ORIGINALARBEIT Elektrotechnik & Informationstechnik (2021) 138/7: 462–468. https://doi.org/10.1007/s00502-021-00928-8

Safety in modular process plants: demonstration of safety concepts

F. Pelzer, A. Klose, J. Miesner, M. Schmauder, L. Urbas

The modularization of process plants addresses the need for flexible production options in the process industry. In order to maintain the advantages of the adaptability of modular plants, an adaptation of established engineering methods and procedures to their dynamic context of use is required. This paper describes the development and the features of a demonstrator, which makes it possible to investigate aspects of modular plant topology, the design of modular process units, and the functional safety of modules and plants. During the engineering of the modules, modular planning principles are applied and evaluated with respect to the requirements for functional safety and with a strong focus on the modification of safety systems through the exchange of PEAs and FEAs. For the design and modification of the safety systems, a safety life cycle, which meets the requirements of modular automation and takes the provisions of IEC 61508 and IEC 61511 into account, is applied. Practical insights into the construction and the implementation of the distributed Safety Instrumented System as well as the Basic Process Control System are described. In addition to the validation of safety concepts related to the interconnection of Safety Instrumented Functions, the demonstrator is used to study human working environments in modular plants.

Keywords: functional safety; functional safety orchestration; modular process plant; process-to-order

Sicherheit in modularen Prozessanlagen: Demonstration von Sicherheitskonzepten.

Durch die Modularisierung von Prozessanlagen wird der Bedarf nach flexiblen Produktionsmöglichkeiten in der Prozessindustrie adressiert. Sofern die Vorteile der Anpassbarkeit der modularen Anlagen erhalten bleiben sollen, ist eine Anpassung etablierter Engineering-Methoden und -Vorgehensweisen an deren dynamischen Nutzungskontext unausweichlich. Dieser Beitrag beschreibt die Entwicklung und Umsetzung eines Demonstrators, in dem die Aspekte modularer Anlagentopologien, die Auslegung von modularen Prozesseinheiten sowie die funktionale Sicherheit von Modulen und Anlagen abgebildet werden. Beim Engineering der Module werden modulare Planungsprinzipien angewandt und hinsichtlich der Anforderungen aus der funktionalen Sicherheit bewertet. Im Fokus der Betrachtung steht die Modifikation von Sicherheitssystemen durch den Austausch von Funktionseinheiten innerhalb eines Prozessmoduls sowie den Austausch eines Prozessmoduls an sich. Für Entwurf und Modifikation der Sicherheitssysteme wird ein auf die Anforderungen der modularen Automation abgestimmter Sicherheitslebenszyklus angewandt, der die Vorgaben nach IEC 61508 und IEC 61511 berücksichtigt. Es werden praktische Einblicke in den Aufbau und die Implementierung von verteilten PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen beschrieben. Neben der Validierung von Sicherheitskonzepten in Zusammenhang mit der Verschaltung von PLT-Sicherheitsfunktionen wird der Demonstrator zur Untersuchung der menschlichen Arbeitsumgebung in modularen Anlagen eingesetzt.

Schlüsselwörter: funktionale Sicherheit; Functional Safety Orchestration; modulare Prozessanlage; Process-to-Order

Received June 11, 2021, accepted August 9, 2021, published online September 17, 2021

1. Introduction

1.1 Motivation

The modularization of process plants addresses the need for flexible production options in the process industry [1, 2]. The use and networking of distributed systems, which are largely self-sufficient in terms of automation and safety, is a key aspect of achieving the goal of flexible production. This requires the implementation of safety concepts without counteracting the dynamic characteristics of modular plants. To address this research area, newly developed concepts and engineering strategies for functional safety in modular plants have been developed [3, 4]. This research is currently based on a mostly theoretical framework that fills gaps which have been identified for instance in the ORCA project [5].

In order to test and validate the approaches in a practical field of application, a demonstrator which considers modular planning [6–8] as well as the integration of Safety Instrumented Systems is needed [3, 4]. The *demonstrator for modular functional safety* is therefore designed according to the design principles of VDI 2776, where regulations and guidelines are sorted for the application of modular process plants. Specifically, four hierarchical levels of modular plants are defined [1], see Fig. 1:

(1) *Components* (COMPs) form the field level of modular plants and embody the smallest, not separable unit.

