# Smart Safety Requirements for Digital Machine Representation 2020

Whitepaper SF-3.3: 09/2020

smartFactory KL®

**Abstract**
Working Group 2 "Connect & Control" (formerly, WG 1 "Smart Infrastructure") at ***SmartFactory***KL is focused on the subject of safety at modular, Industrie 4.0 production plants. The digital representation of machines requires specific safety content for a practical implementation of a simplified, partially or fully automated, machine safety assessment. From a safety perspective, the required content for a digital machine representation should be standardized under a concept based on simple interchangeable machine modules or, a "Plug & Produce" production plant. Furthermore, the need for standard safety semantics is also recognized. Both of these standardization requirements are necessary to ensure the feasibility of "Plug & Produce" as well as to realize "dynamic machine safety" and the associated increase in efficiency and productivity.

**Keywords**
Safety; Industrie 4.0; Automated Certification; Asset Administration Shell

**Autoren**

| | |
|---|---|
| William Motsch | Technologie-Initiative SmartFactory KL e.V. |
| Alexander David | Deutsches Forschungszentrum für Künstliche Intelligenz |
| Michael Pfeifer | TÜV SÜD Industrie Service GmbH |
| Dimitri Harder | TÜV SÜD Produkt Service GmbH |
| Josef Güntner | TÜV SÜD Industrie Service GmbH |

# Table of Contents

# 1. Purpose of the White Paper

This White Paperprovides a summary of the current findings of Working Group 2 on the subject of modular machine safety.

Stakeholders Bosch Rexroth, B&R, Festo, Phoenix Contact, Pilz, and TÜV Süd developed and released a concept for a simplified, partially or fully automated certification at the Hannover Messe 2018 [https://smartfactory.de/wp-content/uploads/2018/04/SF_WhitePaper_Safety_3-1_DE_XS.pdf]. A sub-concept that enables individual component certification of modular machine groups was developed using the descriptions of safety profiles defined and stored within the asset administration shell (cf. DIN SPEC 91345). Based on this work, we expanded the existing safety inspection concept for modular machines by several levels and introduced it at the Hannover Messe 2019 [https://smartfactory.de/wp-content/uploads/2019/03/Whitepaper_AG1_deutsch_042019.pdf].].

White Paper 2020 expands on the two previous White Papers for the purpose of formulating a general, yet unique, structure for the digital safety representation of an asset (machine or components). In addition, it identifies the additional steps required to ensure interoperability between machines and components in a heterogeneous landscape and to evaluate the danger (e.g., the resulting risk) and implement countermeasures using Smart Safety Agents. This White Paper summarizes the current findings of the working group regarding modular machine safety.

# 2. Introduction

The demand for modular plants and machines and the associated challenges are increasing, driven by smaller production lot sizes and the need to react flexibly to fluctuating market requirements.

The machines and components in a Plug & Produce scenario at a modular plant must be able to communicate smoothly with each other. If the components or modular machines are from a single manufacturer, this communication between them can be taken into account during the development phase of the system. In this case, the setup is quite simple, i.e., the concept of interaction is considered in the development/design engineering phase, which simplifies the later configuration effort. In a manufacturing environment with a variety of machine or unit types, however, it may be necessary for the manufacturers of the plants and components to cooperate. Specifically, in smart manufacturing or I4.0 plants where it may not be known what future configuration is required, i.e., what type of machines will have to work together in the future, comprehensive, manufacturer-independent interoperability is essential.

Modular plants much like conventional systems must comply with relevant safety guidance. If changes to the system are required during operation, the change must be subjected to a new safety assessment. Especially, in the case of frequent setup changes, the "down time" for the new safety assessments can add up to the point where the time and cost of manual testing and assessment can significantly reduce the advantages of modular plants.

Whenever components are exchanged or different machine systems are added in a modular plant, the safety assessment must be conducted at a level of technology that permits a technical safety certification to be determined and the corresponding release to be issued.

# 3. Digital Machine Representation of a Machine

The design related work on modular and interchangeable plants systems often requires the use of terms like cyber-physical production systems (CPPS), ***SmartFactory***[KL], digital twin, Internet of Things, digital shadow, etc. Yet, in such a production environment, the basic idea is always the same, i.e., to use the advantages of digital machine representations in manufacturing to provide more flexibility and greater efficiencies.

