Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P0382-cd

The Hidden Gem of IEC 61508: Unveiling the Advantages of the 1oo2D Structure in Embedded Systems

Prof. Dr.-Ing. David Schepers

Department of Safety Engineering, University of Applied Sciences Ruhr West, Germany.
E-mail: david.schepers@hs-ruhrwest.de

M.Sc. Sarah Schwarzer

Department of Safety Engineering, University of Applied Sciences Ruhr West, Germany.
E-mail: sarah.schwarzer@hs-ruhrwest.de

Prof. M.A.T.I. Jesús Hernández Cosío

Department of Computer Systems, Autonomous University of Baja California Sur, Mexico.
E-mail: jhernandez@uabcs.mx

Prof. Dr.- Ing. María Z. Flores López

Department of Earth Sciences, Autonomous University of Baja California Sur, Mexico.
E-mail: m.zflores@uabcs.mx

Embedded systems are used in a wide range of applications, many of which are safety-critical. A failure in such systems can cause significant issues related to safety, functionality, and the overall availability of the application. To meet safety requirements, it is often necessary to develop safety-critical embedded systems in compliance with the IEC 61508 functional safety standard. This standard outlines various architectures for safe hardware design, with common safety structures including 1oo1, 1oo2, and 2oo3, which are widely implemented for safety functions. The optimal solution depends on several factors, such as the desired Safety Integrity Level (SIL), cost constraints, and application availability. This paper emphasizes the rarely applied 1oo2D structure as an excellent compromise between cost, assembly space, safety, and availability. The 1oo2D architecture consists of two redundant channels continuously monitoring themselves for hardware failures. With intelligent testing mechanisms, hardware failures can be isolated to the relevant channel, allowing the faulty channel to be deactivated while the system continues to operate in a reduced 1oo1 configuration. This approach helps prevent spurious trips of the safety function without the need for the more costly 2oo3 structure. To demonstrate the advantages of the 1oo2D structure, a newly developed prototype of an optical smoke detector is introduced, which highlights the advantages of the 1oo2D structure based on a new intelligent fault detection concept for sensor and actuator sub-systems. A Failure Modes, Effects, and Diagnostic Analysis (FMEDA) shows that all potential hardware failures can be safely detected and assigned to the corresponding channel, thereby avoiding false fire alarms while ensuring the availability of the safety function. Digital embedded systems are particularly well-suited for implementing the 1oo2D structure, as hardware failures can typically be detected and isolated to the relevant channel. This reduces spurious trips of the safety function while ensuring high reliability, low costs, compact assembly, and availability.

Keywords: Functional Safety, IEC 61508, Reliability, Electronic Embedded Systems, Optical Smoke Detector.

1. Introduction

The functional safety standard IEC 61508 is an international industrial standard that defines requirements for safety functions for risk reduction. Control of random hardware failures and the avoidance and control of systematic faults within electric, electronic, and programmable electronic safety-relevant systems are the main objectives of the standard. For this purpose, the standard defines hardware and software development requirements depending on the specific risk that the safety function shall

reduce. This contribution shows the advantages of the rarely applied 1oo2D hardware architecture within embedded digital electronic systems based on a new optical smoke detector concept and further explains the limits for applying this structure.

2. Common safety architectures of IEC 61508: 1oo1, 1oo2 and 2oo3

IEC 61508 proposes different hardware architectures for the implementation of safety functions. The most common safety architectures are 1oo1, 1oo2, and 2oo3, which will be briefly introduced.

The 1oo1 architecture consists of one single channel only (Fig. 1). In the event of a component failure, the safety function will trip, or the failure will immediately lead to the unavailability of the safety function. This architecture is the cheapest solution and is usually applied to mitigate lower risks because it is not always possible to detect the loss of the single channel before a hazardous event occurs.