(2) *Functional equipment assemblies* (FEAs) consist of components. A FEA forms a process engineering function (e.g. heating).

Pelzer, Florian, DFG Research Training Group 2323 CD-CPPS, Technische Universität Dresden, Georg-Schumann-Straße 7a, 01069 Dresden, Germany (E-mail: florian.pelzer1@tu-dresden.de); **Klose, Anselm,** Process-To-Order-Lab, Technische Universität Dresden, Dresden, Germany; **Miesner, Jonas,** DFG Research Training Group 2323 CD-CPPS, Technische Universität Dresden, Dresden, Germany; **Schmauder, Martin,** Chair of Labour Engineering, Technische Universität Dresden, Dresden, Germany; **Urbas, Leon,** Chair of Process Control Systems & Process System Engineering Group, Technische Universität Dresden, Dresden, Germany

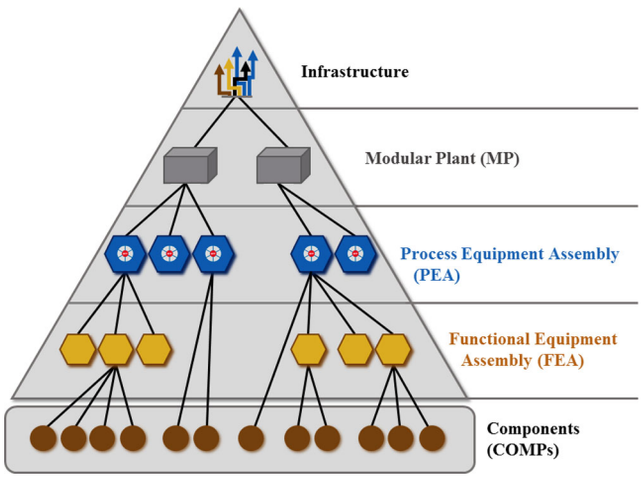


Fig. 1. Infrastructure of modular process plants, adapted [1]

(3) *Process equipment assemblies* (PEAs) form a procedural step (e.g. distillation) and consist of at least one FEA. The PEA has its own automation, which enables the execution of all necessary functions for decentralized operation. Those functions are called *Services*. The characteristic feature of a PEA is the standardized manufacturer-independent interface, the *Modul Type Package* (MTP) [9]. The MTP describes the data which can be exchanged between PEA and higher levels of automation.

(4) *Modular Plant* (MP) form the top level of the hierarchy and consist of at least one PEA. To realize a complex process, PEAs are interconnected on a superior automation layer, called *Process Orchestration Layer* (POL). The sequencing of Services within the POL is referred to as orchestration and enabled by the MTP [10].

To achieve the mentioned goal of dynamic process implementation, process plants can be realized by combining PEAs and integrating their functionality into the POL. This requires pre-engineered, fully automated PEAs. Doing so, a time reduction of 50% [11] or even more can be achieved during plant engineering. Therefore, resulting from the hierarchical structure of the VDI 2776-1, the adaption of a modular plant is realized in two different ways, which can be executed on two different levels: The most common way is the adaption of the plant topology through the exchange of PEAs—intermodular level. Additionally, the operating range of PEAs can be adapted through the exchange of FEAs—intramodular level [1]. In this case, modifications should only be carried out within the foreseen scope of the PEA manufacturer, to maintain the conformity of the equipment.

This layered architecture provides, together with the modular safety orchestration framework [3] the foundation of the *demonstrator for functional safety*, which is being constructed and assembled within the *Process-To-Order Lab* (P2O-Lab)[1] at Technical University Dresden, a research institution that addresses the description, interconnection and usage of information and equipment in a practical manner.

The remainder of the article is structured as follows: In the first Section, the fundamentals that are relevant to the design of the demonstrator are presented. Section 2 focuses on the technical realization and describes the design decisions. In the last section 3, further key findings are presented and placed into the context of the general research questions.

[1] https://tu-dresden.de/ing/forschung/bereichs-labs/P2O-Lab.