Another important term used in relation to the communications in modular systems and their digital twins is the asset administration shell (AAS). The concept of the Asset Administration Shell (AAS) was first introduced in DIN SPEC 91345: Reference Architecture Model Industrie 4.0. The asset administraion shell can represent a component, an entire system, or a combination of systems. A description of the structure of the asset administration shell is found in IEC 62832 – Digital Factory Framework. In general, the asset administration shell contains a set of assets (components or machines) that share common data elements and derive from one or more asset definitions. An asset administration shell consists of a general part that holds identification information and it may also contain multiple sub-models, each representing specific aspects in the AAS (see earlier distinction between "header" and "body").

The characteristic properties of the asset under consideration are stored in specific sub-models, which can also be used to store requirements that the asset must satisfy.

According to DIN SPEC 91345, when developing modular components or machines, the characteristic type-specific properties of the asset can be stored in a so called type-asset administration shell. The owner of a type-asset administration shell can also adapt it at a later time (update), for a machine that is already on the market.

The so called instance-asset administration shell references the type-asset administration shell. In this way, individual components and machines can always remain current [1]. Updates may be necessary, for example, when a software update expands the functional range of a component. Care should be exercised to ensure that the update, i.e., downloading and installing an update to the instance-asset administration shell of an individual component or machine, does not affect the real-time behavior of the machine or plant. The system must always remain capable of transmitting an alarm, reacting immediately to failures, and ensuring plant safety at all times. In this context, the aspect of cyber security takes on particular significance.

The "SecureSafety" approach effectively combines the coordination of safety and cyber security throughout the life cycle. It is advisable to check the IEC 62443 family of norms, supplemented by IEC TR 63069 to account for the above mentioned aspects and comply with the cybersecurity requirements of DIN SPEC 91345 6.1.6 and other requirements discussed in more detail below.

In addition to safety considerations when updating an instance-asset administration shell, it is necessary to ensure that the production machinery is always capable of meeting the operator's operational requirements. Clearly, cyber security efforts are required from both the manufacturer and operator because, in a cyber security assessment, not just safety aspects are evaluated. For example, in the event of a cyber-attack, plant operations and product quality must not be negatively impacted. These considerations, however, are not the focus of this White Paper and are not addressed in any further detail.

The operators of modular production machinery with associated digitalized internal processes are particularly interested in the part of the asset administration shell that holds the descriptions of the properties and current status of a machine or a component. This information, in combination with the work progress, provides transparency to the operator as well as the potential for increased efficiency. The digitalization of machine safety in addition to the required information for design, production planning, maintenance, etc., stored in the instance-asset administration shell provides the potential for even more efficiency and productivity. A possible concept with decision trees and safety agents was presented in the White Papers 2018

Safety in modularen Industrie 4.0-Produktionsanlagen“ [2] and 2019„Smart Safety "Safety on modular machines" [3]. Now, we must address further steps required for practical implementation.

# 4. Plug&Produce: Requirements for the Digital Representation

The digital representation, i.e., an asset administration shell, stores information associated with a machine or a part of the plant that could be relevant at some later time to a variety of functional problems or the departments of the organization. It would be nice to have the information prepared and linked in a contextual way to the machine. In fact, the framework of the I4.0 platform publication "Asset Administraion Shell in practice" [4] refers to some different approaches to contextual linking, for example, to a data sheet, documentation, the environment, or equipment information.

In addition to the above considerations, digitally stored information associated with a machine prepared according to the following additional proposed approaches can be useful to the operator:

- organizational
- technical, or
- event-dependent

The organizational approach would show the contents of the digital twin or, the administration shell, that is of interest to the individual departments like Purchasing, Design, Production, Maintenance, Facility, Sales, and Logistics, etc. The technicians may be interested in the wiring diagram or the manuals, whereas the purchasing specialists may need the parts lists for ordering spare parts. The production and sales managers, in contrast, are not only interested in static data, but rather more in dynamic data such as production progress.

The technical approach can be broken down into the following categories on the basis of IIC discussions on "Trustworthiness":

- Security
  - Safety
  - Security
  - Data protection

- Operations
  - Reliability
  - Resilience
  - Maintenance expense

When looking at the ends of a decision tree and the tasks of the Risk Reduction Agents discussed in White Paper 2019 „Smart Safety – Safety in Modular Production Processes" [3], it is evident that the hazards must be digitally mapped and made available, so that the danger (e.g., the resulting risk) can be compared with available countermeasures, for example, the transfer gate from a neighboring machine module.

