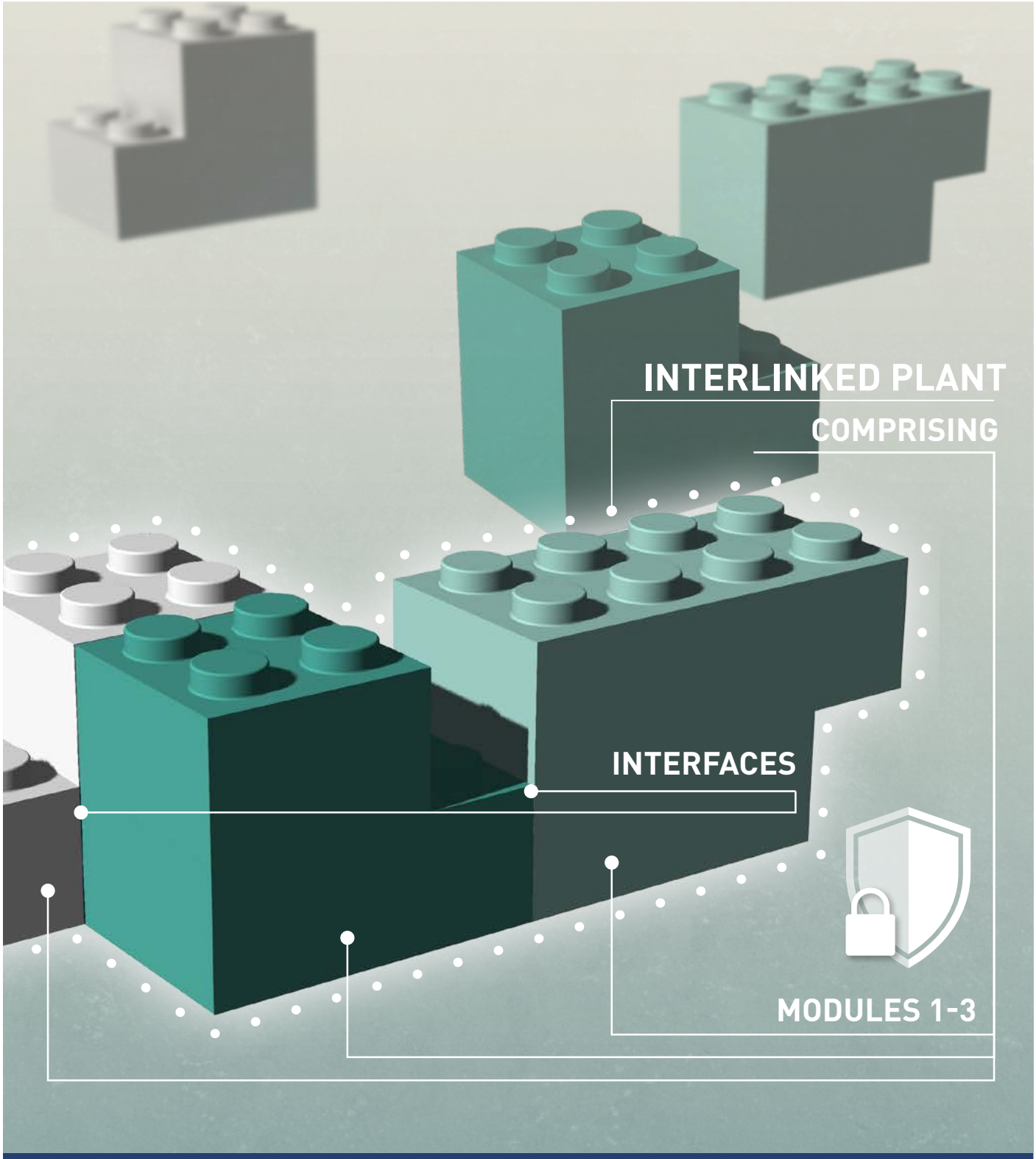


Safety on modular machines

Whitepaper SF-3.1: 04/2018

smartFactory KL®

Abstract
Working group 1 "Smart Infrastructure" of ***SmartFactory***^{KL} deals with the topic of safety in modular industry 4.0 production facilities.

The aim is a plant structure that enables flexibility and changeability, e.g. through modularisation. Intrinsically safe modules are equipped with conventional, functional safety. However, there are still dependencies between the modules. A new safety architecture is required in modular systems that also supports unknown modules.

The concept was integrated into the Industry 4.0 production facility last year to show by way of example that it can also be implemented with today's technologies. Only one single wire coexistence is used for the implementation of safety and machine communication.

Machines and machine modules can be inserted into or removed from production during runtime without affecting the rest of the plant. The necessary safety-related parameters are automatically negotiated, configured and released on the basis of the safety profiles introduced here. The requirements for these are described below.

Keywords
Safety; Industrie 4.0; Automatic certification;

Authors

Jens Popper	Technologie-Initiative SmartFactory KL e.V
Marius Blügel	Technologie-Initiative SmartFactory KL e.V
Hagen Burchardt	Bosch Rexroth AG
Steffen Horn	Phoenix Contact Electronics GmbH
Joachim Merx	Pilz GmbH & Co. KG
Dr. Detlev Richter	TÜV SÜD Product Service GmbH
Werner Varro	TÜV SÜD Product Service GmbH
Michael Pfeifer	TÜV SÜD Industrie Service GmbH
Pascal Staub-Lang	TÜV SÜD Industrie Service GmbH

Table of contents

1. Objective of the Whitepaper

This white paper summarizes the current results of the working group on "Safety on modular machines". In cooperation with the partners Bosch Rexroth, B&R, Festo, Phoenix Contact, Pilz and TÜV Süd, a concept for simplified, partially or fully automated certification was developed. Based on the description of safe profiles, which are defined and stored within the asset administration shell (cf. DIN SPEC 9134), a partial concept was developed to enable the modular certification of machine groups.

According to this concept, a network of machines can automatically be described as safe in relation to specific safety functions if a profile[1] exists that describes this very safety function. The safety functions must be implemented by all machines in the network. If there are machines in the network that have not implemented one of the required profiles or whose profile is outdated, qualified personnel must manually assess the safety risks not fully covered. The manual evaluations of the system configurations that cannot be automatically classified as safe are stored centrally later on. This means that the tested system configuration based on the new safety parameters dynamically stored in the asset administration shell is also available for future considerations. The aim of the working group is to be able to map this process automatically.

