Special edition

05/2020
ISSN 2567-3742

PROZESSWÄRME

The path to standard compliant and consistently safe automated thermoprocessing equipment

von **Ulf Weißhuhn, Hermann Wübbels**

Automatic burner control systems which are certified according EN 298 are the precondition to fulfil the requirements of the EN 746-2 for industrial thermoprocessing equipment. But what if several automatic burner control systems need to be coordinated by a central controller? If additional sensors, consistent fail-safe communication is required and the complete system needs to fulfil the safety requirements under the EU Machinery Directive. Is safe then really always safe?

In the European Union, product safety requirements are regulated by EU directives. The implementation of these EU directives is described in specific standards. These standards are categorized as (Type) A, B and C standards. Type A are basic safety standards, Type B are generic safety standards or group safety standards (e.g. EN 62061 or ISO 13849-1), and Type C are machine safety standards (e.g. EN 746-2 or ISO 13577)

For controller-based safety solutions, EN 62061 and EN ISO 13849-1 are harmonized under the EC Machinery Directive 2006/42/EC in the EU. This means that if the safety functions are designed according to the B standards specified above, (CE) compliance with the EU directives can be proven in this way. For industrial thermal process plants, the C standard EN 746 is harmonized under the Machinery Directive in the EU. In turn, this means that compliance with the EU directives should be proven by the fact that the burner solution corresponds to this C standard.

So how should we proceed if certain points of A, B and C standards contradict each other or even place opposing requirements on the products? For example, EN 62061 and EN ISO 13849-1 require that the safety of safety functions (e.g. of a flame monitor) is verified without gaps. This means from the sensor, through the controller up to the actuator. The safety function must fulfil Safety Integrity Level SIL1 to SIL3 or Performance Level PLa to PLe, depending on the potential danger. In contrast, EN 746-2 states that the safety of a burner controller according to EN 62061 (or EN ISO 13849-1) only needs to be verified for those parts which are not subject to product certifica-tion according to standards for industrial thermal process plants (e.g. according to EN 298). A fail-safe controller (F-CPU) would be an example of such a component.

In practice, this results in a conflict: Should plant safety be verified according to EN 62061 or EN ISO 13849-1 or according to EN 746-2?

The standard EN 13611, which is the basis of further standards for industrial thermal process plants, such as the product standard EN 298, provides a method for converting the assessment of the hardware to SIL/PL. However, despite the same standard basis, this calculated SIL/PL is not the same due to the different objectives.

The reason for this is that EN 13611 defines the requirements for the hardware design via a "class", and not via a "SIL performance level" (or a "category") like with EN 62061 (or EN ISO 13849-1). This makes it very difficult to provide consistent evidence. This results in the absurd situation whereby products developed according to industry-specific standards are delivered with a SIL/PL level which cannot be used to prove the plant safety.

This specific situation raises the question of how we should proceed?

Hierarchical structure of EN standards

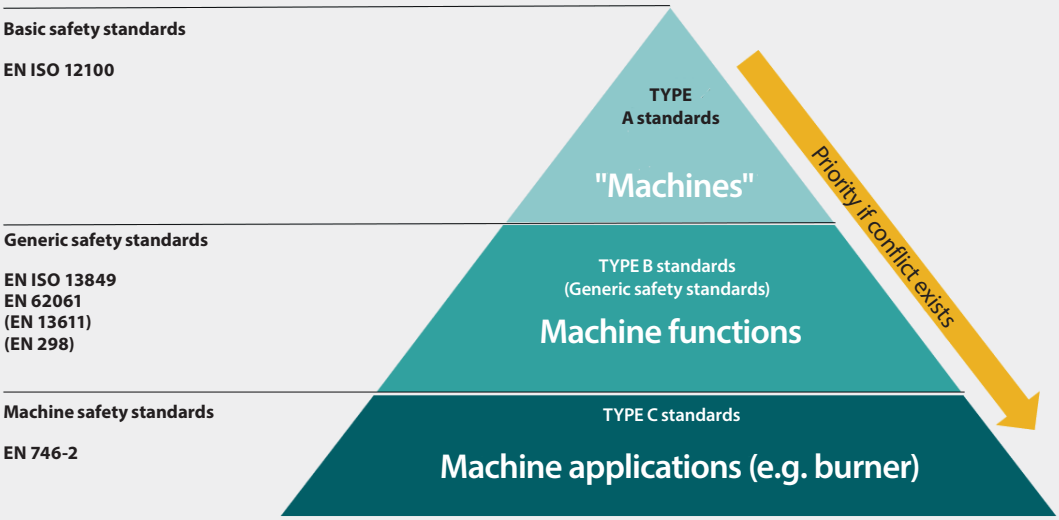

Fig. 1: Standard pyramid (source: Siemens AG)

The standard EN ISO 12100, in which the hierarchical structure of the standards is regulated, provides an answer (**Fig 1**).

