Safety Management and Human Factors, Vol. 64, 2022, 125–134
https://doi.org/10.54941/ahfe1002637

Conducive Design for Safety in Modular Plants

Florian Pelzer[1,2], Anselm Klose[2,3], Jens R. Helmert[4], Leon Urbas[3], and Sebastian Pannasch[4]

[1]DFG RTG 2323 CD-CPPS, Germany
[2]Process-to-Order Lab, Germany
[3]Chair of Process Control Systems and Process System Engineering Group, Germany
[4]Chair of Engineering Psychology and Applied Cognitive Research, Technische Universität Dresden, 01069, Germany

ABSTRACT

The changeability of modular process plants implies the need for fundamentally new safety strategies: Since Operators must implement safety measures, assistance systems are needed to enable the operator to execute safety engineering tasks. We analyze the operator tasks during build up and re-configuration of flexible production systems in the process industry. Based on a state-of-the-art analysis of conventional safety engineering tasks, requirements to assist operators by a technical system are derived. We designed an assistance system and a module self-description to enable operators to implement the safety related interconnection of modules. To prove our concept, we successfully implemented the technical concepts in a demonstration plant. By implementing measures that are conducive to operators, we have been able to maintain their role as the most flexible resource in modular plants.

Keywords: Conducive design, Human operator, Functional safety orchestration, Modular process plant

INTRODUCTION

The chemical industry is facing new challenges resulting from volatile markets, increasing individualization of products, and shorter time-to-market (DECHEMA, 2016). By building changeable modular plants, chemical processes can be flexibly implemented and adapted to current market conditions (VDI 2776, 2020). For this purpose, pre-built modules, so called *Process Equipment Assemblies* (PEA), are interconnected to form a plant configuration. The vision of modularization strategies is to realize (re-)configuration of systems with minimal effort and reduced time. As the system becomes more flexible, work structures must also be designed accordingly. Operators are given new tasks and responsibilities, as they are expected to (re-)configure plants. This results in new challenging tasks for operators, such as plant construction or optimization (Müller and Urbas, 2017), which in conventional plants are performed by specialist trades. To address this, our research focuses on functional safety engineering. Existing safety approaches are highly demanding on qualifications and contradict the flexibility of modular plants (IEC 61511, 2016). To integrate operators, a paradigm shift must take place.

While technical concepts for implementing dynamically changeable safety systems in modular plants have already been developed (see Klose et al., 2020; Pelzer, Klose, et al., 2021), human factors have only been marginally considered. In this article we address the needs to enable the operators to perform safety engineering tasks during (re-)configuration. Therefore, we first investigate functional safety engineering from a human factors perspective and highlight challenges in modular process plants. We then analyze state-of-the-art approaches to implementing plant-wide safety systems at a task level and highlight the challenges faced by operators. From these findings, we derived requirements for conducive design measures that enable operators to overcome these challenges and perform reconfiguration. In accordance with the requirements, we proposed an assistance system as solution to support operators during safety engineering and successfully implemented it in a demonstration plant.

SAFETY ENGINEERING OF MODULAR PLANTS

Initial State: Conventional Safety-Engineering

In a chemical process plant, a product is produced by transforming substances based on physical, chemical, or biological processes with input or output of energy. To realize these processes, different devices (e.g., pumps or agitators) are interconnected via pipelines to realize process steps (e.g., conveying or mixing). This can result in risks to people and environment that must be controlled for safe operation. Therefore, these risks must be identified and reduced to a tolerable level by installing safety measures. These are planned by safety engineers, including the selection of safety-related sensors, logistic components, and actuators. The result is a so-called *Safety Instrumented Systems* (SIS), which technically realize *Safety Instrumented Functions* (SIF) to reduce risks. (IEC 61511, 2016).

Safety engineering of conventional process plants is following the basic assumption, that plant behavior and environment are completely predictable. Appropriate safety measures tailored to the application situation are installed. Accordingly, a conventional process plant is limited in its flexibility to very few preconceived application scenarios. Changes can be implemented by remodeling the SIS following a multi-staged safety lifecycle executed or supervised by safety engineers (IEC 61511, 2016). Each change in the plant configuration, for example caused by an exchange or adaptation of a module, must be evaluated in terms of safety (IEC 61511, 2016), a time-consuming process which contradicts the plant's flexibility (Klose et al., 2020). To balance plant safety and flexibility, new methods to plan and install SIS in modular plants are necessary (Pelzer, Pannasch, et al., 2021).