This concept and its implementation in the ***SmartFactory***^{KL} Industry 4.0 system are explained below.

1 For a definition of profiles see chapter 4

2. Status Quo

2.1. Safety requirements for industrial 4.0 production plants

Due to increasing international competition and increasingly complex products, the production facilities used in industrial production are also characterized by constantly growing complexity. Already today, this very complexity exceeds a threshold above which it can no longer be controlled by the industrial user. There are many reasons for this development. The high availability required by increasing competition, the flexible adaptation of new technologies and the mass production of customer-specific products in batch size 1 due to increased customer requirements must be explicitly mentioned here. Therefore, concepts must be developed with the help of which the perceived complexity of the plant can be reduced by shifting tasks to automation technology.

One such concept inherent in Industry 4.0 is the ongoing modularization and flexibilization of production processes. At the functional control level, extensive concepts were described in the past, in particular through the ***SmartFactory***^{KL} system architecture [SF1.1:04/16] and validated using practical applications. Information from which added values can be generated is available in real time. This modularization and flexibilization of production plants may on the one hand encapsulate the complexity of the entire plant and thus make it controllable, but on the other hand there is an increased effort to meet the safety requirements defined within the Machinery Directive (2006/42/EC or 9th ProdSV in Germany).

The necessary first step in the development of modular systems with regard to safety requirements is to make the dedicated production modules intrinsically safe. Each production module is considered and certified as a complete machine in the sense of 2006/42/EC Art. 2. This procedure does not differ from the certification process of static systems and is therefore not considered in the following. What is rather problematic in the safety-related consideration is the linking of the intrinsically safe modules in operative use[2]. When converting a modular production line, new dependencies may occur at the interfaces (mechanical, electrical, IT) between the intrinsically safe modules, which force a new safety-related consideration. A test forces all interfaces which induce a new safety-relevant connection, i.e. a risk for the user not previously considered.

2 For the definition of an interlinked plant see chapter 2.2

From these considerations it follows that although the increase in flexibility and the modularization of the production plants meet many of the new requirements for industrial production mentioned above, they do, however, cause new problems in the area of safety. In order to meet the existing requirements for the safety of industrial plants - regardless of which machine types are used – new, adaptive safety concepts are required.

A necessary prerequisite for an adaptive safety concept is a cross-module interface information model. This makes it possible to make the module specifications necessary for certification available to a service provided for checking safety features within the business process layer of RAMI 4.0. ***SmartFactory***^{KL} already uses an interface information model based on OPC-UA [SF-2.1:04/17] shown in Figure 1, which describes data and information flows without specifically addressing machine safety. The industry is beginning to formulate information models in VDMA working groups [VDMA17]. This white paper aims to provide a cross-industry building block for existing and future Companion Specifications, which will further improve interoperability in modular production facilities and reduce the administrative effort involved in commissioning interlinked machines.

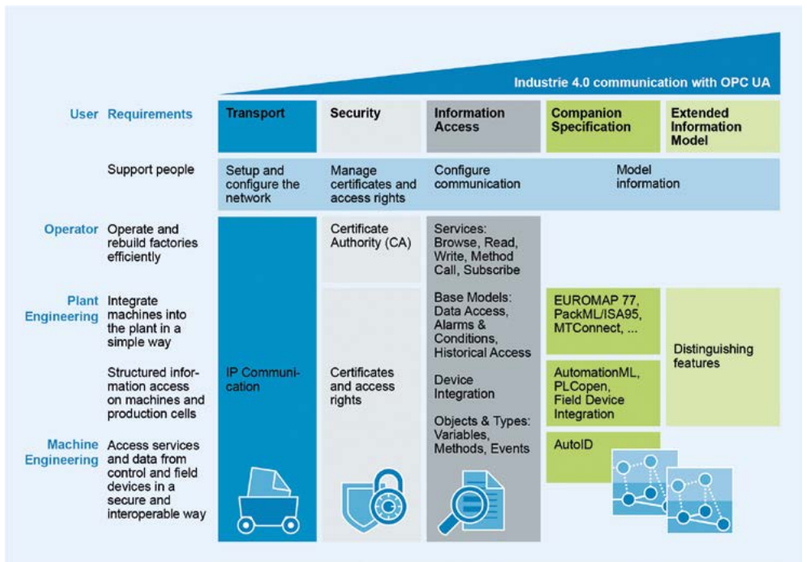


Figure 1:
OPC UA Information Model

2.2. Status Quo – Machine safety of modular systems

Existing standards, such as DIN EN ISO 13857, only describe the safety aspects of static systems. These can only be transferred to flexible, networked systems to a limited extent due to the new challenges already described.

An interlinking of modules to form a plant is to be regarded as a whole of machines within the meaning of the Machinery Directive 2006/42/EC if there is a technical production[3] and safety[4] connection between the interlinked modules (see [BMAS11]). If these interrelationships are proven, the interlinked plant must be assessed as a whole and the operator assumes the legal role of the manufacturer with all duties. This includes the preparation of a risk assessment, on the basis of which a declaration of conformity must subsequently be drawn up. A risk assessment in accordance with Annex I 2006/42/EC consists of a risk analysis in which the risk potentials are identified and a risk assessment in which they are evaluated.

The Performance Level (PL) is used below to describe the reliability of a safety function and to evaluate it in a risk assessment. This is a technology-neutral concept that can be applied to mechanical, electrical and hydraulic safety solutions and is laid down in EN ISO 13849-1. The PL is divided into five categories from a (lowest contribution to risk reduction) to e (highest contribution), which describe the minimum level of safety to be achieved. The required PLr (Performance Level required) is determined on the basis of the three criteria "severity of injury", "frequency and length of stay" and "possibility of avoiding the hazard". The PL achieved, however, results from the interaction of MTTF[5] values, the degree of diagnostic coverage, the average probability of a dangerous failure per hour, redundancy and the common cause of the error.

In order to enable the modularity of a system, for example for standardized machines, today all possible variants/configurations are considered, evaluated and validated. This presupposes that all modules whose safety-related properties are known and the procedure and results are documented and validated by a person responsible. This procedure is only partially effective for modular I4.0 systems. Due to the constantly changing technologies and the requirement for batch size 1, it is not possible to estimate in advance which system configurations will be required in the future. Due to the different safety protocols of different competing suppliers on the market, the manageability of all possible interactions between machines and applications at higher levels is also made more difficult.