In this context, the event-dependent approach is the most practical since the digital machine representation, i.e., the AAS, may also need information about other areas besides the detailed safety-relevant information. The event-dependent approach which is also discussed in the IIC "Trustworthiness Model" could be sub-divided as shown below:

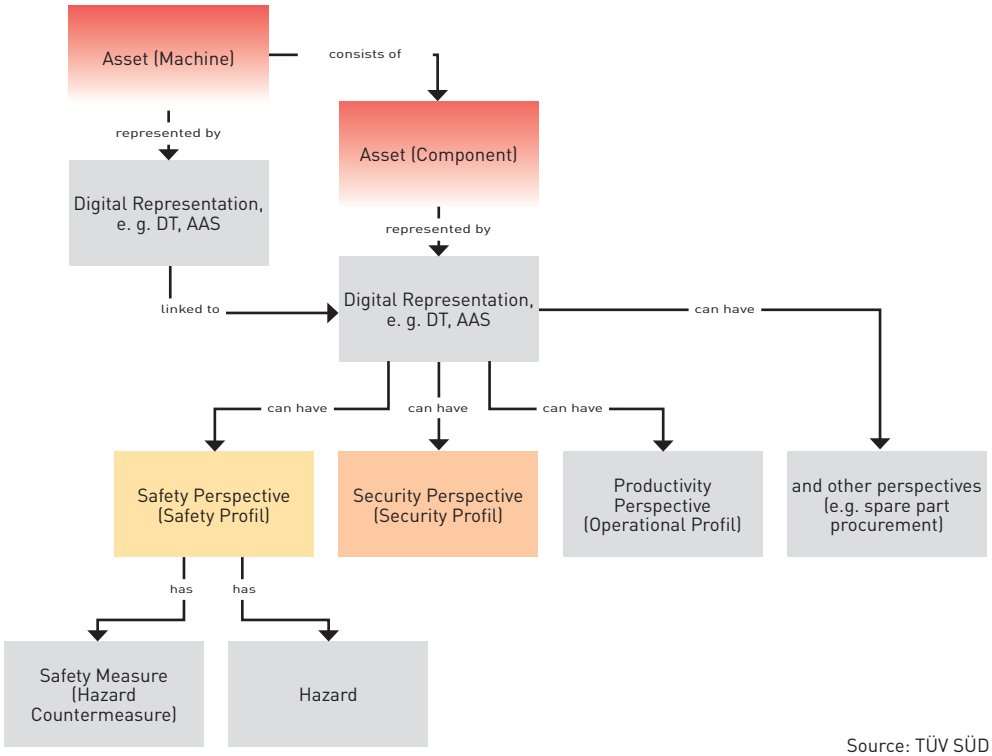
- Safety hazards, according to ISO 12100
- Cyber attacks
- Environmental interference
- Human error
- Technical problem

It should to be noted that the above-mentioned considerations are valid for Plug & Produce, but are equally transferable to other innovative machine safety concepts, as illustrated by the following example of **dynamic machine safety**:

In the case of a plasma cutting machine, toxic fumes may arise when processing certain materials. A failure of the extraction system would result in the process being interrupted and the workpiece ultimately being ejected as scrap. This means losses are incurred by the operator in the form of working time and material. In this thought experiment, knowing that there are no humans present and the cutting process is close to completion, we can assume that if the extraction system were to fail in combination with the command "Ventilate room," no unacceptable amount of toxic gas will accumulate. Clearly, a dynamic machine safety design can improve productivity. If only the conventional functional safety were active when such a technical malfunction occurs and in the absence of environmental information, the machine would be shut down in a safety-oriented procedure.

In light of the various terms in use and the above-mentioned approaches, unambiguous use becomes an explicit imperative. The "Safety hazard" approach for an asset would list the specific individual dangers or instance-risks associated with this asset. In the context of machine safety assessments (see White Paper 2019 "Smart Safety – Safety in Modular Production Processes" [3]), the individual hazard or risk is evaluated and paired with a countermeasure with the help of a "Risk Reduction Agent."