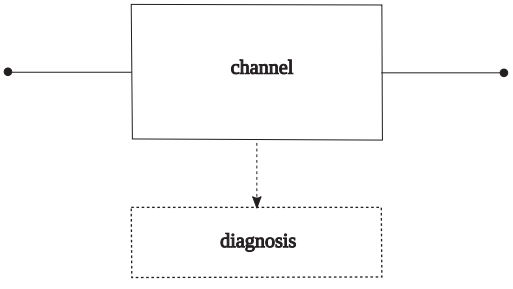

Fig. 1: Block diagram of 1oo1 architecture (acc. to IEC 61508-6 2010)

When applying the 1oo2 architecture, each channel can process the safety function independently (Fig. 2). The loss of one channel within this redundant structure does not immediately lead to a dangerous system failure as the second channel is still available. However, external disturbances or component failures may lead to the demand of the safety function and, therefore, to an undesired spurious trip because the disturbance or component failure cannot always be identified and allocated to the respective channel. This is not critical from a safety point-of-view but may reduce the availability of the industrial application.

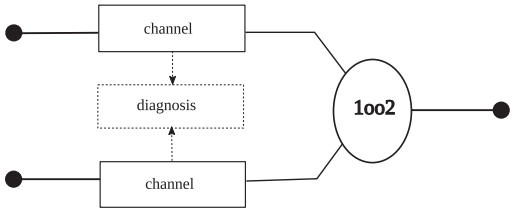

Fig. 2: Block diagram of 1oo2 architecture (acc. to IEC 61508-6 2010)

The 2oo3 architecture (Fig. 3) consists of three channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only one of the three channels demands the safety function. It is assumed that diagnostic testing would only report the faults found and not change any output states or the output voting (IEC 61508-6 2010). If a second channel fails before the previously failed channel can be repaired or replaced, the system will fail dangerously. The 2oo3 architecture is often used in the process industry because it ensures high availability and safety, which is particularly important in this field of application (Basilio 2021; IEC 61511 2016).

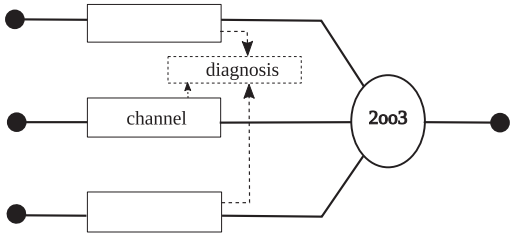

Fig. 3: Block diagram of 2oo3 architecture (acc. to IEC 61508-6 2010)

Further information on 1oo1, 1oo2, and 2oo3 structures and practical examples can be found in safety-related publications (e.g., Basilio et al. 2021; Börcsök 2021).

3. Special features of the 1oo2D architecture

The so-called 1oo2D safety architecture (Fig. 4) is rarely used to implement safety functions. One possible reason is that this architecture is not mentioned or explained in detail in many functional safety publications or sector standards and in many cases, practical examples for implementing this safety structure are missing

(Basilio et al. 2021; Börcsök 2021; IEC 61508-6 2010; IEC 61511 2016; ISO 13849 2023; VDI/VDE 2180 2019; VDI-EE 4020 2024; Wratil et al. 2010; Xie et al. 2023).

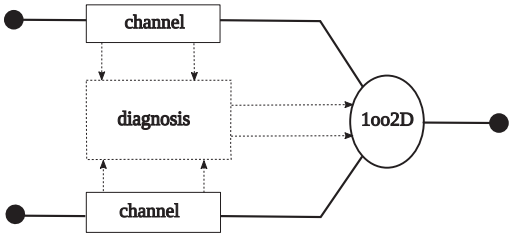

Fig. 4: Block diagram of 1oo2D architecture

According to IEC 61508-6, a 1oo2D architecture consists of two channels connected in parallel. In regular operation, both channels must demand the safety function for it to be executed. In addition, if the diagnostic tests in either channel detect a fault, the output voting is adapted so that the overall output state follows that given by the other (faultless) channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, the output goes to the safe state. Following this definition, the term 1oo2D seems to be misleading because, in fact, 1oo2D describes a 2oo2 architecture with fault diagnosis, which degrades to a 1oo1 architecture if a fault is detected in one of the channels (Hokstad 2005).