3 Arranged as a whole, acting as a whole or actuated as a whole.
4 An event of one machine can lead to a hazard in another machine.
5 Mean time to failure

The aim of the working group is not to define or develop a uniform safety protocol. Instead, requirements are collected at a more abstract level in order to implement adaptive safety with all protocols available on the market and in the future. In this Whitepaper, requirements for safety functions are presented within the framework of a concept, taking into account the complexity and the interaction of existing technologies..

2.3. Safety within the SmartFactory[KL] Industry 4.0 system architecture

The ***SmartFactory***[KL] technology initiative, together with its partners, demonstrated how industry 4.0 paradigms can be implemented with existing manufacturer-independent technologies at the Hannover Fair 2014 (see Figure 2).

Dedicated production modules with their own control take over the execution of individual process steps. Each of these production modules represents a complete machine according to the Machinery Directive and has its own CE conformity. As already mentioned at the beginning, the creation of a machine network from these production modules requires in certain cases a new safety-related consideration of the entirety due to existing relevant interfaces. As a result, no overall CE conformity for the resulting machine network can be derived from the combination of several CE-compliant production modules. The entire industry 4.0 system of the ***SmartFactory***[KL] technology initiative is based on paradigms such as plug & production, vertical networking and decentralized production control in order to enable individualized production in batch size 1 "on demand". These paradigms and intelligent neighborhood detection allow individual modules to be replaced during operation without significantly affecting production. In practice, however, a safety assessment must be made when changing the configuration of a machine group. These revaluations are contrary to the goal of flexibility and thus form a bottleneck.

The challenge within this context is to check as automatically as possible whether it is necessary to re-examine safety after two or more modules have been assembled. Overall conformity is given if the modules are safety-related independent of one another, especially if the system is not an interlinked system (see section 2.2). If, on the other hand, dependencies exist, a new examination is necessary according to the current state of the art. Only the safety risks caused by the combination of the modules and the resulting interfaces are considered. This does not mean that the interface does not increase the risk within a previously intrinsically safe module. The requirements for an analysis of the conformity of such a machine network therefore include the questions,

1) whether the machine is interlinked and

2) if yes, which safety-related interdependencies exist and

3) which consequences result from the evaluation of safety dependencies?

3. Concept

3.1. Requirements

In order to achieve a highly flexible production line with which a wide variety of customer orders can be processed (see Mass Customization), it may be necessary to frequently change the composition of the production modules. The aim is that any combination of I4.0 machine modules from various manufacturers automatically results in a CE-compliant machine network. For this certification process, the obligations for the manufacturer of the interlinked plant summarized in excerpts in the following table arise:

Machinery Directive-obligations	*Source*
Risikobeurteilung (risk assessment)	MRL 2006/42/EG Anhang I
Maschinenkennzeichnung (machine identification)	MRL 2006/42/EG Anhang I.1.7.3
Betriebsanleitung (operating manual)	MRL 2006/42/EG Anhang I.1.7.4
Konformitätserklärung (declaration of conformity)	MRL 2006/42/EG Anhang II
CE-Kennzeichnung (CE-labeling)	MRL 2006/42/EG Anhang III
Technische Dokumentation (technical documentation)	MRL 2006/42/EG Anhang VII

Table 1:
Legal obligations when linking modular systems

To enable these requirements to be met automatically, several basic requirements must be met. These are, for example, CE-compliant machine modules with "basic" risk assessment provided. Furthermore, a clear and complete interface description of each machine module is required, cf. DIN SPEC 91345: RAMI 4.0. The machine modules in turn must be able to communicate with each other and with the central production servers. The use of machine modules from various manufacturers requires a service-oriented, platform-independent communication protocol, e.g. OPC UA via TCP/IP. By removing and adding machine modules, the risk assessment is automatically adapted to the changed production line, eliminating the need to manually change the risk assessment, thus saving resources. Analogous to the machine modules, modules must meet the same requirements (interface description, service-oriented communication).

3.2. Concept for automatic conformity assessment

The following concept describes how the implementation and use of the described requirements can lead to an automatic evaluation of interlinked systems. A distinction is made between different phases, which operationalize the manual procedure for conformity assessment and make it manageable for IT processing.

- ***Discovery phase***
  The discovery phase, as understood in this context, is comparable to that of OPC UA. A data connection is established with the new machine module, this is identified and the module properties are transmitted. The module properties are stored within the management tray and serve as a basis for further conformity testing. During the discovery phase, not all contents of the management shell need to be transmitted, since safety relevant submodels of the asset administration shell are not eligible for automatic conformity assessment. It is therefore sufficient to transmit only the manifest of the header, which serves as a clear table of contents for all information, data and functions within the administrative shell (cf. BMWi 2016).

- ***Validation phase***
  The validation phase essentially consists of two steps. Determining the configuration of the new production plant and validating the configuration using profiles. These profiles represent partial models of the asset administration shell and contain all safety-relevant information of the module. Thus, they form the basis for the further evaluation process. When determining the configuration, it is determined which machine module is docked to which module. This information is required so that the interfaces or the requirements for the interfaces of the individual modules can be evaluated correctly. The combination of modules, work processes and workpiece (material) can result in a different risk potential and therefore different requirements for the safety function – classified by the performance level.

- ***Plausibility check***
  Subsequently, the communication parameters for safe cyclic communication are read from the management shell and subjected to a plausibility check. This compares for example network timings and ensures that reliable response times can be maintained in all safety functions.

- ***Digital conformity assessment (proof of CE conformity)***
  Parallel to the plausibility check, the digital conformity assessment takes place after the validation phase. The information exchanged between the components

involved is transmitted to a cloud service in the form of profiles (configuration of the machine modules, machine module IDs with module and safety module properties, planned work process, etc.) and/or checked during communication.

Cloud does not necessarily mean servers that are set up "somewhere", it can also be local computing systems located on the factory premises or highly secure cloud solutions. In addition to protecting the confidentiality of data during transmission and storage, highly secure cloud solutions require technical confidentiality protection during data processing, i.e. during calculations in the processor, volatile storage in RAM, etc. This includes protection measures such as the Software Guard Extensions (SGX) for Intel processors, the Secure Encrypted Virtualization (SEV) for AMD or the Sealed Cloud from Uniscon[6].