1.2 Functional safety in modular plants

For the commercial operation of modular plants, the same principle applies as for conventional plants: plant operation is not permitted without meeting necessary safety requirements [12, 13]. According to the protection level model [12], part of the overall safety in a MP, can be realized by process control technology. The technical implementation of functional safety measures is carried out by *Safety Instrumented Systems* (SIS), which consist of sensors, logic and actuators. These SIS perform *Safety Instrumented Functions* (SIFs) to control safety-relevant parameter, such as a critical level monitoring in a vessel. The adaptability of SIS to different applications makes it attractive for use in modular plants [14, 15]. For example, the critical level limits of the vessel can be adjusted depending on the hazard potential of the medium present in the process. Depending on the requirements situation, the limit values of a SIF can be adjusted accordingly to ensure process safety.

When thinking of implementing a new process in a modular plant, PEAs are selected for the main process steps [16, 17]. With the basic plant topology, additional PEAs which support the process or the previously selected PEAs can be selected. Looking at the safety of the system, risks can be differentiated between intra- and intermodular [18, 19]. The intramodular perspective considers all risks that occur and can be managed within a PEA. For a process, a PEA with suitable safeguards needs to be selected. If the safety measures do not fit to the requirements, it has to be considered an "*adapt or exchange*"-decision on either the process, the plant or the PEAs [4]. This means, the process could replace with a less dangerous one [20], the plant topology could be changed by choosing different PEAs and their combination, or the PEAs could be modified by changing the FEAs.

Additional intermodular safety measures could be implemented, thus increasing the choice of suitability PEAs. Intermodular safety realizes the combination of intramodular safety functions to further decrease the risks in the plant. This could be done by using SIS's inside of the PEAs. By integrating intramodular SIS's in a superior safety related orchestration (*Functional Safety Orchestration*, FSO), safety-related interconnection of PEAs can be performed according to the principles of POL: PEAs offer their safety functionalities to a *functional Safety Orchestration Layer* (fSOL) where they are interconnected [3]. A triggered safety function in one PEA can then be transferred to other PEAs, which can react accordingly. To ensure the compatibility of the intramodular SISs and the fSOL, standardized description and aligned engineering procedures should be used [15]. For this purpose, two harmonized procedure models for the functional safety of PEAs and modular plants were described in the form of *Safety-Life Cycles* (SLC) in [4].

Previous research in modular engineering in process engineering focused for instance on the predecessor to the PEA, the package-units or similar skids. The limiting feature of the package-unit is the manual, non-automated integration into a higher-level control system. The VDI 2776 [1] and VDI VDE NAMUR 2658 [9] were the first standards to introduce a vendor independent combined concept of modular automation and modular process engineering in the process industries. Recent demonstrators as described in Bittorf et al. [21] focus on the automation and interfaces (MTP, Services and POLs) of PEAs. However, functional safety of modular process plants especially with consideration of adapt and exchange scenarios of PEAs are not mentioned yet specifically.

2. Technical concept and realization of the demonstrator

2.1 Safety demonstrator research questions

The objective of the demonstrator is to validate concepts for functional safety in modular plants and gain practical insights, taking

