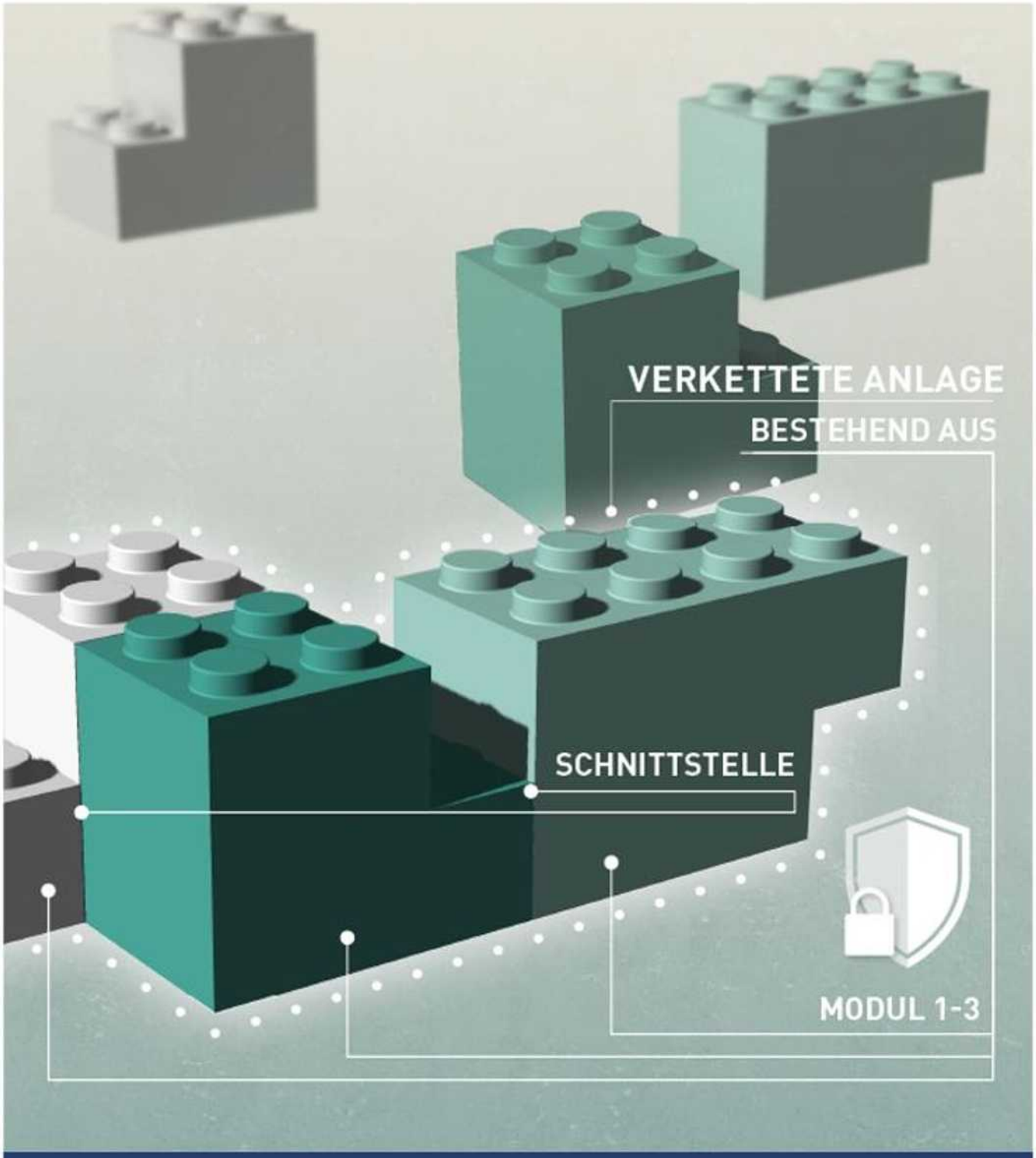

Smart Safety – Safety in Modular Production Processes

Whitepaper SF-3.2: 04/2019

smartFactory KL

SmartFactory^{KL} Whitepaper SF-3.2: 04/2019

SmartSafety – Safety in modular production processes

Abstract

SmartFactory^{KL} Working Group 1 "Smart Infrastructure" addresses the topic of safety in modular Industrie 4.0 production plants.

Even today, the basic principle of functional safety is risk reduction, not the definite exclusion of all possible risk. The use of safety agent systems does not violate this concept. In contrast, it represents the possibility to detect unknown risks and initiate the appropriate responses.