Safety Engineering in Modular Plants and Engineering Tasks

Modular process plants shall be easily changeable by (re-)configuring modules to build any sequence of process steps (VDI 2776, 2020). Pre-planning every configuration is practically impossible, as the flexibility feature of modular plants results in literally infinite possibilities (Trapp et al., 2013).

This issue is addressed by redistribution of engineering tasks: The rationale for functional safety in modular plants is to outsource safety engineering tasks to module manufacturers to reduce the workload during plant safety engineering (Pelzer, Klose, Drath, et al., 2020). This leads to a two-level safety consideration:

- *Intramodular Safety Level*: Intramodular safety deals with managing risks of the modules. In previous work, we were able to show that the implementation of SIS on a module is suitable for managing all risks from stand-alone operation (Pelzer, Klose, et al., 2021).
- *Intermodular Safety Level*: Intermodal safety deals with the management of risks arising from the interconnection of modules. As if he had foreseen already back in his days, Aristotle stated 350 BC: “The whole is more than the sum of its parts”, which applies for safety in modular plants as well. Intramodular safety measures are not sufficient to ensure plant safety without additional measures (Pelzer, Klose, Barth et al. 2020).

The intramodular safety is pre-designed by the module manufacturer and thus does not cause any effort during the (re-)configuration of a plant. Intermodular safety engineering generates efforts. Therefore, the bottleneck for timesaving in safety engineering lies within the intermodular safety engineering. To maintain flexibility, the conventional engineering approach of plant-wide safety measures is adapted to the characteristics of a modular plant (Klose, Pelzer, et al., 2021). Once the process has been designed and suitable modules were selected, the engineering tasks can be clustered into three sequential stages (according to Pelzer, Pannasch, et al., 2021):

(1) *Safety Configuration Engineering*: Hazards and risks resulting from the plant configuration and the desired process must be identified in a plant-wide safety analysis. Risk management must be based on already implemented intramodular safety measures of the modules. The output of this phase is a so-called *Safety Requirement Specification* that defines the implementation of safety measures, including the linkage of intramodular SIFs to mitigate intermodular risks.

(2) *Functional Safety Orchestration*: Next, an intermodular SIS must be set up following the specifications stated in the first engineering phase. Therefore, intramodular safety capabilities of modules are interconnected. The plant wide safety system engineering the so-called *Functional Safety Orchestration* (FSO), is resulting in a safety configuration. Following the intermodular safety concepts of the authors (Pelzer, Klose, Drath, et al., 2020), the safety configuration is executed on a superordinate safety system. To fulfill the requirements of flexibility and reliability according to (IEC 61511, 2016) the safety configuration from (1) must be implemented on a Safety *Programmable Logic Controllers* (Safety-PLC) and translated into Safety-PLC code.

(3) *Physical Configuration Implementation:* The interconnection of the distributed SISs must be physically integrated in the plant (Pelzer, Klose, et al., 2021).

CONDUCIVE DESIGN OF SAFETY ENGINEERING

Conducive Design and Allocation of Engineering Tasks

Conducive Design places operator capabilities at the center of system design. It is assumed that the operator's capability profile is dynamic. Therefore, systems should be designed to challenge and promote the operator's capabilities while avoiding skill atrophy or overload. As operators are the most flexible part in the safety engineering process of a modular plant, we aim to integrate their flexible capabilities with a conducive design of arising tasks. (Ziegler and Urbas, 2015; Romero et al., 2016)

The safety engineering tasks for which a system operator is responsible in modular plants is not yet clearly defined. Depending on the time constraints of the (re-)configuration as well as the demand on the changeability of the system, the three mentioned safety engineering clusters (1-3) must be processed ad-hoc. For maximum system flexibility in plant (re-)configuration, i.e., adaptation and replacement of modules in response to (sudden) changes in production conditions, as proposed in (Müller and Urbas, 2017), the operator should perform safety engineering holistically. However, to address system flexibility we conclude that the safety engineering process must become faster. Even though the qualifications of operators are not precisely defined (see discussion Romero et al., 2016; Taylor et al., 2020). We see operators as plant (re-)configurators according to Müller and Urbas, 2017 with the competency profile as chemical worker according to the german training regulations (BGBl. I 19, 2005). Operators are trained in basic chemical, electrical, and control work procedures, but not in safety-related tasks. Due to high level of complexity and responsibility, this requires a high level of qualification (e.g. 8 years of specialized training to become a SIS Safety Engineer; (TÜV, 2021)). Therefore, the aim of the conducive design measures is to enable operators to master safety engineering by breaking down task complexity.