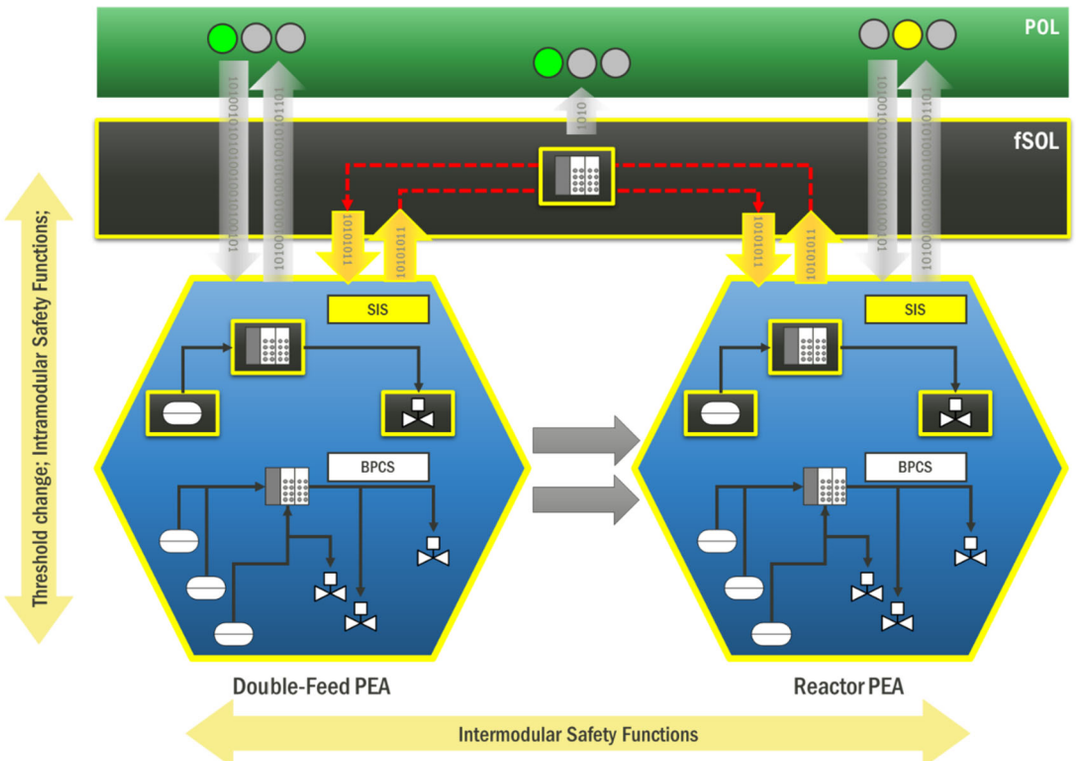


Fig. 2. Schematic representation of the demonstrator, modified [3]

the adaptability and interchangeability of PEAs into account. In this context, the following research questions will be investigated:

- How can intra- and intermodular safety systems be technically implemented without cutting the flexibility of a modular plant?
- Are the concepts of safety lifecycles feasible in practice?
- What activities are to be performed during the disassembly, assembly or adaptation of a PEA? What skills and competencies does a person or operator need to perform these activities?

In order to answer these research questions, a number of requirements for the characteristics of a demonstrator arise. To take the aspects of a modular system and flexible modification of safety systems into account, the demonstrator should respect the structure of VDI 2776-1 (Fig. 1) and consist of more then one PEA, which in turn contain FEAs. To investigate functional safety, the PEAs should each have an intramodular SIS which can be connected to the fSOL via a communication interface (Fig. 2). Both the design of the PEAs and the plant should follow the respective safety life cycles to investigate their applicability [4]. For the purpose of considering ready to use technology and practical investigation, safety-certified sensors, logics and actuators should be used.

2.2 Demonstrator concept

Following the previously formulated research questions and the resulting requirements, a demonstrator, which consists of two PEAs, each with its individual SIS and *Basic Process Control System* (BPCS), was built. The BPCS enables the execution of the operational functions of the PEAs and also ensures the foreseen request rate of the SIF. Inspired by a petrochemical polymerization process where media is dosed in a critical mixing ratio, and by the description of the Stirred Tank Unit described by the BioPhorum group [22], a feed PEA and a reactor PEA were designed (see Fig. 2).

The first PEA, the double-feed-PEA, consists of two identical units with separate vessels, actuators and instrumentation. The equipment and instrumentation for the dosing of the media is designed as FEA, to be easily adjustable to different media. The encapsulation of two streams in one PEA is used to realize a dependent flow ratio of the two streams. Therefore, the individual dosing processes are monitored and set to a specific ratio range with a SIF. Additionally, an overpressure protection of the pumps with a return flow channel is implemented. The two vessels can also be seen as a buffer; both fill-levels of the tanks are continuously monitored to avoid dry running and overfilling. From the double-feed-PEA the two media streams can be transferred to the reactor-PEA consisting of a reaction-vessel with stirrer and heating rods, as well as an additional FEA for dosing the product. The functions of this PEA include the mixing of the two media, tempering, monitoring of the fill level and controlled dosing to avoid dry running. The overpressure protection of the dosing stream is not realized, however, the required fittings are installed for a potential expansion of the FEA.