Using the descriptions of safe profiles defined and stored within the administrative shell (cf. DIN SPEC 91345), a sub- concept was developed that enables modular certification of machine groups. Expanding on these improvements, the existing concept has been upgraded.

Keywords

Safety, Industrie 4.0, automated certification

Authors

Hagen Burchardt	Bosch Rexroth AG
Marco Sprenger	B&R
Steffen Horn	Phoenix Contact Electronics GmbH
Joachim Merx	Pilz GmbH & Co. KG
Simon Schönhar	Pilz GmbH & Co. KG
Marius Blügel	Technologie-Initiative SmartFactory KL e.V.
Tobias Thielen	Technologie-Initiative SmartFactory KL e.V.
Dr. Detlev Richter	TÜV SÜD Product Service GmbH
Werner Varro	TÜV SÜD Product Service GmbH
Enrico Seidel	TÜV SÜD Product Service GmbH
Michael Pfeifer	TÜV SÜD Industrie Service GmbH
Pascal Staub-Lang	TÜV SÜD Industrie Service GmbH

Inhaltsverzeichnis

1. Purpose of the Whitepaper

This white paper summarizes the current findings of the working group for safety in module machines. In cooperation with participating partners Bosch Rexroth, B&R, Festo, Phoenix Contact, Pilz, and TÜV Süd, a concept for a simplified, automated partial or full certification was developed and released at Hannover Messe 2018 [Link to White Paper 2018]. Using the descriptions of safe profiles defined and stored within the administrative shell (cf. DIN SPEC 91345), a sub- concept has been developed that enables the modular certification of machine groups. Expanding on these improvements, the existing concept of safety inspection of module machines is upgraded by several levels. The goal is to define and use application-dependent certified software to demonstrate how the complexity of linked interfaces can be reduced to manageable levels.

2. Motivation

After referencing the extensive discussions in White Paper HM18 in our introduction, it is appropriate to express the need for a new approach to machine safety in the age of Industrie 4.0. The research and application development at *SmartFactory*^{KL} over the past several years has shown how the ongoing digitalization of production processes will fundamentally change manufacturing and society in general. In this context, the scenarios "Plug'n'Produce" and "Manufacturing Lot Size 1" serve to illustrate the topics of "modularity" and "flexibility," while also proving their necessity in a competitive economy. However, by looking at just these two use cases, it becomes clear that the digital transformation of production, in terms of cyber-physical production systems (CPPS), increases the complexity of the applications to a barely manageable level. Today, this is already producing a conflict between automation systems and safety technologies. The aim of modern automation systems is by no means restricted to the mechanization and autonomous control of static processes; rather it is about flexible responses to changing requirements and being able to map highly dynamic processes. In contrast, the aim of modern safety technologies is to protect the owners and operators of the means of production by analyzing defined processes and validating them through static solutions.

The Safety Working Group at *SmartFactory*^{KL} accepts the challenge of analyzing these conflicting objectives and finding ways to adequately support the evaluation of complex safety-related relationships using the current technologies and the given semantics. To this end, a framework has been set up for the safe and extensive use of adaptive automation software within dynamic processes.

This paper uses the general term "Smart Safety Automation" for a target system that illustrates the conflict between conventional automation systems and modern safety technologies. Based on that term, the Safety WG's concept is developed as an approach to the resolution of these conflicting objectives. This concept explicitly shows the need for a uniform safety protocol and standard semantics. The description of "Smart Safety Automation" is based on an implementation at *SmartFactory*^{KL}.

3. Theory

3.1 System theory view of Industrie 4.0 systems

Industrie 4.0 plants already have the properties of complex systems: agent-based[1], non-linear, capable of self-regulation, exhibit emergent and global interactions, open for material transport, and show path dependencies [cf. WIKI19]. The classification of Industrie 4.0 systems is explained below on the basis of *SmartFactory*^{KL}: Although the modules with their complexity are still manageable and can be fully described, complex interactions and non-linear fault behavior can occur between the individual modules during combined operations. If the autonomous guided vehicle system currently employed is also considered, the result is a complex adaptive agent system[2] [STÜTT02]. During runtime these are considered systems of systems and from a safety perspective are characterized by high dynamics and flexibility. The resulting uncertainties in system behavior are in direct contradiction to the classical safety verification guidance, which is based on the assumption of a deterministic, predictable system behavior [LIGG17]. Consequently, a conformity assessment of a complex Industrie 4.0 system is only possible for subsystems at the time of delivery to the operator.

