CHEMICAL ENGINEERING TRANSACTIONS
VOL. 116, 2025
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani

ISBN 979-12-81206-18-2; **ISSN** 2283-9216
DOI: 10.3303/CET25116010

Integrating Machinery Safety Functions into Functional Safety for Process Industry

Gregor Schmitt-Pauksztat[a], Dirk Hablawetz[b], Marco Knödler[c], Dominic de-Kerf[d], Christian Demski[e], Marc Risser[b], Udo Dehner[f]

[a]Bayer AG, 51368 Leverkusen, Germany
[b]BASF SE, 67056 Ludwigshafen, Germany
[c]YNCORIS GmbH & Co. KG, 50354 Hürth, Germany
[d]Cargill, 4551 LA Sas van Gent,The Netherlands
[e]DOW Deutschland Anlagengesellschaft mbH, 21677 Stade, Germany
[f]dsm-firmenich, 4303 Kaiseraugst, Switzerland
gregor.schmitt-pauksztat@bayer.com

From a Process Industry point of view, the integration of Machinery Safety Functions into Functional Safety for Process Safety has always been a challenge. Generally, concepts of IEC 61511 „Functional safety – Safety instrumented systems for the process industry sector" are the basis for safety functions in Process Industry – however these concepts are somehow incompatible with Functional Safety implementations of machines according to IEC 62061 or ISO 13849. Examples are differences in prior use vs. "well-tried safety principles" and proof test approaches and of course the fundamental question of high and low demand of a safety function. Also, the target measure for the risk associated with the two principles are different. One is focusing mainly on very rare events with a high impact where the other is focusing mainly on frequent scenarios with a moderate to low impact.

1. Introduction

IEC 61508 with its first edition in 1999 set out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical / electronic / programmable electronic systems (E/E/PESs)) that are used to perform safety functions. This unified approach had been adopted in order to develop a rational and consistent technical policy for all electrically based safety-related systems. It was intended to facilitate the development of application sector standards based on the common ground of referred unified approach, most prominently aligned in form of the "SIL" – Safety Integrity Level as the main attribute for the ability of risk reduction of E/E/PESs.
25 years of applying IEC 61508 as well as deriving and applying application sector standards on the one hand demonstrate the added value of programmable and automated systems taking care of their share of safety – to be understood as appropriate risk reduction – due to the reliability as well as flexibility of this approach in the context of upgrades and changes in the operation of existing production units.
On the other hand, one can argue that part of the common ground was obviously lost over the years and over the process of deriving and further elaborating on application sector standards, especially outside the IEC realm. The most prominent example in process industry operation might be found in the context of Machinery Safety and Process Safety, even prominently differing in the designation of the ability of risk reduction of E/E/PESs – SIL in the IEC realm vs. PL – Performance Level in ISO 13849.
In process industry operations, it is not uncommon to have machinery and process equipment in operation in a close integration.

Paper Received: 30 November 2024; Revised: 27 January 2025; Accepted: 2 April 2025
Please cite this article as: Schmitt-Pauksztat G., Hablawetz D., Knoedler M., de-Kerf D., Demski C., Risser M., Dehner U., 2025, Integrating Machinery Safety Functions Into Functional Safety for Process Industry, Chemical Engineering Transactions, 116, 55-60 DOI:10.3303/CET25116010

2. Multiple standards in real life

In Process Industry's real life, the existence of different standards for one problem "Functional Safety" leads to astonishing solutions. One example is the implementation of two safety functions for the same risk – one according to IEC 61511 and the second one according to ISO 13849, which is shown in Figure 1. The filling chamber of a filling line needs to be heated for product to keep fluid. The manufacturer of the machine already implemented a heat protection according to ISO 13849 to not overheat the equipment.