Both PEAs provide their mentioned intramodular safety functions to the fSOL (Fig. 2: vertical arrow on the left). The SIFs of the PEAs can then be interconnected to control intermodular risks (Fig. 2: horizontal arrow on the bottom), e.g. to prevent overfilling by communicating the level of the reactor to the dosing PEA. In addition, the SIS can be adapted to process and plant requirements by adapting the switching limits of various SIFs, e.g. the level of the vessel or the maximum pressure of the pump. Specifically, this adjustment can be used to limit the rate at the outlet of the double-feed-PEA in combination with the maximum level in the reactor-PEA, limit the amount of hazardous substances. Being completely separated from each other, the SIFs of the PEAs need to be coordinated by the superior control, the fSOL.

Fig. 3. The double-feed-PEA with view of control cabinet (left) and with view of the vessels (right)

2.3 Demonstrator realization

The double-feed-PEA (Fig. 3) and the reactor-PEA (Fig. 4) were technically implemented following the conceptual description of the previous section. Both PEAs are constructed following the same basic principle: The frame consists of metal system profiles to which the FEA and components are attached. Castors are mounted under the frames to facilitate the mobility of the PEA. To simplify installation and removal and to take ergonomic aspects while FEA-exchange into account, the Feed-FEAs are mounted on rollers as an insert (Fig. 4). Accordingly, the FEAs which have a weight of 70 kg do not have to be lifted for exchange. These measures were taken to design the modification of the plant topology and the modification of the PEA configuration in such a way that the flexible plant adjustment and ergonomic load handling can be realised.

Each PEA has a control cabinet where the logic elements of the SIS and the BPCS are placed and electrical as well as pneumatic energies are distributed. The design of the control cabinet is influenced by the dynamic characteristics of each FEA: To ensure safe plugging and unplugging of FEAs within a PEA-SIS, the installed sensors and actuators must be includable in a flexible and at the same time fail-safe manner. Wiring the sensors directly to the PEA control cabinet is out of the question due to the effort involved for exchanging the FEAs and the potential for (human) errors [23]. For this reason, we have installed a small control cabinet on the FEAs in which all electrical and pneumatic FEA signals are collected. In this cabinet, the signals are connected to a plug with reverse polarity protection, via which the signals can then be passed on to the PEA control cabinet. To process the signals correctly in the PEA level, the pin assignment in the connector must be complementary to each other in the PEA and FEA levels. Therefore, different FEA variations with different (safety-related) sensors have to be considered and corresponding pins have to be provided. Following this, the FEAs in this case are mostly proprietary, since the connector type, the pin assignment, and the safety-related operating approval of PEA and FEA must match.

In order to consider the state of the art and to guarantee the functionality of the SIS, sensor, logic and actuators with an appropriate certification were used. The SIS of both PEAs consist of sensors from Endress+Hauser certified for the application, safety logic controller from HIMA and the operational logic controller and actuators from Festo. Looking at the equipment of the double-feed-PEA, all the necessary equipment is installed to be able to dose two media streams independently of each other. As can be seen in Fig. 3, the PEA has a technically redundant design for both dosing lines to allow independent dosing. For each dosing line there are three inlet ports for different media, for example inerting gas, educt, and solvent, which all lead in one vessel. The vessel (45 liters) has one gas outlet, and one liquid outlet with a hand valve towards the connected feed-FEAs. For safety functions, a radar level sensor at the top and a level-threshold sensor at the bottom of the vessel are installed.

The reactor-PEA is based on the design of the double dosing unit. Instead of two media streams, only one is implemented. A scaled-up heating-stirring vessel (60 liters) is mounted behind the three inlet valves. In addition to the monitoring functions, which are also built into the dosing unit, the vessel can be heated via 4 heating rods, which are mounted in the bottom. The reactor temperature can be monitored via a safety-related temperature sensor, which is also mounted in the bottom of the tank. For mixing of the educts, a stirrer is mounted on the top of the vessel.