3.1. Advantages regarding reliability, availability, and possible spurious trips

Diagnostic tests and the redundant structure of the 1oo2D structure ensure that the safety function is more reliable than the 1oo1 structure. Disturbances or component failures that might cause a deviation between the two channels do not lead (in contrast to the 1oo2 architecture) to a spurious trip of the safety function. In case of a failure in one channel, the other (faultless) channel remains active, and the safety function remains available. Using only two channels, the 1oo2D structure is cheaper than the 2oo3 structure, although it offers similar advantages. Thus, the 1oo2D structure is an excellent compromise between reliability, availability, prevention of spurious trips, and costs (Schepers et al. 2023).

3.2. Challenges for implementation of the 1oo2D structure

The main challenge for implementing the 1oo2D structure is realizing “intelligent” self-diagnosis mechanisms to detect and allocate faults to the respective channel. Also, special requirements for fault detection time must be considered in high-demand mode. This might not be easy, as the following example illustrates. Fig. 5 shows a redundant architecture of a safety function for safe temperature monitoring.

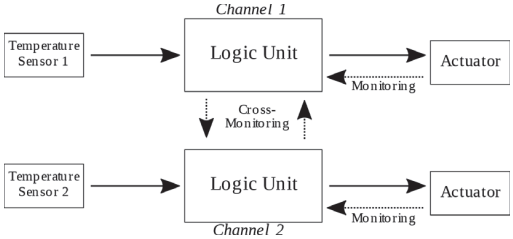

Fig. 5: Redundant temperature monitoring

Suppose the applied temperature sensors deliver (analog) temperature values. Allocating the fault to the respective channel is impossible if a deviation between the two sensors occurs due to an external disturbance or component failure. It cannot be determined which of the two sensors delivers the correct or wrong temperature value. If one sensor demands the safety function, the system must always go to a safe state to avoid risk, even if the demand of the safety function is a consequence of a sensor fault or external disturbance. Thus, this sensor type does not apply to the 1oo2D structure, and spurious trips can only be avoided by applying the (more expensive) 2oo3 architecture with an appropriate voter (Basilio et al. 2021; Börcsök 2021). Furthermore, if using the 1oo2D structure in high-demand mode, fulfilling the requirements for fault detection is challenging. The sum of the diagnostic test interval and the time to perform the specified action to achieve a safe state must be done within the process safety time (PST), or the ratio of the diagnostic test rate to the demand rate of the safety function must equal or exceed 100 (IEC 61508-6 2010).

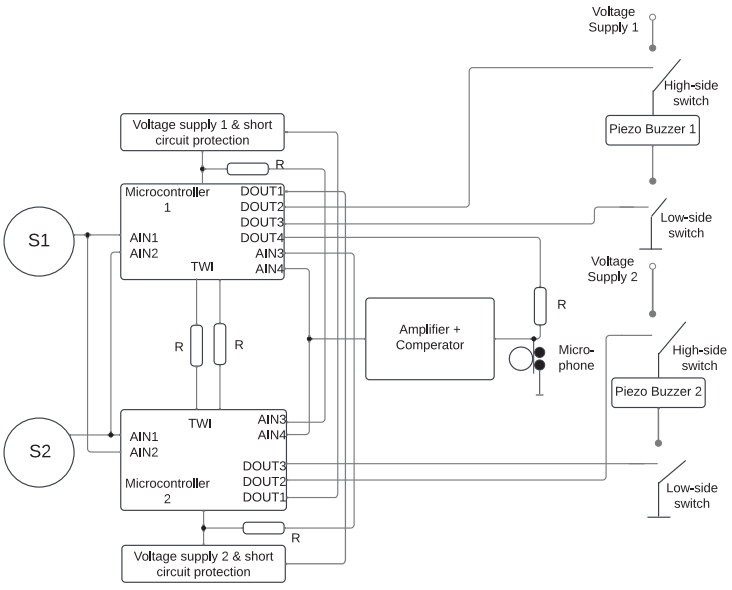

Fig. 6: Redundant 1oo2D structure for smoke detector

Self-tests for logic units (e.g., microcontrollers) are time-consuming, and therefore, it must be verified in advance if the 1oo2D structure is applicable for high-demand mode regarding the requirements for fault detection time. These requirements depend on the specific application.