3.2 Industry status quo

The safety white paper 3.1 [SF18] describes in detail the status quo in the industry and points out the difficulties related to frequent system changes while taking into account the requirements of the EU Machine Directive.

Recall that in practice, a safety assessment must be made whenever the configuration of a machine group changes. All possible versions/configurations must be considered, evaluated, and validated to enable modularity in today's manufacturing plants, for example, production stations.

1 Definition of agent according to VDI/VDE 2653, sheet 1: "definable (hardware and/or software) unit with defined→purposes related to control of a technical system (of a part, if applicable)"

2 Definition of agent system according to VDI/VDE 2653, sheet 1: "Number of →agents, that interact to accomplish one or more tasks together"

This assumes the safety properties of all modules are known and the process as well as the results have been documented and validated by the responsible person. This procedure is only partially effective for modular I4.0 plants. The constantly changing technologies and the requirement for lot size 1, make it impossible to estimate in advance which system configurations will be needed in the future.

3.3 The use of safety agent systems in manufacturing

Agent systems have to be considered as a means to overcome the major problems in the safety aspects of today's adaptable systems. Because of their ability to learn from unknown data, such methods enable machines to adapt rather flexibly to their cooperation partners and carry out processes together.

The use of agent systems in automation engineering is not new. For example, twelve different cases for the use of agent systems in automation engineering are introduced in VDI/VDE, 2653 sheet 3. Explicit reference is even made to modular production plants. Every module in the *SmartFactory*^{KL} has dedicated controls designed to carry out defined production steps using the parameters communicated by the product. The use of agent systems is based on the evolving requirements discussed in Chapter 2 and [White Paper HM18]. Agent systems have the advantage of a conceptual division of objectives, functionalities, and decision-making processes down to autonomous units, which enables a systematic and simple decomposition of the complexity in the development of distributed automation systems. When knowledge about the problem definition is integrated into the agents by means of targets, the place of the decision is moved to the place where the most data about the problem exists. In some cases, this data is first generated by the interactions of various agents, which means a high degree of flexibility and self-organization can be achieved during operation of a technical system. In agent-oriented development, it is not necessary to know all possible processes when designing the system. The major properties of the overall behavior are first incorporated in the agent system at runtime [VDI/VDE 2653, sheet 1].

However, there are reservations about the use of such methods in the field of machine safety, for example, from a standardization perspective. An example of this is IEC 61508, the cross-industry standard for safety requirements for electrically or electronically programmable safety systems. Part 7 declares artificial intelligence methods and dynamic reconfiguration for SIL 2 to 4 as "expressly not recommended." When using a specific agent system for the first time in a safety program, a sound verification and extensive validation is required from the start of safety planning.

The areas of tension between safety and Industrie 4.0 are not limited to IEC 61508 and the use of intelligent methods. The traditional means of meeting the provisions of Machine Directive 2006/42/EG must also be questioned. Clearly, with the frequently changing plant configurations of the production line, the amount of time for printing, signing, and manual archiving of conformity declarations is no longer insignificant and, in the age of Industrie 4.0, digital signatures, and secure online identification processes are no longer timely. The Machine Directive does not explicit-

ly require a paper form of the conformity declaration, rather only that a signed original be presented.

The purpose of the following section is to present a safety approach for flexible, modular Industrie 4.0 plants. The strict and formal interpretation of the existing standards is intentionally omitted, while the effort is made to implement the underlying intent of the existing standards using intelligent systems against the background of the demanding requirements described.

4 Smart Safety - Safety in modular production processes

The following approach is divided into three sub-areas. First, a basic risk assessment (cf. White Paper HM 2018) using decision trees is explained for a single Industrie 4.0 module of the *SmartFactory*[KL]. The discussion then turns to the use of risk reduction agents at the module interfaces, also using defined decision trees to validate the safety of the interfaces to the linked systems. Finally, the different data sources required for a comprehensive safety validation are discussed.