Looking at the safety engineering tasks in modular process plants, the *Safety Configuration Engineering* as well as the Physical Reconfiguration Implementation are already addressed by prototypical conducive design concepts (Klose, Kessler et al., 2021; Pelzer, Klose, et al., 2021). However, the FSO is only considered from a technical point of view in without respecting human factors. Therefore, our research focuses on the elaboration of this area.

Research Approach and Methods

As we demonstrated in previous work (Pelzer, Klose, Barth, et al., 2020) the starting point for realizing functional safety in a modular plant is to analyze conventional plant safety engineering methods and adapt them to the boundary conditions of modular plants. Therefore, our research procedure was twofold.

In the first step, we analyzed the state-of-the-art methods and tasks for FSO from a human factor's perspective. To examine the conventional approaches in the work domain of modular plants, we applied them in a demonstration plant (see Pelzer, Klose, et al., 2021) supervised by safety experts.

We characterize the identified tasks in terms of their complexity by applying the criteria of (Dörner and Funke, 2017). To determine the challenges faced by operators, we compared their skills profile to the complexity of the task. The result of the first step is a characterization of the conventional methods and an identification of challenges for operators.

In the second step, we conducted a feasibility analysis to find out how to reduce the level of complexity. To this end, we propose a prototype solution: We followed the human-centered software development approach of (Leuchter and Urbas, 2004) and considered operator tasks and capabilities to develop a FSO assistance environment. To prove the concepts, we implemented and tested them in the same demonstration system we already used for task recognition.

Step one: State-of-the-Art Analysis

To implement the intermodular safety measures, relevant sensors and actuators must be interconnected on an intermodular Safety-PLC by programming them according to the safety configuration (Pelzer, Klose, Drath, et al., 2020). Therefore, Safety-PLC programming tools and languages applied in conventional plant safety engineering must be used to interconnect safety signals of modules to intermodular SIFs. According to the criteria stated in (Dörner and Funke, 2017) this is considered as a complex design task: First, each intramodular safety signal needed for intermodular risk management must be individually allocated and initialized in the intermodular Safety-PLC program. Second, the intermodular SIFs must be implemented by interconnecting the safety signals (e.g., a temperature sensor and a cooling fluid valve) of the modules. Depending on the intermodular SIF, logical elements, such as threshold comparators, must be added to compute the resulting safety signals. Finally, threshold values for the intermodular SIF must be initialized with suitable values from the safety configuration. This must be done for each connection of safety signals, respecting their interdependencies. The possibilities of solutions of the safety configuration are manifold and stem from the preferences of the programmer.

When analyzing these tasks, it becomes clear that the demands on operators are high. Multiple cross-linked safety signals must be interconnected while meeting several, possibly conflicting, goals of plant flexibility and safety. The programming must be performed using sophisticated programming languages (derived from Molina et al., 2007) while respecting strict programming guidelines and standards (Kanamaru et al., 2007). At the same time, programming errors result in risks, so the cost of errors can be high (IEC 61511, 2016). That is why in conventional plants, only specific Safety-PLC engineers with further training in PLC programming are allowed to change program code (Kanamaru et al., 2007).

In conventional process plants, configurations and processes are not subject to frequent changes during the system's lifetime. Changes can be scheduled in advance so that availability of specialists and time for realizing the changes in the Safety-PLC is given. In modular plants there is a need for action since systems are frequently reconfigured and therefore the Safety-PLC programming must be adapted. Modular plants only really show their advantages when they are quickly and consistently adapted and changed according to current economic requirements. To enable operators by further training as Safety-PLC programmers would only address the lack of qualification but leaves them with the time constraints. Following this argumentation, the implementation of safety configuration must be reduced regarding efforts as well as task complexity to design it conducive to systems changeability (Ziegler and Urbas, 2015). To do so, we derived the following requirements: Matching tasks to the operator's competency profile by avoiding specific Safety-PLC programming knowledge and reducing task complexity.