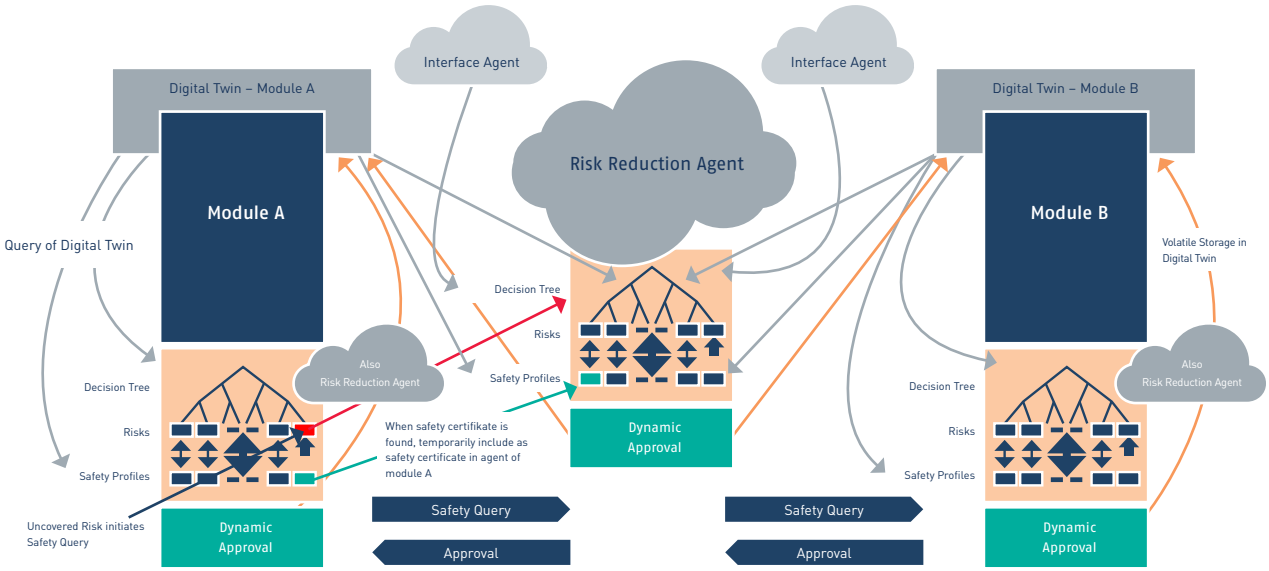
Analyzing the digital machine representation while considering the technical approach as well as the (instance) countermeasures and (instance) hazards for the asset of a machine consisting of different components results in the following relationship diagram:



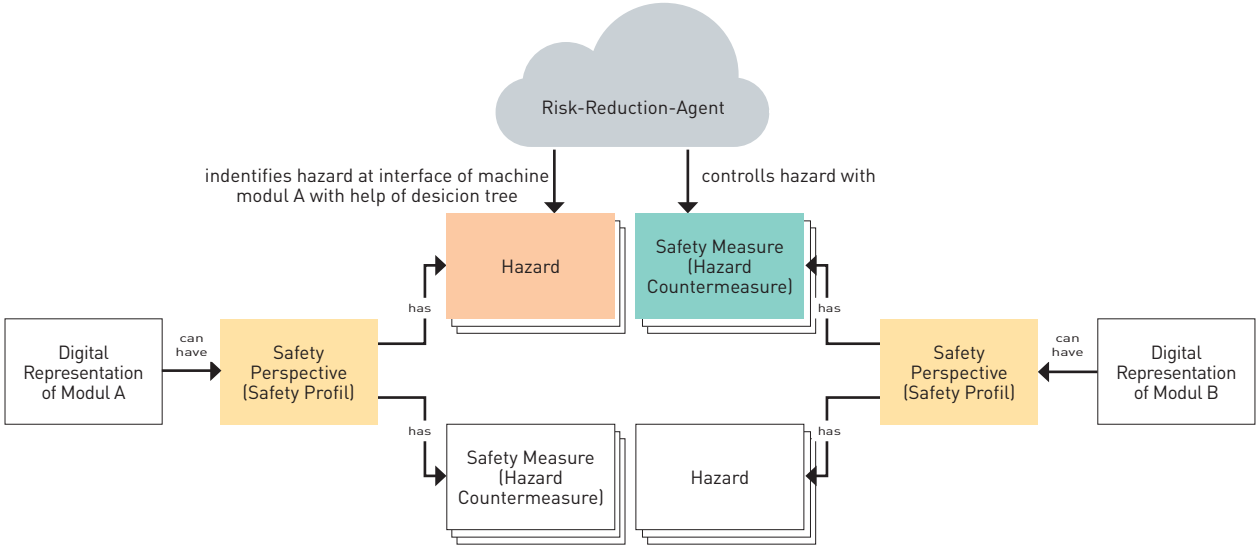

Source: TÜV SÜD

The modular design enables the simple digital exchange of machine components and the automatic update of the hazards and countermeasures associated with the machine. This is a key functionality, because the risk situation of a machine can change when a component is replaced by a component of a different type. For example, if the spindle in the spindle drive of a lathe is exchanged for a more powerful model, the higher maximum speed creates a different hazard situation potentially with regard to parts being spun off.

The following figure shows how the structure introduced in this White Paper fits into the already familiar concept discussed in White Paper 2019 "Smart Safety – Safety in Modular Production Processes" [3]:



The "Risk Reduction Agent" as introduced in White Paper 2019, “Smart Safety – Safety in Modular Production Processes” [3], has the job of monitoring the safety of the machinery. This requires the definition and standardization of the way in which a countermeasure or a hazard is digitally represented. The following discussion makes it clear that simply comparing a danger (e.g., the resulting risk) with a countermeasure is not sufficient to meet the demand for fault-free production. A functioning "Risk Reduction Agent" alone is not enough.




This identifies a need to describe functionally expanded agents, namely "Smart Safety Agents."

As part of the safety profile (or safety sub-model), the digital description of the countermeasure could include the following aspects, to include important links to other profiles or sub-models, e.g., "Operations." (The following examples are merely a source for discussion and further development in the future; the list is by no means a complete one).

- Type of component, e.g., emergency stop button, transfer gate
- Status, e.g., open, closed, etc.
- Countermeasure classifications , e.g., collision avoidance, covers, etc.
- Countermeasure properties, e.g., mesh size of a separating divider or braking dis-tance, etc.
- Spatial coordinates of the countermeasure or safety component, e.g., relative to the machine
- Spatial dimensions, e.g., dimension of the door opening
- Availability requirements, e.g., availability of hydraulics or pneumatics
- Reliability level (performance level for mechanical parts)
- Cyber security requirements:
  - Confidentiality, integrity, and availability
  - Function of the severity of the damage
- Operational Index (impact of the countermeasure on process flow/ productivity)
- Maintenance Index (impact of the countermeasure on maintenance)

While most of the parameters are self-explanatory for people familiar with safety, aspects like "operational index" or "maintenance index" appear to need further clarification. For example, assume two possible countermeasures are available in a specific situation and both are considered equivalent, but only one is required. The choice of which one to apply should not be random. The countermeasure that should be used is the one that has the least negative influence on productivity and incurs the lower maintenance costs. A comparison of a safety light curtain and a transfer gate can be useful. As a rule, the light curtain has less impact on the time flow of production process than the transfer gate, which requires more time to open and close than switching on a light curtain.

Similar to the countermeasures, the hazard must be present in the digital representation, i.e., a description of the individual hazards in terms of type, location, effective direction, spatial and temporal characteristics, and amount for example, energy content [J], etc. However, repeating the hazards as listed in EN ISO 12100 (e.g., acceleration, rotating parts, voltage) is also insufficient; a meaningful grouping of hazards is needed to make the dangers machine readable and enable the Smart Safety Agent to compare a countermeasure with a specific hazard (e.g., the resulting risk). Specifically, a language is needed (safety-semantics) to describe the problem that is creating the hazard. Without standardized safety semantics, the Smart Safety Agent is not able to determine a match between the hazard and an appropriate countermeasure.

---

Comment: It is not within the scope or purpose of this example to show how to implement a certain safe distance, but rather to consider the ability to compare a countermeasure with a danger..

In another example, the risks from machine motion or from the flame of a torch welder could be managed either with a separating divider (e.g., a closed transfer gate) or by a safe distance between the hazard and the human being. Either of these countermeasures could solve the problem. From a manufacturing perspective, there are different advantages to leaving the transfer gate open and the establishment of a safe distance. This implies that the Smart Safety Agent must be able to understand that both countermeasures are applicable to the hazard being controlled. To perform this type of comparison, the computer needs an appropriate grouping of the hazards. Hazards could be grouped according to the underlying problem. In this example, that would be a collision or contact between the dangerous part of the machine (motion or flame) and a human being during operation and safety demands that there will be none. This hazard grouping (part of safety semantics) must be standardized to ensure interoperability and safe operations.