According to this, the requirements on machines and plants should be prioritized higher the more application-related a standard is. In this case, this means that the requirements of EN 746-2 should be prioritized highest. In detail, this means that products certified according to product standards for industrial thermal process plants are not considered when calculating the PFH and MTTF of the safety functions in line with the requirements of EN 746-2. This is tantamount to fault exclusion – and the products are not included in the calculation of the probability of failure of the entire safety function (**Fig. 2**).

This is standard-compliant and is allowed – but are thermal process plants always safe from end to end in this case?

Excluding certain subsystems from the safety assessment has the effect that parameters such as multichannel

SIL/PL evaluation comparison
Safety and burner standard: EN 62061 – EN 746-2

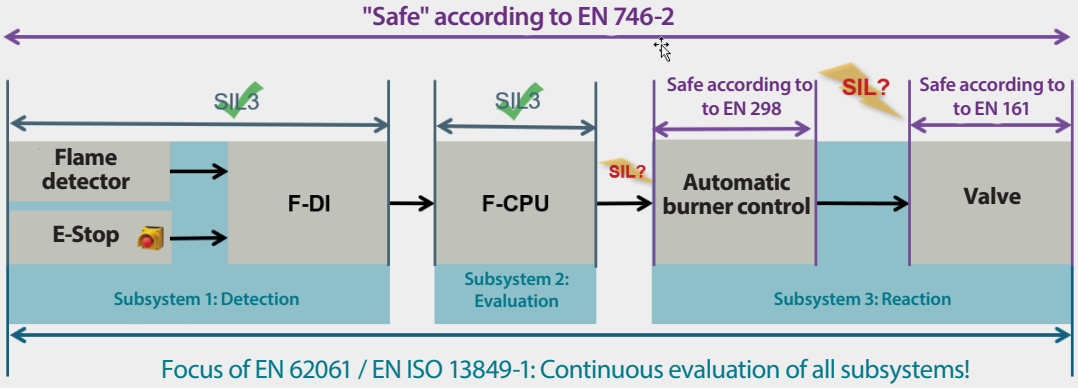

Fig. 2: Safety assessment (source: Siemens AG)

Initial situation: Roller hearth furnace system (example)
Sub-applications/sub-systems and their automation

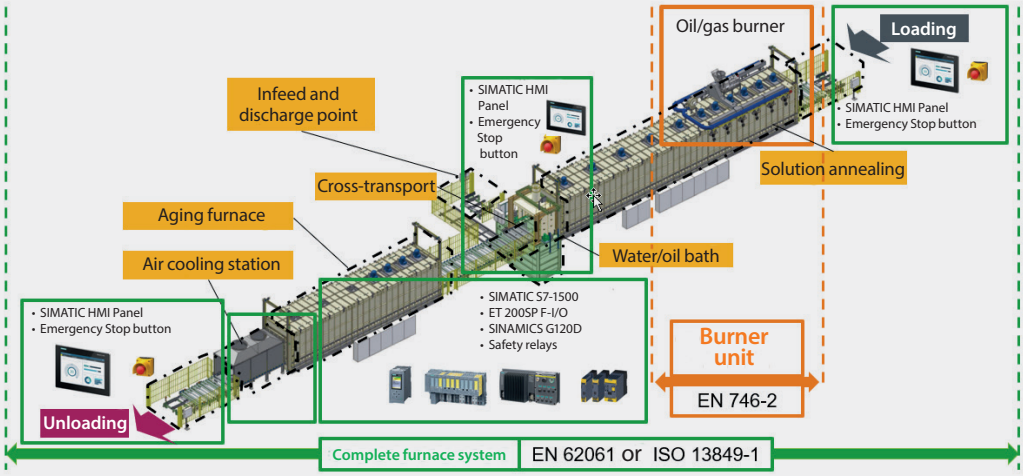

Fig. 3: Schematic structure of a thermal process plant as part of a machine (source: Siemens AG)

capability or diagnostics capability are not considered for this.