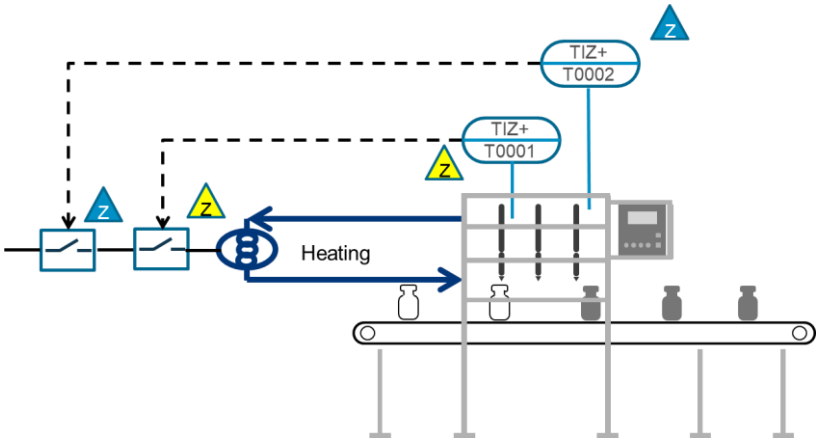

Figure 1: Safety functions to avoid overheating in a filling line

In Figure 1 this is marked with yellow triangles. For Process Safety reasons an additional safety function for heat protection due to the product properties was implemented separately according to IEC 61511, see blue triangles in Figure 1.
Both safety functions target the heat of the product but the equipment for instrumentation is selected with different boundary conditions. They might even lead to different Hardware fault tolerance and therefore redundant implementations in one implementation but not the other.
The main reason for this deficiency is that – although all safety standards refer to IEC 61508 – standards are developed by different panels. Sometimes in the beginning of the creation of new standards, it's not obvious what other neighbouring standard may be affected.
The double implementation of the example in Figure 1 may be compliant to all regulatory requirements but do not increase necessarily the safety of a process plant. It only increases cost and may even lead to confusion when doing maintenance.

The NAMUR working group 4.5 Functional Safety and working group 4.5.1 Machinery Safety have taken up the challenge of finding pragmatic solutions for implementing Machinery Safety Functions in Process Safety Functional Safety Systems, e.g. leveraging from existing complex Machinery Safety Functions or simply using Machinery Safety equipment as part of Functional Safety for Process Industry.
The following sections describe three best practices, how to merge Machinery Safety Functions into Process Industry Safety Functions.

- If the decision is still possible, whether a safety function is built according to Machinery Safety or Process Safety, consider the section "Decide up front".
- From a company's point of view, acknowledging the equivalence of both measure types is an easier approach. This is discussed in section "simply accept the equivalence".
- If for any reason, both approaches are not helpful and you are stuck with Machinery Safety components that must be integrated in a Process Safety Function, refer to section "combination".

3. Decide up front

In HAZOP studies of process industry there is often a discussion whether safety functions for Machinery Safety shall be discussed within the regular process safety HAZOP or not. The challenge is that, when separating the discussion – e.g. first discuss Machinery Safety risks and afterwards discuss process safety risks – one might end up with two separate safety functions that need to be implemented. When taking both risk types, Machinery Safety and Process Safety, in a combined discussion, safety engineers might struggle what kind of measure to implement – Machinery Safety or Process Safety.

The general approach when designing new safety functions shall follow the target of a safety function. If the main risk is Machinery Safety, go for a Machinery Safety function. If the target is Process Safety, go for a Process Safety function.
That's easier said than done. In the Machinery Directive, Directive 2006/42/EC and its replacement, Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery, there is no differentiation between Machinery Safety and Process Safety (see annex III of Regulation (EU) 2023/1230). Generally, all hazards need to be considered within Machinery Safety – not only e.g. moving parts or falling from heights.