In summary, consider an AGV (Autonomous guided vehicle (AGV)) that has the countermeasures "Stop," "Change route," or "Lane request" available to react to a collision hazard or friction contact hazard, etc. (problem behind the hazard: "prevent contact"). The action "lane request" is only useful in connection with machines (e.g., entrance doors) that are capable of providing an answer. In this example, the Smart Safety Agent proposes a new route before the AGV enters the intersection that is currently heavily frequented by pedestrians and where it would be stopped by colllision detection sensors. The current, commonly used "standstill" countermeasure is replaced by "safety distance" and implemented by using an alternate routing. As a technical safety function, the collision detection feature remains active and available as a "fall back" position.

The Smart Safety Agent represents an extension of today's safety functions, i.e., the Smart Safety approach as described in this white paper is a multi-level concept. The lowest level, the "fall back" position in our example, contains only the known functional safety and from there provides additional independent, expanded safety functions at higher levels. This design enables increased efficiency and higher productivity in plant operations.

# 5. Safety–Informationsmodel

The structure derived above is based on the ability to process safety-relevant properties and parameters, e.g. the modular changes in a plant or a machine. This is seen as a requirement for a generic information model and is further described briefly below:

The basic data for the **safety sub-model** of an asset administration shell takes the form of an information model with content as derived above, i.e., the countermeasures and the hazards. The information model for the hazards (internal and external, e.g., mechanical hazards, electrical hazards, etc. (see DIN EN ISO 12100) would look similar to the information model of the countermeasures.

What content is required for a **safety layer**?

A safety layer must be clearly assigned to an asset, i.e., a plant system, machine, or component. This is implemented using a sub-module in the respective asset administration shell. The safety layer sub-model refers to its own, uniquely assigned reference-ID and is described as "idShort = Safety_Layer." The individual safety-relevant profiles can be integrated using "Properties" in the safety layer sub-module. In the case of modular systems, since the value of the safety profile is checked during runtime and changed if necessary, the category "Variable" properties is used. By implication, the AAS of that module must also provide read privileges to other modules. The sub-models are then referenced from the appropriate links (references) in the type-asset administration shell. In the context of Industrie 4.0, IEC 61499 provides a standardized modeling language and architecture for distributed control systems [5]. In addition to property variables, the sub-model can also contain executable operations such as a readiness test or actions for risk reduction/avoidance.

As discussed above, the exchange of safety engineering profiles in modular plants is necessary to understand whether all safety engineering functions are effective and working properly when combined in the plant. A semantic such as "eCl@ss" is required for the exchange and shared understanding among the digital representations systems. A multitude of products and services is already accessible today by means of standardized characteristics and product class master data. Furthermore, IEC 61360 and ISO 13584 contain standard data element types and the corresponding classification scheme, which can be used for a semantic description of the AAS.

## *Literatur:*


[1] Platform Industrie 4.0: Part 1 – The exchange of information between partners in the value chain of Industrie 4.0 (Version 2.0), Federal Ministry for Economic Affairs and Energy (BMWi), 2019

[2] Technologie-Initiative ***SmartFactory***$^{KL}$ e.V., Safety an modularen Maschinen; Whitepaper SF-3.1: 04/2018

[3] Technologie-Initiative ***SmartFactory***$^{KL}$ e.V., Smart Safety – Sicherheit in modularen Produktionsprozessen; Whitepaper SF-3.2: 04/2019

[4] M. Wenger, T. Müller, Connecting PLCs with their Asset Administration Shell for Automatic Device Configuration, IEEE 16th International Conference on Industrial Informatics (INDIN), 2018

[5] Plattform Industrie 4.0: Diskussionspapier Verwaltungsschale in der Praxis https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/2019-verwaltungsschale-in-der-praxis.pdf?__blob=publicationFile&v=11

**Version history**
Whitepaper SF-3.3: 09/2020

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

**T** +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
**T** +49 (0)631 20575-5237
**M** achim.wagner@smartfactory.de