4. Example: Highly Reliable Optical Smoke Detector based on 1oo2D structure

Applicable European standards for smoke detectors are, among others, EN 14604 and EN 54-7 (EN 14604 2005, EN 54-7 2018). However, the requirements of EN 54-7 and EN 14831 do not include the relevant aspects of functional safety. By now, applying IEC 61508 is not mandatory for developing smoke detectors. External disturbances or component failures may lead to a false alarm, or the smoke detector may fail to detect a fire event. In order to significantly improve the reliability and availability of the smoke detector and to avoid possible false alarms due to external disturbances or component failures, a new prototype of a smoke detector was developed based on the 1oo2D structure. The smoke detector prototype is based on the scattered light principle. This kind of smoke detector contains a light-emitting (infrared) diode and a photo element in its measuring chamber (Fig. 7). Only if smoke enters the measuring chamber the infrared radiation from the emitting diode will be scattered by the smoke particles and reach the photoelement, activating an alarm in order to warn people.

Fig. 7: Measuring chamber of smoke detector based on scattered light detection

Fig. 6 shows the proposed redundant structure for the smoke detector to be developed, consisting of sensor elements (S1, S2), logic units (microcontrollers 1 and 2), and actuators (piezo buzzers 1 and 2). Each channel can test itself or elements of the other channel to detect faults and allocate them to the respective channel. The technical details are described in the following sections.

4.1. Sensor for Smoke Detection

Fig. 8 depicts the new smoke detection sensor concept. Each channel of the sensor unit consists of two infrared diodes (emitters) and one photodiode (receiver). The crosswise arrangement allows intelligent self-testing of all components.

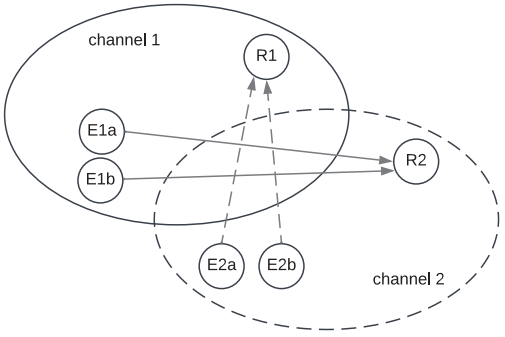

Fig. 8: Redundant architecture of smoke detection sensor

Without smoke in the chamber, receiver R1 of channel one does not detect (scattered) light. In contrast, receiver R2 of channel two can be used to test the functionality of emitter E1a and emitter E1b of channel one. Two emitters are necessary for each channel to allocate all possible faults to the respective channel. The same applies to channel two. This is essential for the implementation of the 1oo2D structure.

The timing diagram in Fig. 9 illustrates the smoke detection and intelligent fault diagnosis strategy. The diagram shows the digital signals (H: high signal, L: low signal) at the sending infrared diodes and the digital signals at the receivers, assuming all components are faultless. A high signal at the sender means the corresponding sending diode is activated. A low signal at the receiver means light is received (either scattered light in case smoke enters the chamber or light of the opposite diode of the other channel). When E1a sends at time T1, R2 must receive the light, and the digital signal must be low. The digital signal of R1 is only low if smoke is detected; otherwise, it will be high. The same applies when E1b sends at time T2.

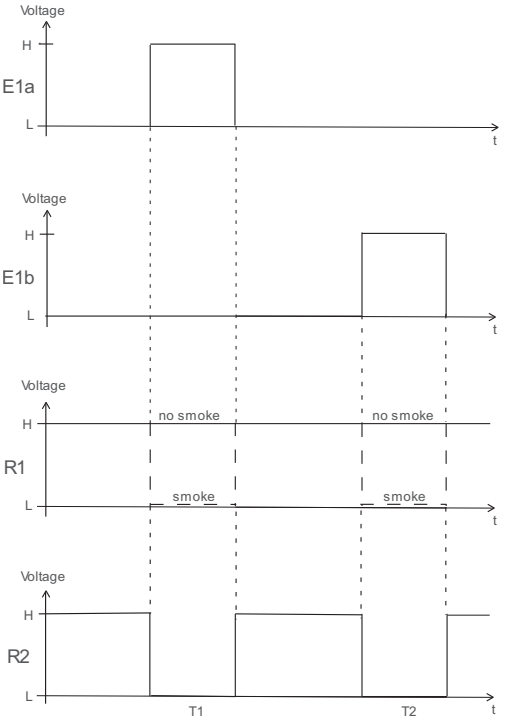

Fig. 9: Timing diagram for realization of diagnosis

Table 1 shows the logic evaluation of R2 for fault diagnosis. This intelligent fault diagnosis strategy can detect and allocate all possible sensor faults to the respective channel.