And it is precisely here where the potential risks of EN 746-2 lie: If you exclude subsystems of the safety chain from the overall assessment, you ignore interfaces with all the resulting consequences. Irrespective of the question of which standard requirements should be classified higher, it is much more relevant to ask how safety can be assessed from end to end.

- For example, what can be done if an EN 298-compliant automatic burner control is certified as safe in itself, but signal acquisition needs to be "sufficiently ro-bust" according to SIL3/PLe due to the requirement of EN 746-2 on the control system? Where does the requirement of EN 746-2 end – directly at the automatic burner control or at the input module of the controller?
- How can the controller know with sufficient robustness whether a controlled automatic burner control is actually working, and should the automatic burner control be controlled with SIL3/PLe and the operating state be read out with SIL3/PLe? How can it be verified that multiple automatic burner controls can be reliably coordinated with SIL3/PLe if they do not return sufficient feedback?
- What happens with a gas leakage check performed via central controller if the valves required for this are controlled by a local automatic burner control? Does the automatic burner control have to be switched off in compliance with SIL3/PLe in this case and only switched on again after a successful leakage check?
- How do you initiate a SIL3/PLe fault shutdown of a furnace controller (with several individual burners) if the higher-level controller records the temperature centrally, but the control of the safety shutoff valves of each individual burner is the responsibility of an automatic burner control?
- Or in general terms: Is the certification of a flame detector according to relevant product standards still valid if parts of the safety-related functionality of the automatic burner control are outsourced to a central controller and the automatic burner control only acts as its "extended arm"? How can this be proven in specific cases? Is the certification of the automatic burner control itself even still valid?

If even one of these questions cannot be answered positively, an aspect of the safety concept is questionable and it may not be possible to guaranty for end-to-end safety.

In addition, further specific and general questions arise relating to the technical, economic and/or standard-compliant feasibility of certain things.

End-to-end safety is possible

Safe does NOT always really mean safe. To be able to rule out the specified discrepancies and uncertainties, all relevant system components need to be included in the safety assessment. However, this requires EN 61508-compliant components with standardized inter-faces (e.g. PROFIsafe) throughout. Additional connection by means of permanent wiring would be one alternative, but this would be very extensive in complex plants, as well as very inflexible and therefore not future-proof.

End-to-end safety can be implemented in a simpler, more efficient and more convenient – and therefore cheaper – way through the integration of burner-specific safety functions into the existing fail-safe machine controller (**Fig. 3**). In addition, the verification work is much simpler due to the homogeneous standard requirements – especially when all safety functions

1. are standardized
2. are represented in the PLC software program
3. and can be implemented flexibly within the controller.

Part 2 of this article describes in detail how this works.

AUTHORS

Ulf Weißhuhn
Siemens AG
Digital Industries
Nuremberg, Germany
ulf.weisshuhn@siemens.com

Hermann Wübbels
Siemens AG
Digital Industries
Cologne, Germany
hermann.wuebbels@siemens.com

Special edition
07/2020
ISSN 2567-3742
PROZESSWÄRME

Integrated safety for thermo-processing equipment

By **Ulf Weißhuhn, Hermann Wübbels**

As presented in part 1 of our two-part article series ("The path to standard compliant and consistently safe automated thermoprocessing equipment", PW 5/2020), the safety assessment of the complete system including the subsystems could result in some undefined areas in regards to the safety evaluation. A way to standard compliant and consistently safe automated thermoprocessing equipment, which solves this challenge, is the integration of burner-specific safety functions into the fail-safe machine control system. This solution not only fulfils the requirements of EN 746 and ISO 13577, but offers even more advantages for plant manufacturers and operators.