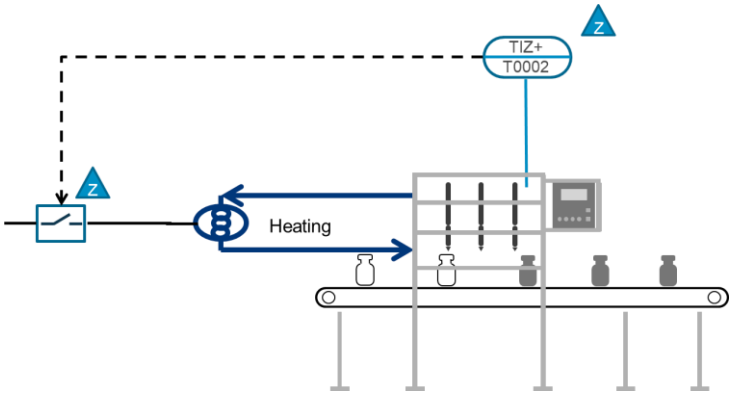

Figure 2: Process Safety Function to avoid overheating in a filling line

However, the generally accepted approach is to cover e.g. "risks related to moving parts", "moving parts involved in the process", "electricity supply hazards", "risk of being trapped in a machine" via Machinery Safety, and cover "static electricity", "explosion", "chemical risks" via Process Safety.
There is only a choice to be made up front of a safety study – machinery risk assessment or HAZOP. There is no perfect approach to cut between Machinery Safety and Process Safety - as long as safety risks are addressed.
A common approach is to decide on higher severity of impact, giving higher severities to Process Safety. The overheating protection could protect an operator from being burnt (Machinery Safety) but it could also prevent the product from reaching its decomposition temperature with potential multiple fatalities (Process Safety).
Considering the example from Figure 1, the decision on what standard to follow the safety function would be up front. Assuming that the target of the safety function is preventing the product from reaching its decomposition temperature, the Safety Function would be designed according to IEC 61511. And ideally this would have been addressed in the machine's specification before purchasing it.
Ideally, only the Process Safety Function would be implemented as shown in Figure 2.

4. Simply accept the equivalence of risk reduction for all types of safety functions

An even more pragmatic approach is accepting the equivalence of the risk reduction of all types of safety functions. E.g. accept that an IEC 61511 SIL3, an IEC 62061 SIL3 and an ISO 13849 PLe have a similar risk reduction.
The combination of different "fit for purpose" measures of risk reduction is a proven and successfully applied practice for companies in Process Industry. In order to achieve an appropriate risk reduction according to the ALARP (As Low As Reasonably Practicable) principle, different technical measures such as automated and mechanical safety as well as organizational measures are combined.
A common practice for the evaluation of combined means of risk reduction are the LOPA (Layer Of Protection Analysis) methodology and the so called Risk Reduction Factor.
Following this line of thoughts and the proven track record of successful practice, it seems valid to accept both, Process Safety and Machinery Safety measure to mitigate risks equivalently – among other possible solutions not using Functional Safety e.g. pressure relief valves.
The only open question is what risk reduction can be claimed for what measure. That claimed risk reduction should not differ depending on the application of the measure or the industry that it is used.
This approach is similar to IEC TS 63394 "Safety of machinery – Guidelines on functional safety of safety-related control system" and TRGS 725 "Hazardous explosive mixtures – measuring, control and regulation equipment as part of explosion protection measures".

Most companies of Process Industry define their own approach to risk mitigation. For example, to mitigate a risk of maximum one fatality per year cannot be excluded, mitigation measures IEC 61511 SIL2, IEC 62061 SIL2 and ISO 13849 PL_d are accepted.
Of course we cannot cherry-pick requirements for the safety function.
First of all, the safety function needs to be designed for the process – sensors and final elements must be feasible for the application. If a full safety function is designed according to a certain standard, also functional safety management including test procedures and intervals must follow that standard. E.g. one cannot build a safety function according to IEC 62061 SIL3 and ignore its (usually higher test frequency) and simply start with one proof test per year according to IEC 61511.
This means, if the equivalence of IEC 61511 and IEC 62061 and ISO 13849 functions is accepted, we still need to follow the corresponding management system including test procedures.

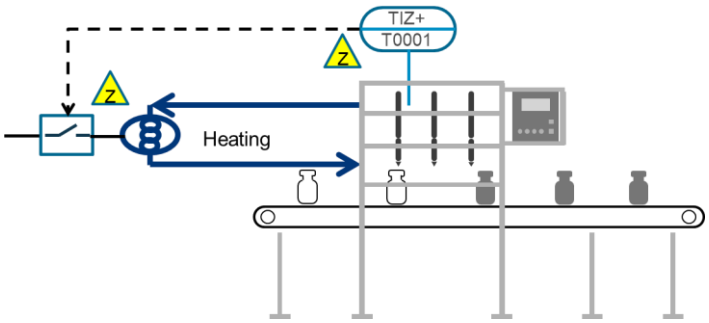

Figure 3: Machinery Safety Function to avoid overheating in a filling line

Looking back at the example from Figure 1, and assuming again that the target of the safety function is preventing the product from reaching its decomposition temperature, there are more possibilities to reach the target. Of course, a Safety Function according to IEC 61511 could be implemented. But assuming the manufacturer already covers the risk of overheating with a Machinery Safety Function, e.g. according to ISO 13849, that implementation can also be used for preventing the product from reaching its decomposition temperature as long as the risk reduction of that Safety Function fulfils the desired risk reduction from the HAZOP.
In that case, as shown in Figure 3, no additional Safety Function would need to be implemented.