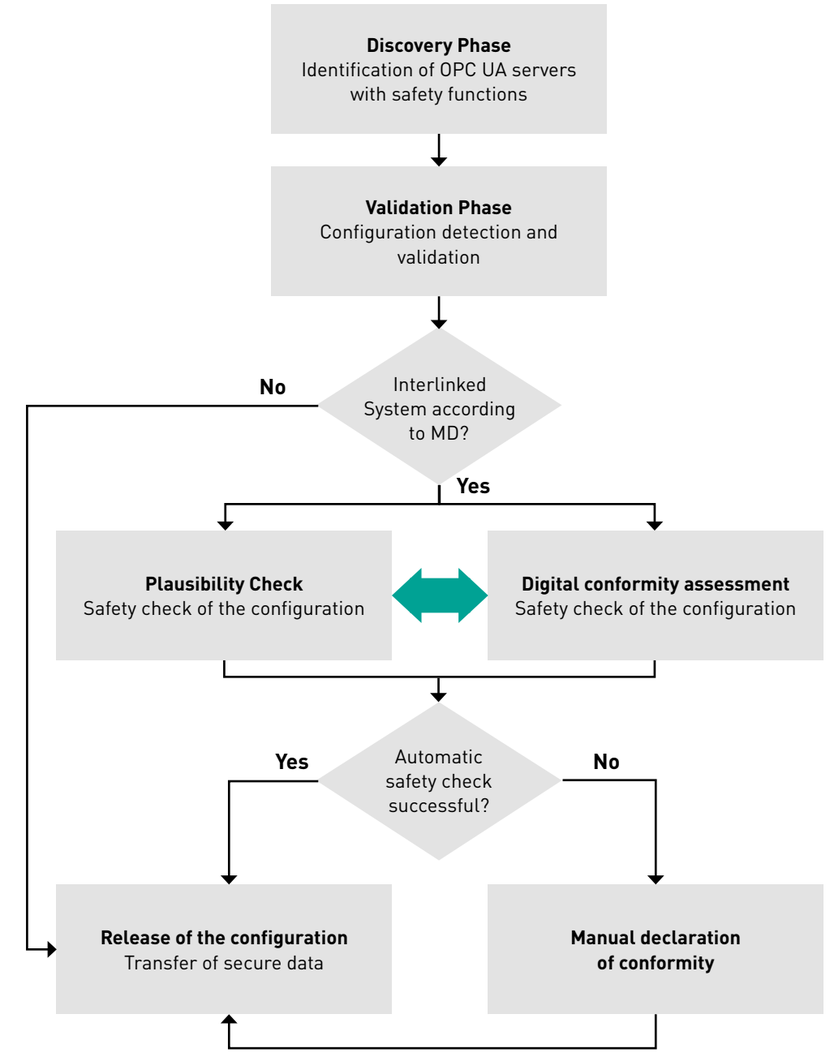
  Taking into account the characteristics of the individual machine modules, interface requirements, requirements resulting from the linking of certain machine modules, etc., the required performance levels are compared with regard to compliance by the machine modules (see SISTEMA). Furthermore, the documents required by the Machinery Directive (e.g. risk assessment) are automatically derived from the safety profiles of the modules involved and created, stored and archived accordingly. If the cloud service concludes that the requirements with regard to machine safety are fulfilled by the machine module network, the declaration of conformity is created and also archived and keys are generated. The keys contain the logical IDs of all safety actuators and sensors involved, the ID of the safety control, the typology and the achieved performance level. The keys are transmitted to the respective safety controllers and stored there. The safety controller checks the accessibility of the logical participants. By applying the safety functions with the specified participants, the correctness of the respective key is checked. This information is enriched with packet runtimes by the security controller and a new key is created. This key is transferred back to the cloud, checked and archived.

- ***Approval of the machine group***
  Once the described process is complete and successful, the cloud service releases the production plant to put itself in standby mode.

In order to maintain today's high level of machine safety, and at the same time to take advantage of the possibilities of new technologies, a 2-way communication was implemented in this automated concept, such as it is used by rescue services, for example. The automatically generated documents can be called up at any time and could be made available for review by an expert if required.

The following figure illustrates the phases described for the automated integration of a new machine module into a production line using a flow diagram:

FIgure 3:
Phase diagram



6 Viewable at www.uniscon.de

4. Realization within the SmartFactory[KL]

4.1. Structure of the modules and applications

The modules of the ***SmartFactory***[KL] are identical with regard to their internal workpiece transport. Transport takes place via two counter-rotating conveyor belts, each of which is secured at its ends by gates. The gates controlled by pneumatic cylinders can be the "open" and "closed" states. The following figure describes the transport device of the ***SmartFactory***[KL] modules:

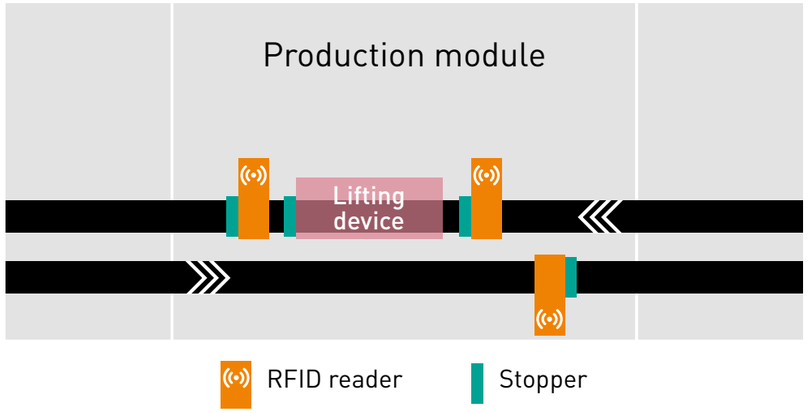
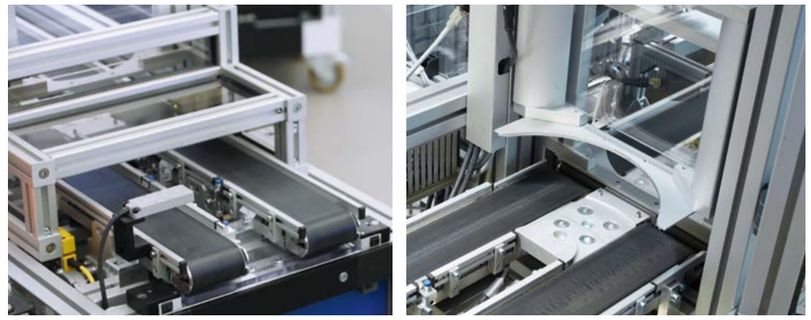