Table 1. Logic table for sensor fault diagnosis

Time	Sender	Receiver	Status
T1	E1a HIGH	R2 LOW	Sensor OK
T2	E1b HIGH	R2 LOW	
T1	E1a HIGH	R2 HIGH	E1a defective
T2	E1b HIGH	R2 LOW	
T1	E1a HIGH	R2 LOW	E1b defective
T2	E1b HIGH	R2 HIGH	
T1	E1a HIGH	R2 HIGH	R2 defective
T2	E1b HIGH	R2 HIGH	

The same logic table for sensor fault diagnosis applies to senders E2a/E2b and R1. Thus, all possible sensor faults can be detected and allocated to the respective channel.

4.2. Logic Unit

The logic unit consists of two (simple) microcontrollers (Fig. 6), which evaluate the sensors, and in case scattered light is detected using the photodiodes, an acoustic alarm is activated. The software implements fault detection mechanisms for all components (sensor, logic, and actuator elements). Different methods for fault detection are applied, and the diagnostic coverage (DC) can be estimated based on IEC 61508-2 (IEC 61508-2 2010) or determined by an FMEDA, as shown in Table 2. All relevant functional units are tested using appropriate diagnosis functions. An FMEDA determined the resulting DC for the sensor to be 99 %, and the (conservative) estimation for both the logic unit and the actuator is DC = 60 %.

Table 2. Measures for fault detection and DC

Element	Measures for fault detection by software	DC
Sensor	Dynamic test pattern (DC determined by FMEDA)	99 %
Logic Unit	Combination of temporal and logical monitoring of program sequences with independent time bases, march-C RAM test, flash test (CRC), register tests by test pattern, voltage monitoring with overvoltage and short-circuit protection, dynamic test pattern for ADC	60 %
Actuator	Monitoring of sound pressure level	60 %

4.3. Acoustic Actuator

Piezo buzzers are applied to implement the acoustic actuators. If both channels are fault-free, the buzzer of channel one is applied in case of an alarm. If channel one fails, the alarm will be indicated by the buzzer of channel two. Fig. 6 shows the redundant structure of the actuator unit. The acoustic actuators are tested through an electret microphone, an amplifier, and a comparator. The detection level of the comparator can be adjusted to the sound pressure level of the piezo buzzers. The test can be conducted by a short activation of the buzzer (approx. 50 ms) and detecting the sound pressure level at the microphone. Each piezo buzzer can be tested independently. This newly developed testing strategy allows dangerous failures (no sound or low sound pressure level) to be detected and allocated to the respective channel. High-side and low-side switches are applied to prevent false alarms due to a defective switch.

4.4. Software Structure

According to IEC 61508-3 (IEC 61508-3 2010), the software must be developed considering the V-model and all relevant measures for fault avoidance. The software's main tasks are:

- Implementation of fault diagnosis for all components, and deactivation of the respective channel in case of fault detection.
- Evaluation of the optical sensors.
- Activation of acoustic alarm in case the optical sensors detect smoke.

The flow chart visualizes the software structure in Fig. 10.

Before the sensors are evaluated to detect smoke, each channel tests itself for possible faults. If the channels are fault-free, both must detect smoke to activate an alarm. If one channel detects a fault, it is deactivated, and a blinking LED is activated to show that the smoke detector must be replaced. The remaining channel guarantees that the smoke detector's functionality is still available until the device is replaced.

5. Analysis of the 1oo2D Optical Smoke Detector

The optical smoke detector's electrical circuit in 1oo2D architecture was analyzed in detail through an FMEDA (Failure Modes, Effects, and Diagnostic Analysis). The results are summarized in Table 2.

