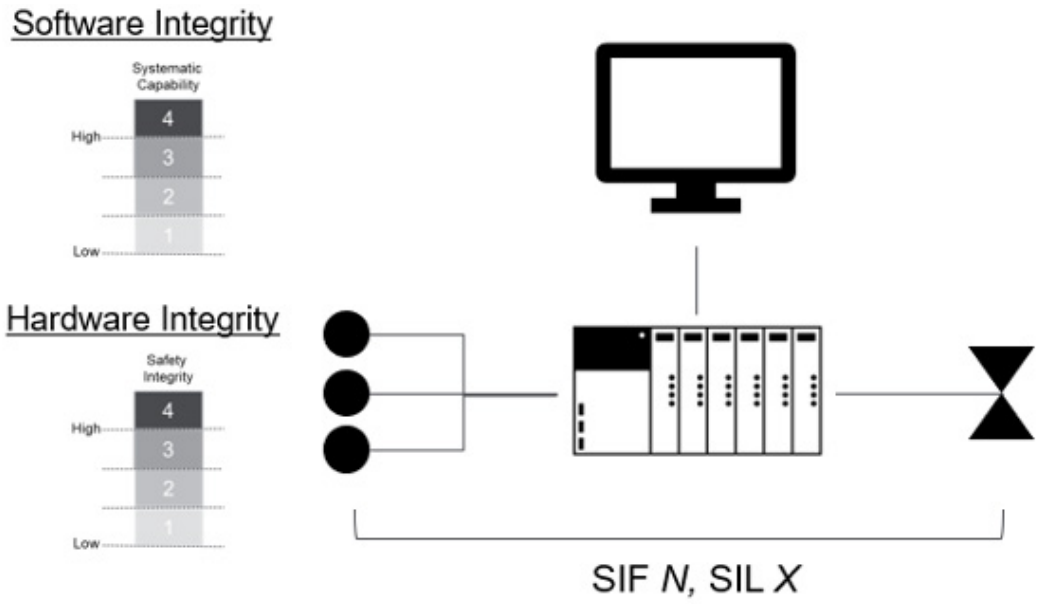
Simply put, the SC level should match the highest SIL level being impacted. For example, if you are impacting a SIL3 loop, the software you are using should be certified to SC3.

IEC61508-3, section 7.4.2.10 states:

Where the systematic capability of a software element is lower than the safety integrity level of the safety function which the software element supports, the element shall be used in combination with other elements such that the systematic capability of the combination equals the safety integrity level of the safety function.

**Figure 3**

*Systematic Capability / Safety Integrity relationship*




*Important Note*: don't confuse Systematic Capability (SC) with Safety Integrity Level (SIL).

**Table 1**

*Systematic Capability versus Safety Integrity Level comparison*

| Systematic Capability (SC): | Safety Integrity Level (SIL): |
|---|---|
| Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual.<br><br>Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults in IEC 61508-2:2010 and IEC 61508-3:2010. The systematic failure mechanism depends on the nature of the device. For a device comprised solely of hardware, only hardware failure mechanisms are considered. For a device comprised of hardware and software, it is necessary to consider the interactions between hardware and software failure mechanisms.<br>A systematic capability of SC N for a device means that the systematic safety integrity of SC N has been met. | Discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS.<br><br>The higher the SIL, the lower the expected PFDavg for demand mode or the lower the average frequency of a dangerous failure causing a hazardous event for continuous mode.<br>SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest. |

## If you are not cybersecure, you are not safe.

Regrettably, it is a fact of life that cyber-attacks are more frequent, more complex, and no system is immune from attack, so what-ever systems you rely on for bypasses, don't leave them vulnerable. If you choose to use software-initiated bypasses, make sure that the software is designed with cyber-security built in, and then implemented in accordance with the latest cybersecurity standards, such as IEC 62443.

IEC 62443 has been developed by both the ISA99 and IEC committees to improve the safety, availability, integrity, and confidentiality of components or systems used in industrial automation and control. The IEC 62443 series of standards can be utilized across industrial control segments and is approved by many countries. In the same way that there are Safety Integrity Levels, and Systematic Capability levels, for cybersecurity there are also Security Levels. Technical requirements for systems (IEC 62443-3-3) and products (IEC 62443-4-2) are evaluated in the standard by four Security Levels (SL) which indicate the resistance against different classes of attackers. The levels are:

- Security Level 0: No special requirement or protection required.
- Security Level 1: Protection against unintentional or accidental misuse.
- Security Level 2: Protection against intentional misuse by simple means with few resources, general skills, and low motivation.
- Security Level 3: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge, and moderate motivation.
- Security Level 4: Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge, and high motivation.

*Important Note*: at a minimum, you should select Security Level 1 (SL1) for software bypass applications, and have independent certification for example, TÜV.

## What should you consider when deciding the best way to implement bypasses?

Before you next think about how to implement bypasses, take a moment and ask the following:

- ☐ Are bypasses considered as safety-related?
- ☐ Do operators know what is in bypass? And more importantly, why?
- ☐ Have there been any near misses or unplanned outages due to improper bypassing?
- ☐ Does the existing bypass method meet current safety standards?
- ☐ Is the existing bypass method cybersecure?
- ☐ In your opinion, what makes the current bypass methods challenging?
  - General (complex, stressful, frustrating, inefficient, error prone)
  - Speed (Time consuming, slow, difficult to execute, inconvenient)
  - Stability (problematic, challenging, inconsistent)
  - Output (Ineffective, costly, wasteful, poor quality, less than ideal)
- ☐ If hardwired initiated bypasses are used, what would the impact be if you changed to software-initiated bypasses?