Figure 4:
Transport unit of the production modules

Protective/maintenance doors and emergency stop switches have been installed on each module as physical protective devices. A necessary step with regard to modular safety has already been taken by dynamically expanding the emergency stop circuit of the modules belonging to it from a local point of view. In addition to the modules already described, there are special transfer modules (hereinafter referred to as docking stations) that realize workpiece transport at the end of a production line to the "Robotino" driverless transport system. These docking stations do not have any gates themselves, as there is no immediate danger from the functional assembly of this module. In order to prevent a possible hazard due to intervention in an adjacent module, a protective tunnel was implemented which is directly adjacent to the gate of the neighboring module and, due to its height, makes it impossible to reach through. The Robotino itself has an emergency stop switch which stops the Robotino alone or the entire production line. All relevant safety functions are wirelessly connected to the safety system. During the docking phase on one of the various production lines, a workpiece transport takes place between the line and Robotino, which, from a safety perspective, must be temporarily assigned to the corresponding line. Therefore, the emergency stop switch of the driverless transport system must be integrated into the emergency stop circuit of the corresponding line during the docking phase until undocking from the line. The assignment of the Robotino to one of the emergency stop circuits is determined by the current position (redundant location position) and signalled by different coloured, controllable LED rings. A specific color is assigned to each machine line, which visually represents the affiliation to the user.

The further versions are limited to the interfaces for linking the described system modules. The following illustrations show the protection devices "gate" and "protective tunnel" that have been implemented:

Figure 5:
Protective tunnel left and gate on the right



From this described structure of the modules and the resulting properties of a concatenation of these, different cases arise, which require a safety-related consideration.

Case 1:
A problem with neighboring machine modules arises when an attempt is made to access another module by opening a v through the gates:

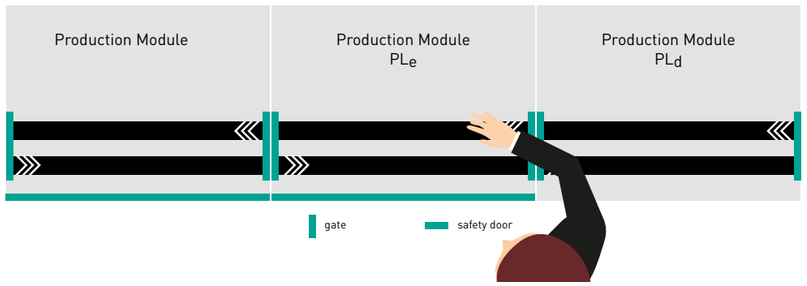


FIgure 6: Case 1

Such a case must be considered in automatic digital conformity assessment. If neighboring modules have different PL, restrictions may arise. For example, the module with the higher performance level could affect the safety evaluation of the module with the lower performance level.

Case 2:
Another conceivable case exists if one module has a door lock and the neighboring module does not. This case follows directly from the considerations in case 1 and results from different PL of the modules. If the maintenance and/or safety door without a lock of the module is opened, the gates must close immediately if a module with a PLr greater than the PLr of the module in question is adjacent in order to prevent penetration during operation of the neighboring module. If the PLr of all adjacent modules is equal to or less than that of the module under consideration without locking, it is not necessary to close the gates immediately.

Case 3:
If neighboring modules are in different operating modes (e.g. manual, automatic operation, docking or undocking), there is another case of a possible additional hazard in interlinked operations. In this case, the gates between the modules must always be kept closed.

4.2. Safety profile definition

Through the described structure of the modules and the safety-related consideration of the interfaces as well as the resulting hazards, different profiles can be defined which should enable automatic conformity assessment when linking the modules. For a ***SmartFactory***^{KL} production module, the profiles are “Performance Level”, “Emergency Stop”, “Gates” and “Protective Door”, regardless of which module it is.

Safety profile performance level
The risk assessment is used to determine the PLr of the machine module, which must be evaluated via the profile for an interlinked machine. As mentioned above the production modules are intrinsically save, thus PLr = PL applies. This means that all protective measures used within and at the module interfaces meet the requirements resulting from the module's functions.

Profile definition performance level: PL = PLr = x ϵ [a, b, c, d, e]

Safety profile emergency stop
The emergency stop switch must be present in each module. Therefore, each module also has an emergency stop safety profile. The emergency stop acts on the module itself and, in the case of an interlinked machine, on the entire line.

A red light on the switch indicates that the emergency stop switch is in the active state. There is an additional second light ring around the switch, the colour of which indicates the functional affiliation. Emergency stop switches that are functionally assigned to the same machine group have the same color.

Profile definition emergency stop:
- Emergency stop available

Safety profile safety door
The safety door allows access to the inside of the module. If there are dangerous points or dangerous movements in the module, the system must be shut down when the safety door is opened. If a timely shutdown is not possible, the safety guard must be equipped with a locking device.

Profile definition of the safety door
- safety door available
- door lock available
- PL