Step two: Safety Module Interface and FSO Assistance System as Conducive Design Solution

As shown in the state-of-the-art, the operator cannot perform the programming of the safety PLC. Continuing this line of reasoning with respect to the operator's role as (re-)configurator, this task must be eliminated. Various strategies and technical solutions can be pursued, such as the use of artificial intelligence. However, keeping operators out of the loop of FSO may result in negative effects on operator performance and trust in the system (Parasuraman and Manzey, 2010). Instead, we motivate the development of conducive design measures that enable operators to perform the FSO. To prove the successful integration of the operators in the process of the FSO, we propose a technical solution below.

To meet the previously formulated requirements, our approach is to reduce FSO tasks to decision-making processes, to support these decision-making processes, and to avoid tasks that require extensive qualification in safety engineering. The concept we are pursuing is to limit the solution space for FSO and to eliminate the need for manual programming of the Safety-PLC. This approach is related to the principle of "low-code programming", a computer-aided software engineering approach that originated in app development. It elevates manual programming to an abstract level to allow people without extensive programming skills to create software products. The resulting product is (1) built by pre-configured functionalities which are (2) provided through an assistance system. The user's task is to link the individual functionalities to meet the (3) product specification (Sanchis et al., 2020).

Merging the low-code approach to the implementation of safety systems in modular plants looks like this: (1) pre-configured functionalities are provided by modules in the form of safety capabilities. (2) These capabilities are integrated on a platform, the FSO assistance system, which supports operators to interconnect of the capabilities. (3) The sum of all connections builds the safety plant configuration.

Now to the implementation of the FSO assistance system and the resulting tasks of operators (user's task flow, although shown in Figure 1): The (1) safety capabilities of modules must be integrated into the (2) FSO assistance system. To address this issue, we have developed a digital representation of the module's safety system, which is provided through an interface. The

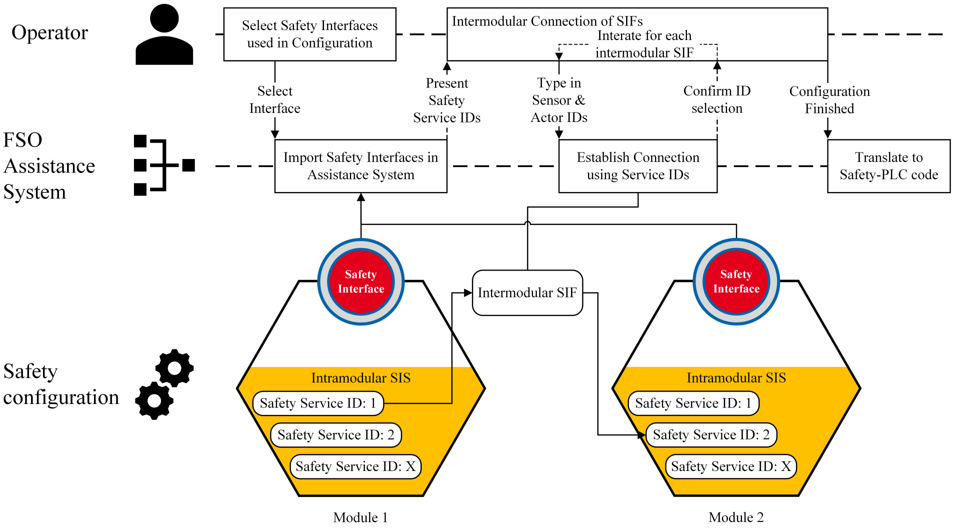

Figure 1: Tasks during FSO with assistance system with two modules.

integration of the interface into the FSO assistance system allows access to the safety capabilities. We encapsulate these capabilities in *Safety-Services* to avoid signal-based data exchange according to the low-code programming concept. Each *Safety-Service* has an *identification number* (ID) through which it is accessible for intermodular connection. For example, the signal of a temperature sensor can be accessed via ID "3" on the FSO assistance system. In the (2) FSO assistance system, the user is presented with the IDs and the short description of the individual Safety-Services available in the plant configuration. Intermodular SIFs are implemented by mapping the IDs of Safety-Services to each other. In our prototypical implementation this is done by entering the ID numbers of the intermodular SIF into a text field. Extensive logic is not needed since the complexity, e.g., thresholds, is already encapsulated in the Safety-Services of the modules. The entirety of the interconnected Safety-Services then forms the safe plant configuration.