The FEA realized the flow of the media with branches for the product, the waste, and a return-flow port. The main output is connected to the subsequent process step, the waste outlet is supposed to be used for the draining of media or solvent, and the return flow channel is supposed to be used as a safety pressure relief leading back to the tank. The pressure in the FEA is created by a pump and measured by two pressure sensors, one of which is used for the SIF to open the return flow channel. The flow of the main outlet is measured by a sensor and used for flow-control with a corresponding valve. Two of the three built FEAs are equipped as described above and are originally used in the double-feed-PEA. For the intended use

Fig. 4. The reactor-PEA, prepared for FEA exchange

of the reactor, a return flow channel is not foreseen. Therefore, the pipe, valve as well as one of the pressure sensors was not implemented in third FEA.

Following the two variations of the FEAs, the SIS in the PEAs have two different configurations accordingly—one for each type of FEA. To ensure the exchange of the FEAs without additional programming, these two configurations are pre-implemented in the safety controller and can be switched with a key-switch. This also means, that each configuration was tested and validated before hence. Alternative methods without organizational measures to switch configurations are possible, but must be safety proof.

For both PEAs, the adjustment of temperature, level and flow limits are integrated in the implementation.

The technical realization of the fSOL is executed on a HIMA F35 safety controller. The data transfer between the SIS of the PEA and the fSOL is established via a network connection. The goal is to realize data exchange via the manufacturer-neutral safety bus protocol »OPC UA Safety«. For this purpose, the intramodular Safety-Controller must allow access to safety-related data (e.g. SIF and limit values) via the network, i.e. act as a server. The fSOL must be able to access the data provided by the intramodular SIS and exchange data with them, i.e., act as a client. To always ensure independent safety of the PEAs, the SIS on the PEAs can run even without communication to the fSOL. Only intermodular functions are dependent on the communication.

To validate the safety functions, the possibility to trigger errors in the demonstrator is integrated. This is realized by manual valves to block the air flow to the pneumatics control of the valves. The position of the valves can then no longer be adjusted by the BPCS and is then transfered to the safe state by triggering safety-exhaust valves as part of a corresponding safety function. The scenarios were evaluated in form of a *modular Hazard and Operability Analysis* (mHAZOP) and chosen in that way, that the safety system never gets compromised.

3. Practical insights in modular planning approaches

With the technical realization as described, various safety concepts can be integrated and therefore validated as described in the previous sections. Additional key aspects were:

In order to consider aspects of modular design in the engineering of the demonstration plant, separate engineering processes were applied for the development of PEAs as well as FEAs, resulting in specifications for physical and electrical specifications.

The planning of the FEAs itself could be reused for all three realized assemblies, with some small reductions for the third FEA. The concepts of modular planning [6–8] could be applied with some variations, so that there were no additional efforts during the planning of the individual FEAs.

For the design of the PEAs, the SLCs proposed by Pelzer et al. [4] were used to ensure intra- and intermodular compatibility of the SIS of the MP, PEAs as well as FEAs. Special attention was paid during the execution of the SLC to the risk assessment, for which a mHAZOP according to the concept of Klose et al. [19] was applied. The advantage of mHAZOP through the separation of device-based and process-based analysis comes into play, both, when integrating a PEA into an MP and further when integrating an FEA into the PEA. The mHAZOP of the FEA only needed to be done once and could later be combined with the surrounding PEAs. With the definition of the boundary and application conditions of the FEAs and PEAs during the HAZOP analysis, a later mapping of installed safety measures to the requirements of the process can be conducted. This allows a decision to be made on the safety suitability of the PEA for the application.

All concepts were applied successfully but need further examination during the short- and long-term operation of the demonstrator. Also, efforts and potential of reuse with conventional planning is not compared directly yet, which should be done to for an extensive comparison.

4. Conclusion and outlook

In this article, we described the implementation of intra- and intermodular Safety Instrumented Systems in the context of modular plants. It could be shown, that the structure of modular process plants according to VDI 2776 can be used advantageously for the flexible adaption of safety systems of PEAs. Furthermore, the approaches for modular planning can also be applied when implementing safety systems, which was shown by building three interchangeable FEAs with slightly different characteristics. The engineering of the demonstrator served for the validation of the safety lifecycles for PEAs. In addition, initial practical experience was gained in realizing functional safety in modular plants.