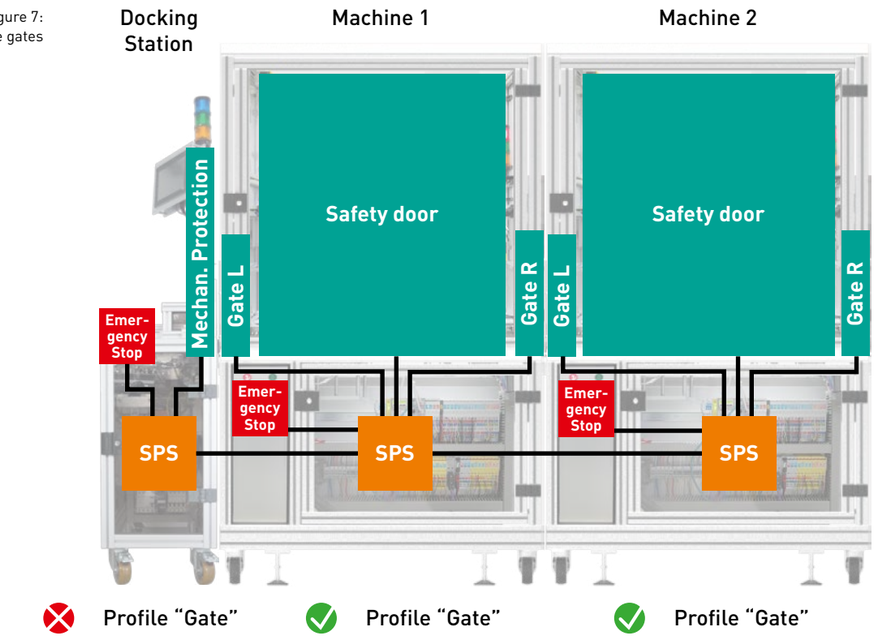
Safety profile gates
The material is transported between the modules through the gates. The gates can be opened and closed. When closed, the gate prevents access to the dangerous movement. If there is no danger from one module, the lock door can be omitted. In stand-alone operation of the machine module, the gates are closed. If the machine module is at the end of the line, the gate must be closed at the front. At the docking stations, no gate but a protective tunnel was implemented, which is included in the "gate" profile due to the same protective function.

Profile definition:
- Gate on the left side available
- Gate on the right side available
- Gate == protective tunnel
- PL
- Operating mode

As explained above, the profiles describe the structure, behavior and interfaces of a machine. For the use case 'gates' this means that a profile 'gate' presupposes the existence of a physical gate, which is shown in the asset administration shell. It also means that the profile for safety gate monitoring must be implemented.

Runtime validation ensures that the machine has the necessary components to implement its profiles, as can also be seen from the asset administration shell. The profile also describes the behaviour that lgates must be closed when a safety door is unlocked.

Figure 7:
Use-case gates



If all machines in a group have implemented the profile, the group can automatically be certified as safe in regard to the safety functions that require this profile. If it lacks the necessary information, qualified personnel must evaluate the possible safety guidelines. This way, manually confirmed configurations for this system configuration are stored and can also be automatically certified in the future on the basis of the new safety parameters dynamically stored in the asset administration shell.

4.3. Application-related description of digital conformity assessment

From the concept in Chapter 3 and the profile definition in Chapter 4.2, the steps within the validation phase and the digital conformity assessment are described as examples. The following flow chart describes the digital conformity check when several machine modules are linked to form a system:

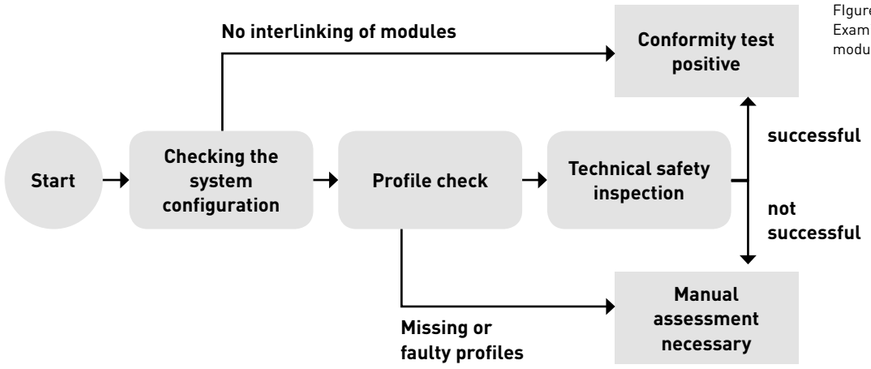


FIgure 8:
Examination of interlinked modules

The first step is to check whether the plant is generally an interlinked system within the meaning of the machinery directive. For each module, the system checks which other modules it has a neighborhood relationship with. If there are no neighborhood relationships, the conformity test is completed due to the intrinsically safe individual modules. If neighborhood relationships exist, these are saved and the profile check is triggered. Figure 9 illustrates the check of the system configuration:

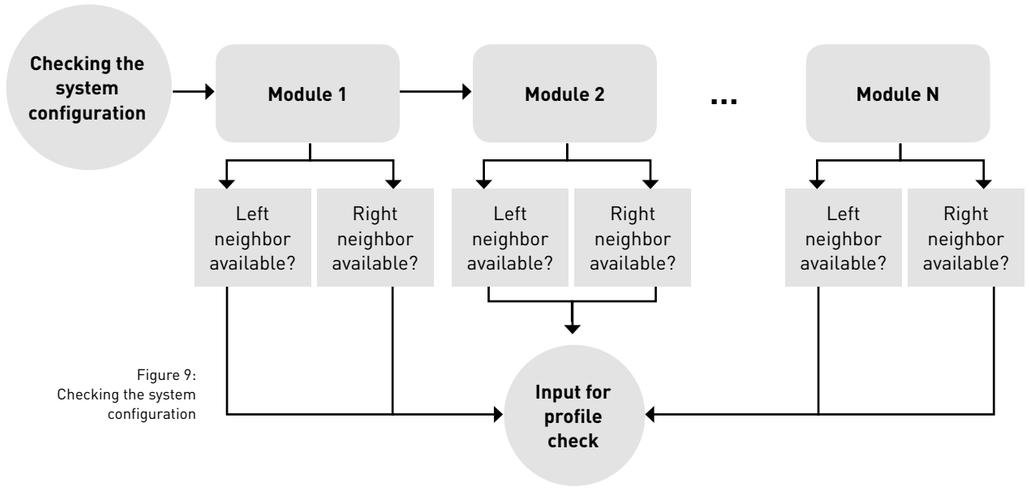
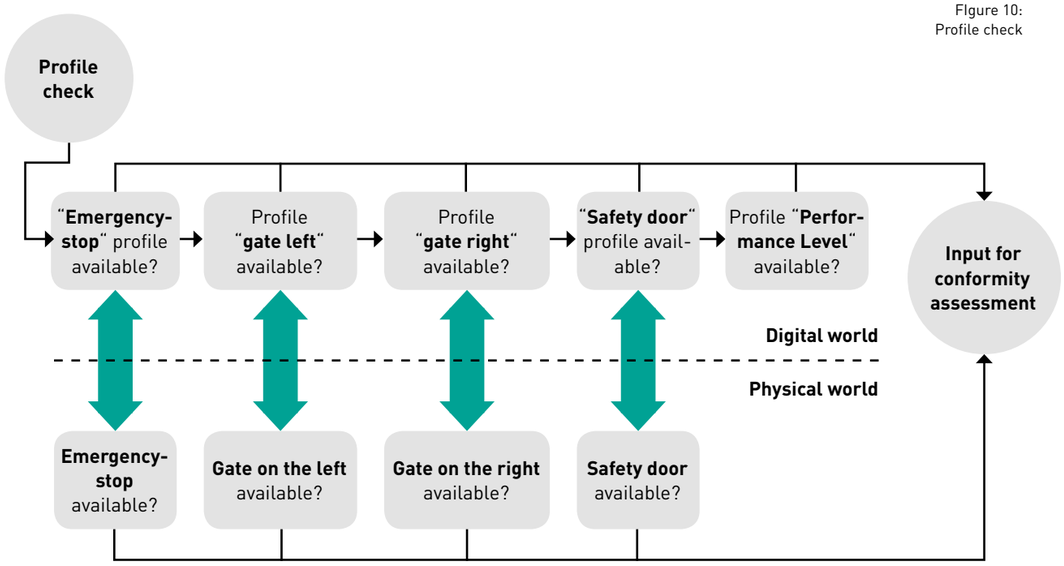