5. Combination of Machinery Safety and Process Safety in one safety function

Dealing with new machines and new safety functions is rather the exception than the norm. People are facing brown field installations and therefore, could face the challenge of combining Machinery Safety and Process Safety applications.
The baseline of any attempt to combine the two management systems is to understand the requirements coming from each. They might be different to the target risk reduction. In addition, it must be clear that a redundancy requirement from one standard cannot be substituted by the probabilistic math of another standard. This works typically in the direction from the continuous or high demand mode application overruling the design rules towards the low demand mode requirements. The same is applicable for the exchange / overhaul frequency.
This section only deals with the integration of Machinery Safety (usually high demand) components into Process Safety functions (usually low demand mode).
A practical approach on how to implement safety functions that consist of Machinery Safety and Process Safety components is given in IEC TS 63394 - although this document focusses on implementing Process Safety components into Machinery Safety functions. The basic idea is to calculate the PFD or PFH margin of all components and their percental width of the corresponding SIL level:
For example, a IEC 61511 SIL2 sensor sub-system's partial PFD is $3x10^{-3}$, which corresponds to 30% of the SIL2 width, the IEC 61511 SIL2 logic's PFD is $1x10^{-3}$, which corresponds to 10% of the SIL2 width, the IEC 62061 PFH of the final element sub-system is $4x10^{7}$/h, which corresponds to 40% of the SIL 2 width – thus 30% + 10% + 40% = 80% of the SIL2 width are used, the whole safety function is SIL2 capable).

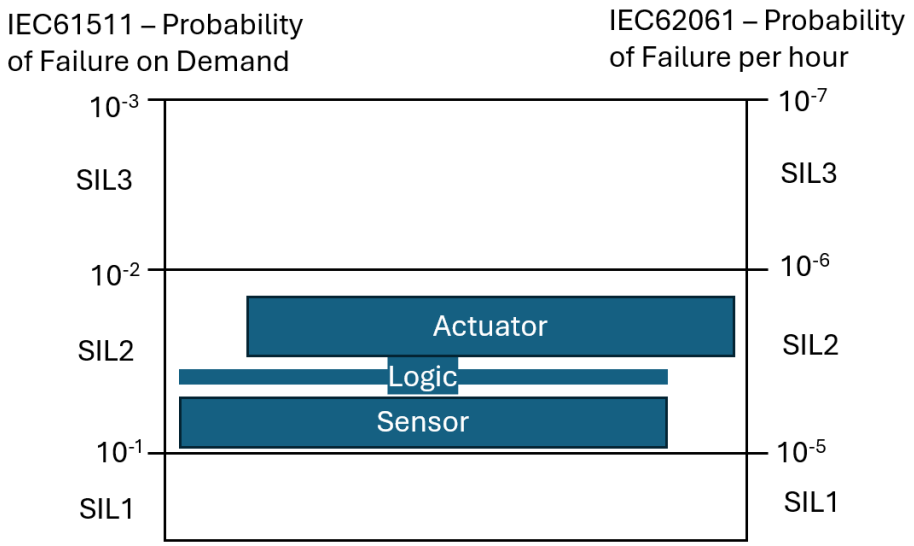

Figure 4: Machinery Safety Function to avoid overheating in a filling line

Although this is a quite feasible approach, for process industry and thus IEC61511 safety function an even easier way is proposed. Just do the IEC 61511 low demand PFD calculation e.g. according to IEC 61508-6 and take the PFH value of a machinery component as the failure rate for dangerous undetected failures: λ_{DU} = PFH. From an academic point of view, this may be not entirely correct. As a practical approach, this is feasible and is also generally supported by manufacturers.
Of course, it is necessary to stick to IEC 61511's requirements about hardware fault tolerance (HFT), if you want to build the corresponding sub-system according to IEC 61511. Components according to IEC 62061 or ISO 13849 can be assumed to follow a safety standard in their development and therefore fulfil according to NE 130 the requirements of prior use.
Following up on the example from Figure 2 and assuming the final element sub-system is designed with Machinery Safety components and already delivered as part of the filling machine and further assuming the sensor sub-system is Process Safety, a design similar to that in Figure 5 would be feasible. In that case, it would also not be necessary to replace already existing components from the machine.