Conventionally, protection systems of burner systems are controlled and monitored by a series of components that all comply with specific product standards (**Fig. 1**): For example, an automatic burner control may meet the re-quirements of EN 298 and a safety shutoff valve can be designed according to the EN 161 standard. In turn, the overall system must fulfil the requirements of the standard EN 746-2, which is relevant for industrial thermal pro-cess plants. This describes such a setup as a "hard-wired system" in which all components are permanently connected to one another without an intermediate PLC. Operational practice certainly shows that these configurations are safe. However, this variant does not consider the use of a higher-level controller and its wiring to the automatic burner control with respect to diagnostics in the event of a fault. Another point is that this variant is not very flexible in terms of changes or the implementation of new or specific tasks. This lack of flexibility is increasingly causing problems for both plant builders and plant operators: For one thing, it can be expected that fluctuations in the composition of natural gas as an energy source will continue to increase. This can be problematic for industrial burner systems in manufacturing companies in particular, because fluctuations in the composition of gas can have a negative efficient on the emission of pollutants, product quality, energy efficiency and the service life of systems or components. This alone is already increasing the demand for more controllable burner systems. On the other hand, there are greater demands on process control, for example when the systems should be run with different temperatures, and the general need of plant builders to improve the ease of operation and maintenance of their plants is growing.

PLC-based, integrated safety solution according to EN 746 and EN 62061

As an alternative to traditional safety systems, it makes sense to integrate the safety functions into the fail-safe automation/controller of the plant.

In the vast majority of cases, the process plants are already equipped with a suitable higher-level controller which addresses actuators and sensors, such as valves, pressure switches and fans, as well as safety equipment, such as emergency stop switches. Such a PLC-based solution is also permissible according to EN 746-2, if the complete system meets SIL3 requirement.

Fig. 2 shows what such a solution could look like based on a protection system in a flame monitoring system. In this configuration, the flame detector monitors the flame via a probe and reports the status over two channels to fail-safe digital inputs (F-DI). The fail-safe controller/PLC (F-CPU) evaluates the signal and controls the safety shutoff valve, which interrupts the fuel supply in the event of a flame failure, via the fail-safe digital output module (F-DQ).

According to EN 62061, in which the structure of a safety function is divided into three subsystems Detection, Evaluation, Reaction, the system looks like this: The flame state is detected through the combination of flame detectors and F-DI, the F-CPU handles the analysis, and the reaction takes place through a cooperation of the F-DQ and the valve. To be able to assess safety according to EN 62061 or EN ISO 13849-1, the entire system therefore needs to

SIL/PL evaluation comparison
Safety and burner standard: EN 62061 – EN 746-2

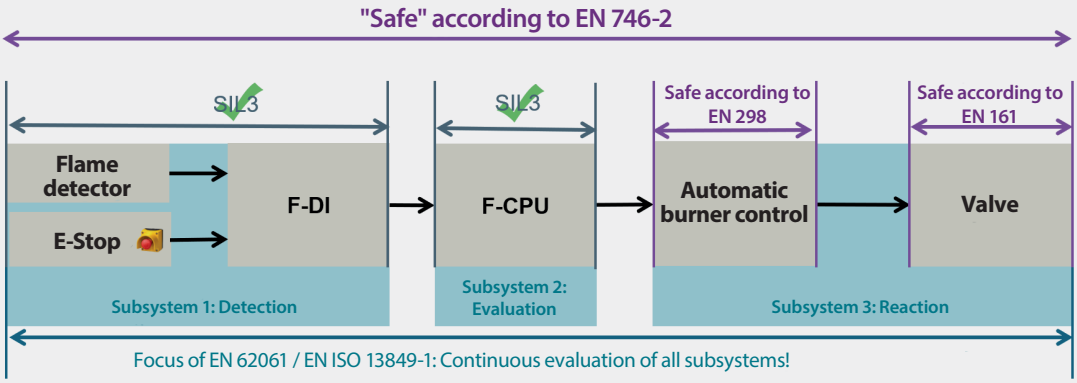

Bild 1: Sicherheitsbetrachtung bei konventionellen Schutzsystemen für Brenneranlagen (Quelle: Siemens AG)

be considered. The specifications of EN 62061 or EN ISO 13849-1 can be used for this purpose according to Section 5.7.2 Part d) of EN 746-2.

Siemens supports the assessment of the safety functions of the overall system required here with the safety evaluation function in the TIA Selection Tool (TST) (**www.siemens.de/safety-evaluation**) for the standards IEC 62061 and ISO 138491. This tool provides the results as a standards-compliant report that can be integrated in the machine documentation as proof of safety (**Fig. 3**). In this way, plant builders can easily prove that the PLC-based solution complies with EN 62061 and therefore also meets the requirements of EN 746. However, the question of how such PLC-based solutions can be integrated in existing burner concepts remains. Especially in continuous furnaces, a large number of burn-er controls must be accommodated in a very small space, so the components of the PLC-based solution need to be correspondingly compact. However, by selecting suitable components, these challenges can be mastered, as shown in Fig. 4. Instead of the usual automatic burner controls that only control and monitor one burner head in each case, a distributed SIMATIC ET 200SP station is used together with correspond-ingly certified flame detectors and ignition transformers in this example. The distributed SIMATIC ET 200SP stations are available in many variants and do not require more space