The FMEDA results show that most dangerous failures can be detected (depending on the DC for each component). All detectable failures can be allocated to the respective channel; consequently, the faulty channel can be deactivated. As the correct functionality of each channel is tested just before the sensors are evaluated, the probability of spurious trips due to component failures is very low.

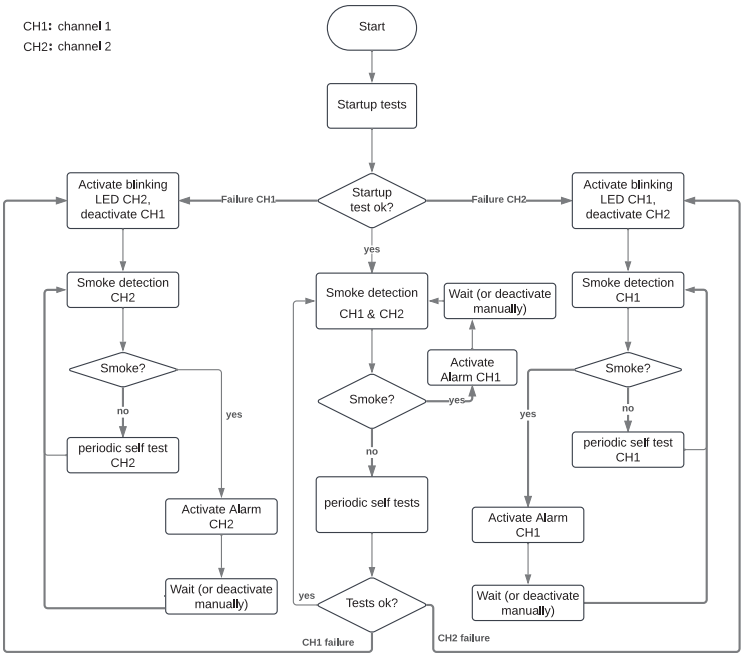

Fig. 10: Software flow chart

This was verified not only by the FMEA but also by practical fault injection tests.

The Probability of Dangerous Failure per Hour (PFH_D) for high demand mode of the safety function and the Average Probability of Dangerous Failure on Demand (PFD_{avg}) for low demand mode of the safety function was calculated for the optical smoke detector in 1oo2D architecture based on the formulas of IEC 61508-6 (IEC 61508-6 2010):

$$PFD_{avg} = 2(1-\beta)\lambda_{DU}\big((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\big)t_{CE}{}'t_{GE}{}' + 2(1-K)\lambda_{DD}t'_{CE} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (1)$$

$$PFH_D = 2(1-\beta)\lambda_{DU}\big((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\big)t'_{CE} + 2(1-K)\lambda_{DD} + \beta\lambda_{DU} \quad (2)$$

$$\text{with } t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{\lambda_{DU}+(\lambda_{DD}+\lambda_{SD})} \quad (3)$$

$$\text{and } t'_{GE} = \frac{T_1}{3} + MRT \quad (4)$$

Conservative assumptions of the applied parameters are: DC (for whole channel) = 60 %, K = 60 %, λ (whole channel) = $401 \cdot 10^{-9} \cdot h^{-1}$, β = 5 %, β_D = 5 %, MTTR = 1008 h, MRT = 336 h, T_1 = 20 years (lifetime). For details on calculating PFD_{avg} and PFH_D, refer to (Schepers et al. 2023).

Results of the calculations:

$$PFD_{avg} = 2.24 \cdot 10^{-3}$$

$$PFH_D = 1.01 \cdot 10^{-7}\frac{1}{h}$$

$$SFF = 80\ \%$$

Both probabilities are below the allowed limits of SIL 2, and the structural requirements, according to Table 3 of IEC 61508-2 (IEC 61508-2 2010), are also fulfilled for SIL 2. Therefore, the optical smoke detector based on the 1oo2D structure fulfills the probabilistic and structural requirements for a SIL 2 safety function.