This concept shifts the complexity of Safety-PLC programming to the module manufacturers, as they must program the Safety-Services. Safety-Services can be interconnected without manual Safety-PLC programming. Part of the back-end functionalities of the FSO assistance system, i.e., the functionalities that are not visible to the user, are the translation of the user's Safety-Service assignment into Safety-PLC code.

Discussion of the Results

The FSO assistance system as well as the safety interface were iteratively developed, implemented, and tested on a demonstration plant. By comparing the conventional Safety-PLC programming methods and the assisted FSO, a significant reduction in task complexity was found. The FSO is reduced to decision-making about which IDs need to be connected. The process to implement the safety configuration can therefore be reduced to 2+n interactions of operator and FSO assistance system (with n the number of intermodular SIFs resulting from the safety configuration). By this means, the implementation of the safety configuration could be transferred from a "know-how" task of Safety-PLC programming to a "know-what" task of module interconnection. Therefore, the operators can contribute to FSO with their characteristics as enabler of flexibility (Romero et al. 2016), while their "weakness" of not being a universal genius is managed. However, directly influencing safety systems remains a demanding task to perform, particularly in terms of conscientiousness and correctness.

The development of the FSO has been driven by the demonstration that operators can be integrated into the process. Therefore, the focus was on the technical implementation without considering the usability of the FSO assistance system. The execution of the FSO prototype is completely text-based and is done by entering commands in a control field (comparable to the Command Prompt). The development of a user interface could further improve the usability and accessibility of tasks. Evidence of the conduciveness of measures taken for the operator is limited, as the system has only been tested by engineers in a laboratory. Statements about the execution of the FSO by operators can therefore not be made. A comparative study with operators performing safety engineering using conventional and assisted methods should be conducted to gain practical insights into the efficiency of measures taken and manageability of FSO. In this context, special attention should be paid to possible human errors and the development of appropriate avoidance measures.

The modularization goes hand in hand with higher demands on the safety related automation of the PEAs (Pelzer, Klose, Barth, et al., 2020) as well as the competence profiles of the operators (Romero et al., 2016). Developing the FSO is like crossing swords on a scientific level: Following the Dynamic Safety Model of Rasmussen 1997, the constraints of costly failures, high workload, and changing safety configurations of modular plants fight against each other. Therefore, the rapid increase in the complexity of operator tasks, coupled with the tightening of time constraints and the high demands placed on safe execution, makes it essential to support safety-related (re-)configuration tasks.

CONCLUSION

Our research has analyzed the need for assistance in the development of safety systems in modular process plants. Our results revealed that operators will not be able to fulfill all requirements. Therefore, a safety-related assistance system was implemented, that allows operators to (re)configure the safety logic. Based on conducive design requirements derived from the analysis of conventional safety engineering tasks, a technical solution was developed. Using this approach, the complex task of intermodular safety engineering was reduced to the linking of IDs of pre-implemented safety functions, which are provided from an interface. This is shifting efforts to an earlier phase, the Safety-Configuration-Engineering, which can be done experts in advance. In further research, we will provide empirical evidence of the effectiveness of the FSO assistance system by conducting a study with operators.

ACKNOWLEDGMENT

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 319919706/RTG2323. The Authors further thank the TaskForce "Safety-MTP" and the P2O-Lab for support during practical implementation.

REFERENCES

BGBl. I 19 (2005). Verordnung über die Berufsausbildung zur Produktionsfachkraft Chemie. pp. 906–912.

DECHEMA e.V. (2016). Modular Plants. Flexible chemical production by modularization and standardization - status quo and future trends.