SIL/PL evaluation comparison
Safety and burner standard: EN 62061 – EN 746-2

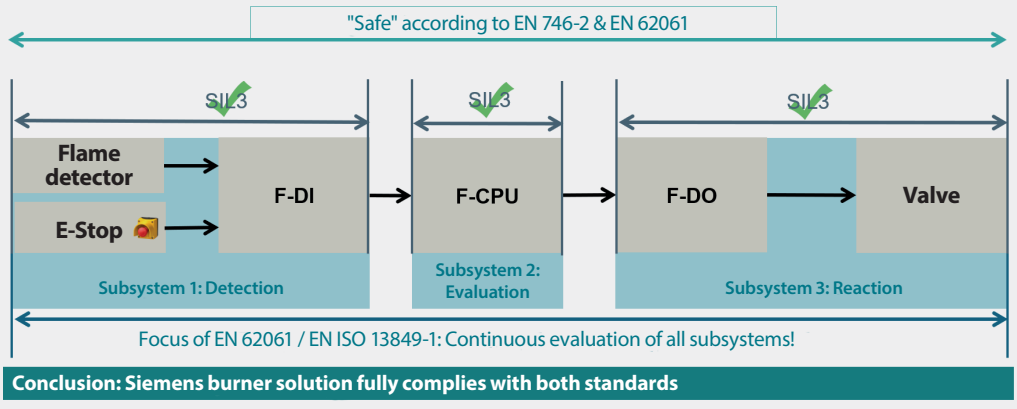

Bild 2: Bewertung einer SPS-basierten Brennerlösung gemäß EN 746 (Quelle: Siemens AG)

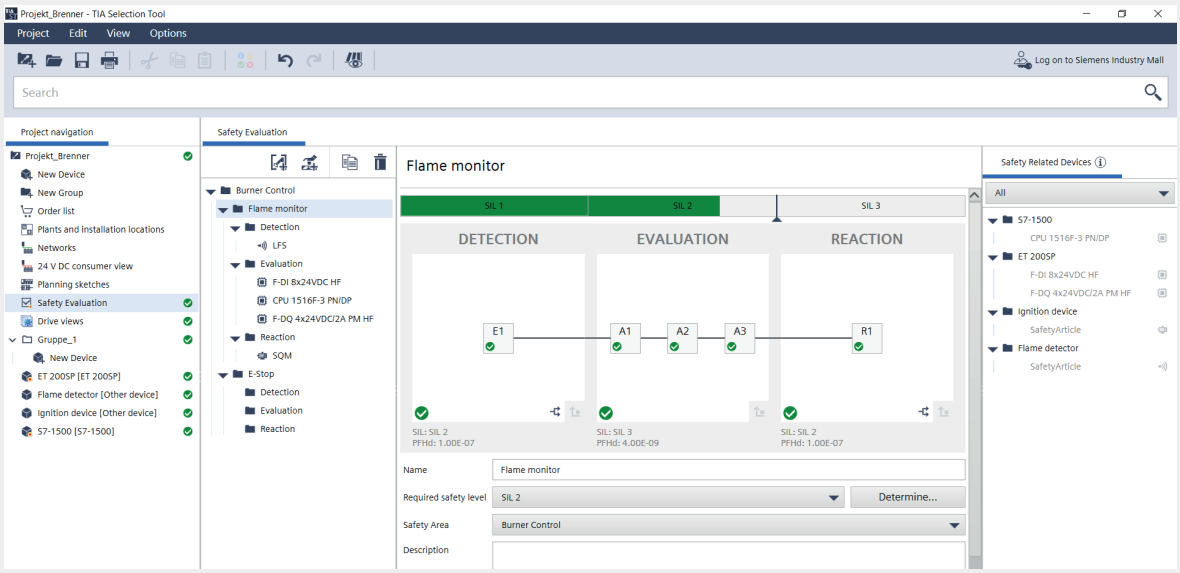

Fig. 3: Assessment of a safety function in the TIA Selection Tool (source: Siemens AG)

than a conventional automatic burner control, but provide greater functionality because further components can easily be integrated in the automation system. Examples are sensors for pressure and temperature monitoring. This means that multiple firing zones and burners can be controlled via an ET 200SP station, which reduces hardware requirements.