Figure 9:
Checking the system configuration

The profile check takes place at different levels. First, the profiles required due to the neighborhood conditions are loaded from the asset administration shell. If one or more of the required profiles do not exist, the process is terminated and the interface must be valuated manually. If all profiles are available, they are compared with the information stored within the PLC. If there is no physical representation of the profile, a manual check must also be initiated. When all required profiles are available and up-to-date, the actual safety check of the interfaces is initiated Figure 10 illustrates the profile check:

FIgure 10:
Profile check



Within the safety-related check, the loaded and verified profiles are compared. Automatic conformity assessment can only take place if the profiles at the corresponding interfaces are identical. There are two exceptions. First, when a gate is adjacent to a protective tunnel. In this case, it is sufficient if the profile contains either the instance "left gate available" or "right gate available" or "gates==protective tunnel". In the second case, there are no gates, but identical safety door profiles on all adjacent modules, which completely avoid intervention in potentially hazardous operating modes. Figure 11 illustrates the safety check:

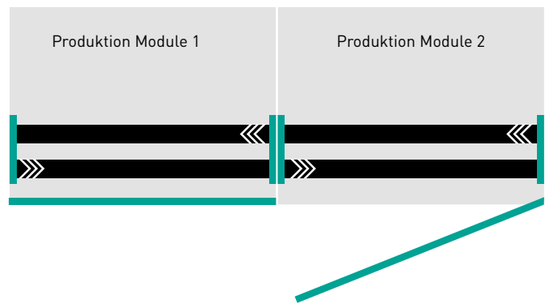
FIgure 11:
Safety check

If the safety check is not successful, the conformity check must be carried out manually.

4.4. Exemplary conformity check of two linked modules

Finally, the procedure described in Section 4.3 is illustrated using the example of two interlinked module. In this case, it is an interlinked system with two individual modules, shown in figure 12:

FIgure 12:
Linked modules



The following table summarizes the existing profiles of the intrinsically safe modules and serves as a basis for the subsequent evaluation:

Profile	*Module 1 (left)*	*Module 2 (right)*
Performance Level	PLC	PLC
Emergency stop	Available	Available
Gate left	Gate right	Gate right
Gate right	Gate left	Gate left
safety door	Available With door locking	Available With door locking
OM	Auto	Auto

The check of the system configuration shows that there is an interlinking and a profile check must be carried out.

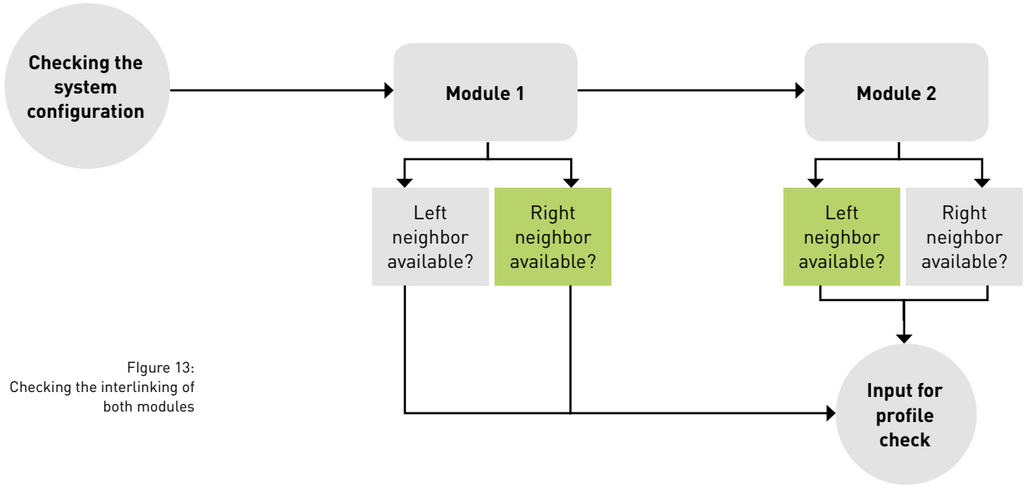


FIgure 13:
Checking the interlinking of both modules

To do this, all necessary interface profiles must be available.