6. Summary and Conclusion

The 1oo2D safety architecture offers some important advantages compared to the widely applied 1oo2 or 2oo3 architectures. The 1oo2D structure may avoid unwanted spurious trips of the safety function and offers a good compromise between reliability and availability versus costs and space requirements. This applies especially to safety functions in low-demand mode. A new concept of an optical smoke detector showed how the 1oo2D structure could be implemented and how the necessary self-diagnosis routines could be realized using appropriate hardware design and software routines.

However, to implement the 1oo2D architecture, "intelligent" self-diagnosis must detect and allocate faults to the respective channel. Especially for simple analog sensors, this might be a challenge. As the 1oo2D architecture does not allow a discrepancy between both channels in high-demand mode, it is essential to detect possible faults before the safety function is demanded. Otherwise, the safety function will not be executed if a faulty channel leads to a discrepancy between both channels. Depending on the PST (Process Safety Time), executing all self-tests in time might not be possible. The microcontroller self-tests (see Table 2) are especially time-consuming and might not fulfill the requirements.

To solve this problem for applications in high-demand mode, it might be possible only to realize the sensor elements in 1oo2D architecture and use the classic 1oo2 for the logic and actuator elements. The drawback of this solution is a higher probability of spurious trips due to possible component failures in logic units or actuators.

References

Basilio, A., G. Landrini, and T. V. Capelle (2021). *Safety Instrumented Systems – Manual for Plant Engineering and Maintenance* (4th Edition). G.M. International s.r.l., Villasanta, Italy.

Börcsök, J. (2021). Funktionale Sicherheit – *Grundzüge sicherheitstechnischer Systeme.* VDE Verlag, Berlin, Germany.

EN 14604 (2005). *Smoke alarm devices.* European Standard of the European Committee for Standardization (CEN).

EN 54-7 (2018). *Fire detection and fire alarm systems – Part 7: Smoke detectors – Point smoke detectors that operate using scattered light, transmitted light or ionization.* European Standard of the European Committee for Standardization (CEN).

Hokstad, P. (2005). *Probability of Failure on Demand (PFD) - the formulas of IEC 61508 with focus on the 1oo2D voting.* Proceedings of the European Safety and Reliability Conference, ESREL 2005, Tri City (Gdynia-Sopot-Gdansk), Poland, 27-30 June 2005. CRC Press.

IEC 61508-2 (2010). *Functional safety of electrical/ electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.* International Standard of the International Electrotechnical Commission (IEC).

IEC 61508-3 (2010). *Functional safety of electrical/ electronic/programmable electronic safety-related systems, Part 3: Software requirements.* International Standard of the International Electrotechnical Commission (IEC).

IEC 61508-6 (2010). *Functional safety of electrical/ electronic/programmable electronic safety-related systems, Part 6: Guidelines on the application of IEC 61508-2/-3.* International Standard of the International Electrotechnical Commission (IEC).

IEC 61511 (2016). *Functional safety – Safety instrumented systems for the process industry sector,* Parts 1-3. International Standard of the International Electrotechnical Commission (IEC).

IEC 62061 (2021). *Safety of machinery - Functional safety of safety-related control systems.* International Standard of the International Electrotechnical Commission (IEC).

ISO 13849 (2023). *Safety of machinery – Safety-related parts of control systems,* Parts 1 and 2. International Standard of the International Organization for Standardization (ISO).

Schepers, D. and S. Schwarzer (2023). *Cyber-Physical Systems and Control II (Proceedings of the 2nd International Conference on Cyber-Physical Systems and Control)*, pp. 168 – 181. Springer Nature Switzerland AG, Cham, Switzerland.

VDI/VDE 2180 (2019). *Functional safety in the process industry,* Parts 1-4. Verein Deutscher Ingenieure (VDI), Düsseldorf, Germany.

VDI-EE 4020 (2024). *Einführung in die Funktionale Sicherheit nach IEC 61508.* Verein Deutscher Ingenieure (VDI), Düsseldorf, Germany.

Wratil, P. and M. Kieviet (2010). *Sicherheitstechnik für Komponenten und Systeme.* VDE Verlag, Berlin, Germany.

Xie, G., Y. Zhang, R. Li, K. Li, and K. Li (2023). *Functional Safety for Embedded Systems.* CRC Press, Boca Raton, USA