An HMI Panel provides additional advantages. The plant operator can thus monitor the plant locally. Through the end-to-end safety solution, complete, detailed system diagnostics is possible, from the wiring to the program sequences. This facilitates efficient maintenance and troubleshooting. The user-friendliness and flexibility are improved not only through the graphical user interfaces, but also through the option of transmitting process parameters to the fail-safe SIMATIC controller via the HMI in a convenient and fail-safe manner (up to SIL 3), for example in order to set a desired process variant.

The overall system is controlled by a fail-safe controller.

Structure of burner controller
Based on SIMATIC S7 1500 and ET 200SP

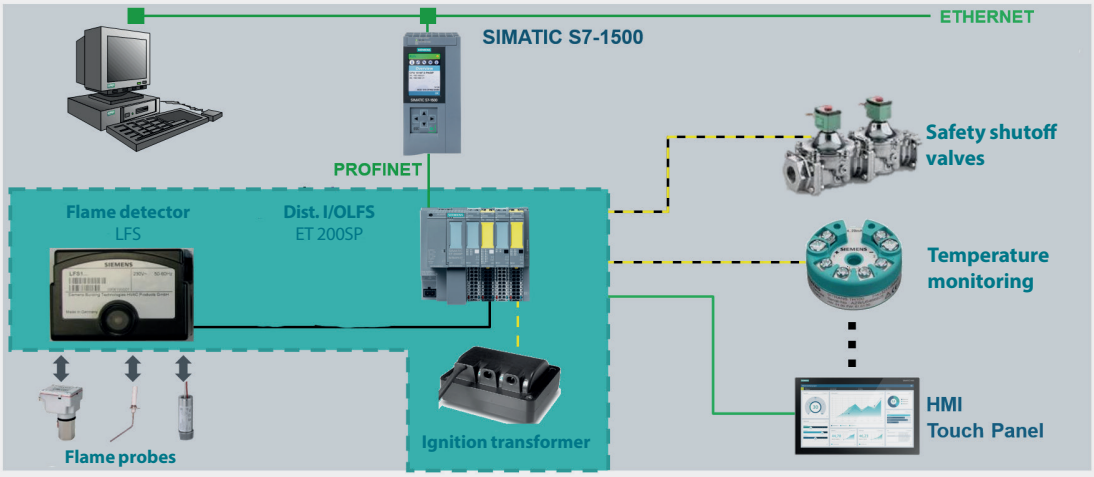

Fig. 4: Safety-related automation of a PLC-based burner controller (source: Siemens AG)

Flexible through software

To implement the safety functions required by EN 746-2 in this system, Siemens provides the user with a block library for configuration in the engineering tool (STEP 7 Professional TIA Portal). This free block library for burners contains several blocks for functions such as controlling and monitoring a gas or oil burner, performing a gas leak-age test, and other burner functions (**support.industry.siemens.com**, entry ID 109477036) The individual functions are modular in structure and can be interconnected as required. In this way, the safety functions for burners can be conveniently created in the familiar configuration environment for the Siemens automation system, which reduces the engineering workload and facilitates migration to an integrated PLC-based safety solution. Another advantage for the plant builder is that addi-tional functions can be retrofitted at a later time and customer specific functions can be implemented. The PLC-based solution also provides significant advantages in terms of the control quality when realizing the following burner functions:

- Realization of an electronic compound itself, e.g. via a defined air/fuel ratio
- Temperature control
- Oxygen control based on the residual oxygen in the exhaust gases.

Overall, this enables the burners to cope better with fluctuating gas compositions so that the plant operators not only avoid additional emissions and quality losses due to process fluctuations, but can also optimize the energy efficiency of their plants.

A PLC-based safety solution offers advantages in many cases because it often uses existing systems, such as a higher-level controller. Through the use of a suitable system configuration, all of these advantages can be used and continuous plant safety can be guaranteed – also according to the globally valid standard ISO 13577.

AUTOREN

Ulf Weißhuhn
Siemens AG
Digital Industries
Nürnberg
ulf.weisshuhn@siemens.com

Hermann Wübbels
Siemens AG
Digital Industries
Köln
hermann.wuebbels@siemens.com