The interdisciplinary framework of the Process-to-Order Lab and the Research Training Group (RTG 2323) of the TU Dresden enables research in modular automation taking human aspects and the modification of plant structures into account. In this context, the demonstrator represents an experimental plant in which adapt and exchange processes can be studied from different perspectives. For example, the demonstrator is designed considering ergonomic aspects, so that such processes can be examined in terms of occupational safety in addition to functional safety.

In further work, the necessary competencies of operators for the modification of safety systems will be investigated. In addition, the interdisciplinary team of the RTG is investigating the preservation of operator competencies in highly automated systems and causal structures in risk assessment.

Acknowledgements

The presented work has been receiving funding by the German Research Foundation (DFG) within the framework of the Research Training Group 2323 "Conducive Design of Cyber Physical Production Systems (CD-CPPS)" (project number 319919706) and by the BMWi in the project ORCA (FKZ 03ET1517-A). The authors would like to thank the members of the TaskForce Safety-MTP of NAMUR Working Group 4.5 for their support in the implementation of the demonstrator. Thanks to the P2O-Lab for providing the infrastructure and resources to implement the demonstrator. A special thanks to Endress+Hauser, Festo SE & Co. KG and HIMA Paul Hildebrandt GmbH (alphabetic Order) for the support in realizing the demonstrator.

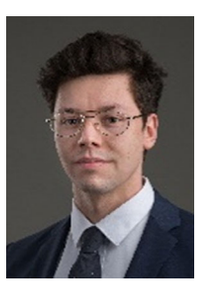
Funding Note Open Access funding enabled and organized by Projekt DEAL.