## There is now another choice for bypasses.

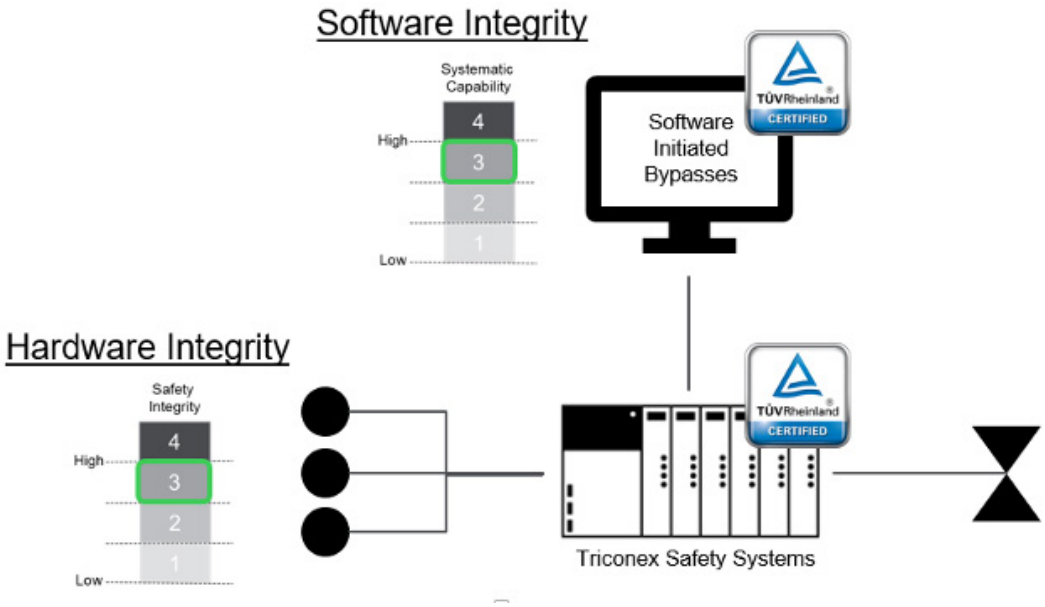
Good news – technology is no longer a limiting factor. There is now a new choice to consider for software-initiated bypasses: EcoStruxure™ Triconex™ Safety View.

This fit for purpose bypass and alarm management application:

- Meets the international safety standards
- Is TÜV certified to systematic capability level 3
- Is TÜV certified for use in safety-related applications up to SIL3
- Is cybersecurity certified to IEC62443
- Is designed specifically for bypasses
- Aligns with digital transformation programs or initiatives

**Figure 4**

*Hardware and Software Certified Integrity*




EcoStruxure™ Triconex™ Safety View is the first, and only, TÜV certified software application intended specifically for bypass and critical / priority alarm management. It can be used in any SIL3 rated SIF as part of the operator interface covering bypass, inhibits and reset alarm display, including first out indication, plus other safety-critical operator actions because:

- The TÜV approved function blocks running in the Triconex safety system provide approved and secure communication.
- The straight-forward configuration process immensely simplifies the management of change process.
- Simplified point-to-point read and write connection to the Triconex controller allows the DCS connection to be read-only for display and logging purposes as required.

# Conclusion

Bypasses by any name are risky. Never apply a bypass unless you fully understand why it's needed, the consequence, and what mitigating measures to put in place to manage the operational risk gap (i.e. perform an operational risk assessment before the bypass is applied).

The need to perform bypasses hasn't changed, but the means to execute more efficiently and safely has grown by leaps and bounds from decades-old approaches.

Be aware of the international safety standards IEC61508 and IEC61511, and cybersecurity standard IEC62443, as these provide specific guidance on bypass implementation and security measures.

The integrity of software used in safety-related applications is extremely important. You need to know that it will **work when needed** and **won't introduce any adverse effects**, so check the Systematic Capability level and certification levels when deciding.

Embrace change. New choices such as EcoStruxure™ Triconex™ Safety View are available with the potential to create new value.

# Appendix A: References

IEC6108: Edition 2.0 Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC61511: Edition 2.0 Functional safety – Safety instrumented systems for the process industry sector

IEC62443: Industrial communication networks – IT security for networks and systems

Colonial Pipeline cyber-attack ransom: https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom

EcoStruxure™
Innovation At Every Level

EcoStruxure™ is our open, interoperable, IoT-enabled system architecture and platform. EcoStruxure delivers enhanced value around safety, reliability, efficiency, sustainability, and connectivity for our customers. EcoStruxure leverages advancements in IoT, mobility, sensing, cloud, analytics, and cybersecurity to deliver Innovation at Every Level. This includes Connected Products, Edge Control, and Apps, Analytics & Services. EcoStruxure™ has been deployed in 480,000+ sites, with the support of 20,000+ system integrators and developers, connecting over 1.6 million assets under management through 40+ digital services.

Find out more about EcoStruxure **click here**.

## About the author

**Steve Elliott** is a Schneider Electric Senior Director of Process Automation Offer Marketing and is responsible for formulating future directions and go-to-market strategies. He is a certified functional safety engineer with more than 20 years of experience in the process control and automation industry. He has extensive experience designing safety systems and implementing the safety lifecycle.

## Contact us

For more information about the content of this white paper:

Visit the EcoStruxure Triconex Safety View web page:
https://www.se.com/uk/en/work/products/industrial-automation-control/triconex-safety-systems/software-applications/safety-view.jsp

If you are a customer and have questions specific to your bypass requirements:

Contact your Schneider Electric representative at
https://www.se.com/ww/en/locate/395-schneider-electric-offices-around-the-world

**Schneider Electric**
© 2021 Schneider Electric. All Rights Reserved.
998-21557359