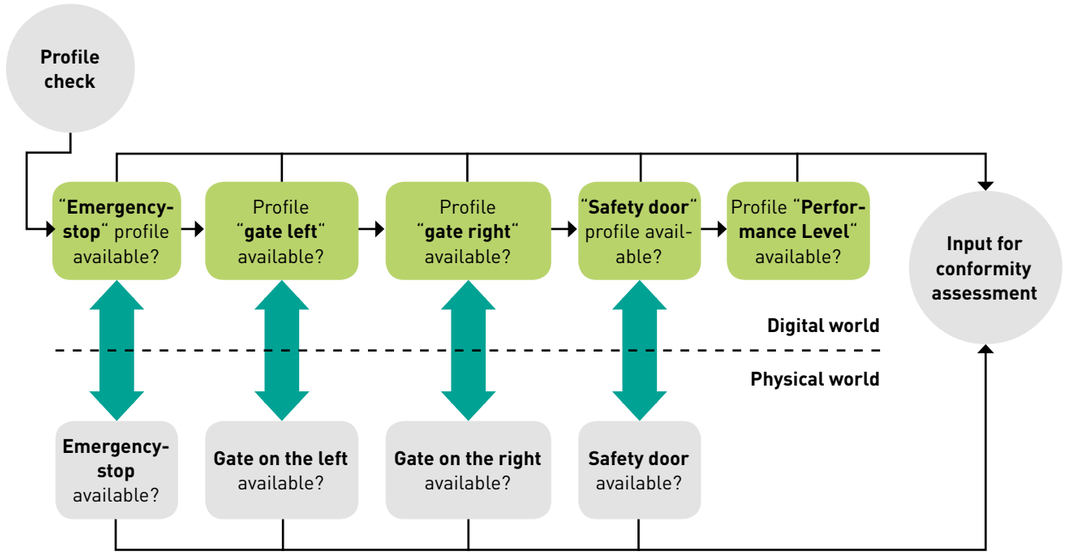


FIgure 14:
Profile check of the modules

The subsequent check of the determined interface profiles shows that the "safety door" profile differs between the two modules. The safety door of module 2 has no door locking, which means that an automatic conformity test is not possible at this point.

FIgure 15:
Completion of the safety test

A manual conformity check must therefore be carried out in which all the potentially arising risks from the interlinking must be considered and assessed.

Operating phase

The gate may be opened if all of the following conditions are met:

- If adjacent modules are present, the two adjacent modules must be in the same operating mode.
- No neighbor and manual operating mode

The gate must be closed if:

- own or adjacent safety door is opened (same OM) and gate area is free

Secure information to communicate:

From the machine module:

Profile	*Signal*	*Bit-Nr.*
Emergency stop	Local emergency stop (low active)	0
	Local reset	1
Safety door	Safety door closed	2
	Door locking active	3
Gate	Gate left closed	4
	Gate right closed	5
OM	Manual=0, Auto=1	6
	Undocking request	7

To the machine module:

Profile	*Signal*	*Bit-Nr.*
Emergency stop	Global Emergency Stop (low active)	0
	Enable machine	1

5. Summary and Outlook

Summary

This white paper describes a concept for the automatic certification of Industry 4.0 production modules. The aim is to provide greater flexibility when changing machine groups. Changes to the machine group are accepted as safe (machinery directive) if the individual components have the safety profile expected for the overriding protective function in which the safety functions are described and are implemented by all machines in the group. If there are machines in the group that have not yet implemented the required profiles, or if these profiles are obsolete, they must be revaluated manually. These are stored in the asset administrative shell and will be available to the machine group in the future.

The thoughts presented in this white paper on automatic conformity assessment and its exemplary use case provide an impulse for the implementation of the concept in practice.

Outlook

The white paper provides an impulse for automatic certification of machine modules, but there are still work packages to be worked out before implementation. The safety profiles must be created uniformly, they must not differ from machine to machine, so that uniform Ind4.0 validation requirements can be considered for automatic certification.

Furthermore, the cloud is a central component of the concept. However, this also places special requirements on them. It must be clarified how the communication between the machine and the cloud must be designed in order to meet the security requirements for the desired certification. With UNISCON's Sealed Cloud as an external cloud service, the process can be implemented because the issue of data security has already been considered. The certification process must be described in detail.

Working group 1 "Smart Infrastructure" of ***SmartFactory*** continues with the goal of developing new concepts on the topic of safety and evaluating them with regard to their practical suitability.

6. Sources

Scope Online: OPC UA und openSAFETY – Linien sicher automatisieren,
https://www.scope-online.de/automatisierung-steuerungstechnik/b-r--linien-sicher-automatisieren.htm

Hanser Konstruktion 2017: Flexibler dank neuem Safety-Konzept,
https://www.hanser-konstruktion.de/news/uebersicht/artikel/flexibler-dank-neuem-safety-konzept-3137879.html

Wirautomatisierer.de 2017: Smart-Factory-KL-Anlage um Safety-Konzept erweitert,
http://wirautomatisierer.industrie.de/top-branchennews/branchennews/smart-factory-kl-anlage-um-safety-konzept-erweitert

Computer-Automation.de 2017: Modulare Safety in der ***SmartFactory***^{KL},
http://www.computer-automation.de/steuerungsebene/safety-security/artikel/144904/

TÜV Süd Product Service 2015:
Modulare Zertifizierung für dynamisch konfigurierbare Industrie-Systeme

BMWi 2016: Bundesministerium für Wirtschaft und Energie (BMWi) (2016): Struktur der Verwaltungsschale. Berlin. Online verfügbar unter http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=6, zuletzt geprüft am 13.04.2017.

[BMAS11] Bek. d. BMAS v. 5.5.2011, IIIb5-39607-3:
Interpretationspapier zum Thema "Gesamtheit von Maschinen", 2011

BMWi 2016: Bundesministerium für Wirtschaft und Energie (BMWi) (2016): Struktur der Verwaltungsschale. Berlin. Online verfügbar unter http://www.plattform-i40.de/ I40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=6, zuletzt geprüft am 13.04.2017.

[SF-1.1:04/16]: ***SmartFactory***^{KL} Systemarchitektur für Industrie 4.0-Produktionsanlagen. Whitepaper SF-1.1:04/2016, http://smartfactory.de/wp-content/uploads/2017/08/SF_WhitePaper_1-1_DE.pdf

[SF-2.1:04/17] Exemplarische Übertragung der RAMI 4.0-Verwaltungsschale auf die ***SmartFactory***^{KL} Systemarchitektur für Industrie 4.0-Produktionsanlagen. Whitepaper SF-2.1: 04/2017, http://smartfactory.de/wp-content/uploads/2017/11/SF_WhitePaper_2-1_DE-1.pdf

Version history:
Whitepaper SF-3.1: 04/2018

Issued by:
Technology Initiative SmartFactory KL e.V.
Trippstadter Straße 122
67663 Kaiserslautern

P +49(0) 631 20575-3401
F +49(0) 631 20575-3402

The technology initiative SmartFactory KL e. V. (***SmartFactory***^{KL}) is a non-profit association under public law registered at the association register Kaiserslautern.

Association registration number: VR 2458 Kai

Scientific coordinator:
Dr.-Ing. Achim Wagner
P +49 (0)631 20575-5237
M achim.wagner@smartfactory.de