References

1. VDI 2776-1 (2020) Verfahrenstechnische Anlagen – Modulare Anlagen – Blatt 1: Grundlagen und Planung modularer Anlagen. www.vdi.de.
2. Czybik, B., Ehrlich, M., Trsek, H., Oswald, A. (2020): Eine differenzierte Betrachtung ganzheitlicher Selbstorganisation im Rahmen von Industrie 4.0. In Tagungsband der Automation. VDI-Bericht, (Vol. 2375, pp. 1055–1068).
3. Pelzer, F., et al. (2020): Intermodulare funktionale Sicherheit für flexible Anlagen der Prozessindustrie – Teil 2: Architektur und Engineering intermodularer Sicherheit und Safety-MTP. atp Mag., 62(10), 44–53. https://doi.org/10.17560/atp.v62i10.2508.
4. Pelzer, F., et al. (2021): Sicherheitslebenszyklen für die modulare Automation in der Prozessindustrie. atp Mag. 63(6–7), in press.
5. ENPRO-Projekt (2021): http://enpro-initiative.de/ENPRO+2_0/ORCA.html (visited 11. June 2021).
6. Fleischer, C., Wittmann, J., Kockmann, N., Bieringer, T., Bramsiepe, C. (2015): Sicherheitstechnische Aspekte bei Planung und Bau modularer Produktionsanlagen. Chem. Ing. Tech., 87(9), 1258–1269. https://doi.org/10.1002/cite.201400188.
7. Radatz, H., Elischewski, J., Heitmann, M., Schembecker, G., Bramsiepe, C. (2017): Design of equipment modules for flexibility. Chem. Eng. Sci., 168, 271–288. https://doi.org/10.1016/j.ces.2017.04.021.
8. Eilermann, M., Post, C., Radatz, H., Bramsiepe, C., Schembecker, G. (2018): A general approach to module-based plant design. Chem. Eng. Res. Des., 137, 125–140. https://doi.org/10.1016/j.cherd.2018.06.039.
9. VDI/VDE/NAMUR 2658-1 (2019): Automatisierungstechnisches Engineering modularer Anlagen in der Prozessindustrie – Allgemeines Konzept und Schnittstellen. www.vdi.de.
10. Bloch, H., et al. (2018): State-based control of process services within modular process plants. Proc. CIRP, 72, 1088–1093. https://doi.org/10.1016/j.procir.2018.03.037.
11. Holm, T. (2016): Aufwandsbewertung im Engineering modularer Prozessanlagen. Dissertation, Helmut-Schmidt-Universität.
12. DIN EN 61511 (VDE 0810) (2019): Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie. www.beuth.de.
13. Richtlinie des Rates über Mindestvorschriften für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln durch Arbeitnehmer bei der Arbeit (89/655/EWG) 1989.
14. Pelzer, F., et al. (2020): Intermodulare funktionale Sicherheit für flexible Anlagen – Teil 1: Grundlagen und Anforderungen. atp Mag., 62(6–7). https://doi.org/10.17560/atp.v62i6-7.2488.
15. Klose, A., Pelzer, F., Etz, D., Strutzenberger, D., Frühwirth, T., Kastner, W., Urbas, L. (2021): Building blocks for flexible functional safety in discrete manufacturing and process industries. In 26th IEEE international conference on emerging technologies and factory automation (ETFA), Västerås, Schweden (online), in press.
16. Menschner, A., et al. (2019): Von der Prozessbeschreibung zur modularen Anlage. In Tagungsband der Automation 2019. 1. Aufl. (Vol. 2351, pp. 287–300). Düsseldorf: VDI Wissensforum GmbH.
17. Schindel, Polyakova, Harding, Weinhold, Stenger, Grünewald, Bramsiepe (2021): General approach for technology and process equipment assembly (PEA) selection in process design. Chem. Eng. Process. https://doi.org/10.1016/j.cep.2020.108223.
18. Fleischer, C., Wittmann, J., Kockmann, N., Bieringer, T., Bramsiepe, C. (2015): Sicherheitstechnische Aspekte bei Planung und Bau modularer Produktionsanlagen. Chem. Ing. Tech., 87(9), 1258–1269. https://doi.org/10.1002/cite.201400188.
19. Klose, A., et al. (2019): Safety-lifecycle of modular process plants—information model and workflow. In 2019 4th international conference on system reliability and safety (ICSRS), Rome, Italy (pp. 509–517). https://doi.org/10.1109/ICSRS48664.2019.8987685.
20. Kletz, T. A. (1996): Inherently safer design: the growth of an idea. Process Saf. Prog., 15(1), 5–8. https://doi.org/10.1002/prs.680150105.
21. Bittorf, L., et al. (2020): Demonstratoren für dienstgesteuerte modulare Prozesseinheiten und deren effiziente Orchestrierung. In Automation 2020 (pp. 129–144). https://doi.org/10.51202/9783181023754-129.
22. BioPhorum (2021): Automated facility plug-and-play—Stirred tank unit interface specification. https://doi.org/10.46220/2021TR001.
23. Swain, A.D., Guttmann, H.E. (1983): Handbook of human-reliability analysis with emphasis on nuclear power plant applications. Sandia National Laboratories.

Authors

Florian Pelzer
(1994) has been employed as a research associate in the DFG Research Training Group 2323 "Conducive Design of Cyber-Physical Production Systems" at TU Dresden since July 2020. His research area includes safety-related orchestration and safety-related modification of modular production systems.



Anselm Klose
(1994) has been working as a research associate at the Chair of Process Control Engineering/AG Systems Process Engineering since 2018 and as one of the Managing Directors of the Process-to-Order Lab at TU Dresden since 2020. His research area includes safety analysis and orchestration of modular plants.

Jonas Miesner
(1994) joined TU Dresden in April 2020 as a research associate in the DFG Research Training Group 2323 "Conducive Design of Cyber-Physical Production Systems ". His research focuses on ergonomics in the application context of modular production systems.

Martin Schmauder
(born 1962) is Professor of Industrial Engineering at the Institute of Technical Logistics and Work Systems at TU Dresden. Together with his team, he carries out research in the field of ergonomics, occupational health and safety, and work organization.

Leon Urbas
(born 1965) holds the professorship for Process Control Engineering and is head of the Systems Process Engineering working group at the TU Dresden. With his team, he conducts research on semantic models, discipline-integrating methods and automation architectures for the digital transformation of the process industry.