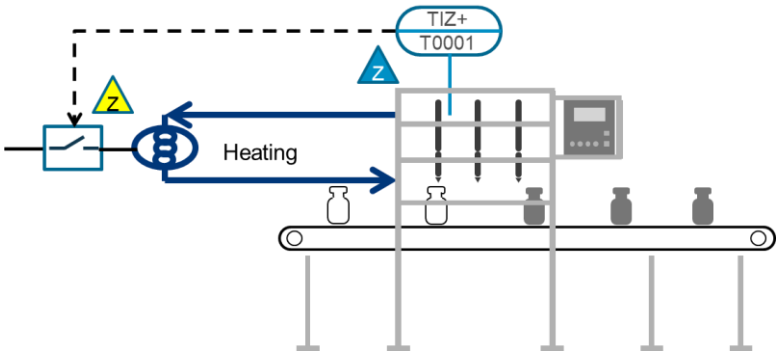

Figure 5: Combined Safety Function with Machinery Safety and Process Safety components to avoid overheating in a filling line

Depending on local rules and regulations, e.g. DIRECTIVE 2006/42/EC, additional assessments concerning the safety of the machine and or its declaration of conformity might be necessary. This will not be discussed as part of this paper.

6. Conclusion

Designing Safety Functions for Process Industry can be challenging when touching multiple standards for implementation. However, these easy practical hints give a solid basis for using Machinery Safety components within Process Safety Functions.

Deciding up front whether a Safety Function should be covered by Process Safety or Machinery Safety is generally a good advice – but let's face it: Process Safety reaches a machine after its installation and not during specification time.
The implementation of Machinery Safety components into Process Safety Functions is a practicable backup solution but horrible when it comes to maintenance. This is due to the different requirements regarding frequency and complexity of maintenance.
The most powerful approach is accepting the equivalence of the risk reduction of all Safety Functions – Process Safety and Machinery Safety. That also eases the tension in HAZOP discussions.
From the authors point of view, the latter approach is in line with the original intent of IEC 61508 of an "unified approach […] in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems".
This rational and consistent technical policy is relevant for actionable and cost-effective safety lifecycle management of automated safety in chemical operations due to the quite heterogenious and complex combination of assets in operation to date.
It can be argued that e.g. Safety 4.0, AI and digital transformation of industrial processes are only possible when being built upon a common ground of the originally adopted unified approach to functional safety especially regarding the integration or at least close alignment of Functional Safety approaches for Process Safety and Machinery Safety. This is due to the necessary holistic approach for digitally augmented services within the lifecycle that cannot be put into effective action when being applied in a heavily segmented field of application standards.
Due to the trends of modularization and flexible production increasingly incorporating "on-demand" reconfiguration of modular machine-process-arrangements, the same seems true for "Safety in relation to sustainability and resilience in process industry", "Safety of decarbonization and energy transition processes", and "Safety of new materials and technologies".
Finally, the Safety and security of chemical and energy infrastructures is even more depending upon a holistic approach due to the closely integrated and connected automation architecture.

References

Directive 2006/42/EC of the European Parliament and of the council of 17 May 2006 https://eur-lex.europa.eu/eli/dir/2006/42/oj

NE 130, 2023, "Selection of Field Devices for Safety Instrumented Systems Considering Operational Experience." NAMUR Recommendation.

IEC 61508-1,1998/COR1:1999, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

IEC 61508-6, 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6:2010)

IEC 61511-1, 2017, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, Ed. 2.1

IEC 61511-2, 2016, Functional safety – Safety instrumented systems for the process industry sector –Part 2: Guidelines for the application of IEC 61511-1: 2016

IEC 62061, 2021, Safety of machinery – Functional safety of safety-related control systems (IEC 62061:2021)

IEC TS 63394, 2023, Safety of machinery – Guidelines on functional safety of safety-related control system, 2023-2

ISO 13849, 2023, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design, Fourth edition, 2023-04

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC, https://eur-lex.europa.eu/eli/reg/2023/1230/oj

TRGS 725, 2023, Dangerous explosive mixtures – Measuring, control and regulating equipment in the context of explosion protection measures