Dörner, D. and Funke, J. (2017). Complex Problem Solving: What It Is and What It Is Not. *Frontiers in Psychology*, 8:1153

IEC 61511. (2016). Functional safety – Safety instrumented systems for the process industry sector. www.vde-verlag.de

Kanamaru, H., Mogi, T., and Aoyama, N. (2007). Functional safety application using safety PLC. *SICE Annual Conference*, pp. 2489–2492.

Klose, A., Pelzer, F,..., Urbas, L. (2021). Building Blocks for Flexible Functional Safety in Discrete Manufacturing and Process Industries. *26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vasteras, Sweden

Klose, A., Kessler, F.,...,Urbas, L. (2021). Representing Causal Structures in HAZOP Studies. *26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vasteras, Sweden.

Klose, A., Pelzer, F.,..., Urbas, L. (2020). Distributed Functional Safety for Modular Process Plants. *25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1381–1384.

Leuchter, S., and Urbas, L. (2004). Integrierter agiler Entwicklungsprozess für softwareintensive Mensch-Maschine-Systeme. In: C. Steffens, M. Thüring and L. Urbas (Eds). *Entwerfen Und Gestalten. 5. Berliner Werkstatt Mensch-Maschine-Systeme*, pp. 53–68.

Molina, F. J., Barbancho, J., Leon, C., Molina, A., and Gomez, A. (2007). Using industrial standards on PLC programming learning. *Mediterranean Conference on Control and Automation*, pp. 1–6.

Müller, R., and Urbas, L. (2017). Cognitive Challenges of Changeability: Multi-Level Flexibility for Operating a Modular Chemical Plant. *Chemie Ingenieur Technik*, 89(11), pp. 1409–1420.

Parasuraman, R., and Manzey, D. H. (2010). Complacency and Bias in Human Use of Automation: An Attentional Integration. Human Factors: *The Journal of the Human Factors and Ergonomics Society*, 52(3), pp. 381–410.

Pelzer, F., Klose, A.,..., Urbas, L. (2020). Intermodular functional safety for flexible plants in process industries – Part 1: State of the art and general requirements. *atp magazin*, 62(06–07), pp. 84–92.

Pelzer, F., Klose, A.,..., Urbas, L. (2020). Intermodular functional safety for flexible plants in process industries – Part 2: Approach to intermodular safety architecture and engineering, Introduction of the Safety-MTP. *atp magazin*, 62(10), pp. 44–53.

Pelzer, F., Klose,…, Urbas, L. (2021). Safety in Modular Process Plants: Demonstration of Safety Concepts. *E&I Elektrotechnik und Informationstechnik*, 138(7).

Pelzer, F., Pannasch, S. and Urbas, L. (2021). Evaluation of Safety Life Cycle Models in Modular Automation. *Chemie Ingenieur Technik*.

Rasmussen, J. (1997) Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, 27, pp. 183–213

Romero, D., Bernus, P., …, Fast-Berglund, Å. (2016). The Operator 4.0: Human Cyber-Physical Systems & Adaptive Automation Towards Human-Automation Symbiosis Work Systems. *IFIP Advances in Information and Communication Technology*. Cham, Germany. pp. 677–686

Sanchis, R., García-Perales, Ó., Fraile, F., and Poler, R. (2020). Low-Code as Enabler of Digital Transformation in Manufacturing Industry. *Applied Sciences*, 10(1)

Taylor, M. P., Boxall, P.,…, Adeniji, A. (2020). Operator 4.0 or Maker 1.0? Exploring the implications of Industrie 4.0 for innovation, safety and quality of work in small economies and enterprises. *Computers and Industrial Engineering*, 139

Trapp, M., Schneider, D., Liggesmeyer, P. (2013). A Safety Roadmap to Cyber-Physical Systems. In J. Münch and K. Schmid (Eds.), *Perspectives on the Future of Software Engineering*. Springer. pp. 81–94

TÜV (2021). FS Engineer. https://www.tuv.com

VDI 2776 (2020). Process engineering plants of modular plants. www.vdi.de

Ziegler, J. and Urbas, L. (2015). Förderliches Gestalten komplexer Mensch-Maschine-Systeme. In: GfA e.V., ed. *Arbeitswissenschaft. Mit Interdisziplinarität und Methodenvielfalt*. Dortmund: GfA-Press.