The following graphic depicts the approach:

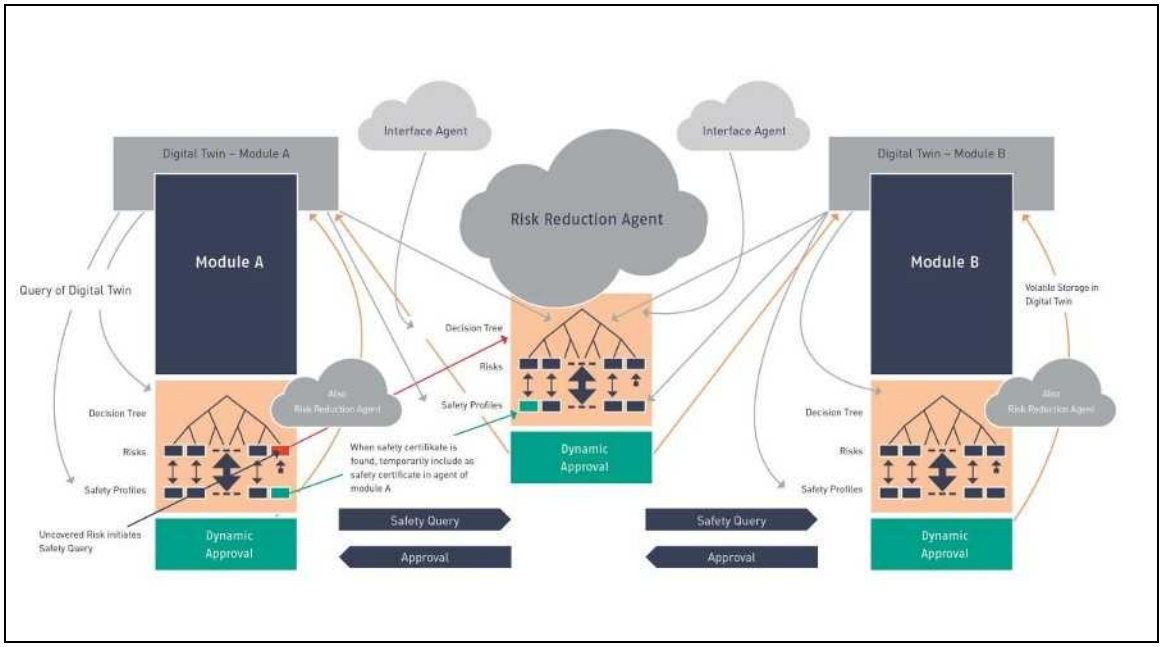

Figure 1: Smart Safety - Risk reduction agents

4.1 Implementing a dynamic approval for individual modules

As stated, the prime goal of safety was originally to protect people, yet this is increasingly being replaced by a complex system of goals. The thought process for this system includes goals such as "maximum availability" or "no departure from system boundaries" in addition to the prime goal, which states "no harm to people". A dynamic approach is now imperative for the optimization of the system because some of these new goals often conflict with the primary safety objective. One possibility to make the dynamics of modular production plants more manageable is to use decision trees as the basis for intelligent basic risk assessments during runtime.

In this case, a decision tree that includes every possible safety condition based on predefined parameter ranges is required for each module. The manufacturer must define these parameter ranges in the design phase and store them as non-editable files. Any operation of the module outside the defined parameter range leads to the immediate disable command and the shutdown of the machine. The connection of all process-relevant parameter ranges in a decision tree quickly leads to great complexity, which makes it necessary to employ expert software for the development of these decision trees. First, the expert knowledge about the safety queries required for the identification of risk potential must be recorded and automated, and then added to the paths defined by the parameter ranges. The end nodes of a decision tree represent the possible risks in each process parameter. If a path has an end node with an intolerable residual risk, the existing safety profile (cf. Whitepaper HM18) must be consulted and confronted with the risk with the aid of risk reduction agents. If the safety features stored in the safety profile correspond to the Safety Integrity Level (SIL) indicated for the residual risk, a release can be enabled at runtime. In the case of the safety features being inadequate or if a certain risk is not covered in a safety profile, the release is disabled for those parameter settings. According to White Paper HM18, a release that is generated and then disabled is safely stored for future use. The decision trees mentioned here can be completely defined by the manufacturer and supplied to the owner/operator. This enables the operator to realize lot size 1 manufacturing with previously unknown processes without violating the provisions of worker safety laws. The expert software for accessing the decision trees must be built in such a way that after an unsuccessful automated risk assessment, a safety expert can be authorized to perform a manual reassessment.

4.2 The use of risk reduction agents at the module interfaces

The interfaces between production stations are subject to other constraints. At this point, it is necessary to develop standard decision trees for the various sectors that can draw on the decision trees of the modules themselves. The parameter settings of the individual modules are not considered, but only the risk identified at the interfaces between modules. As a rule, these risks correspond to the nodes of the decision tree for the individual module and no safety profile of the respective module is available. A problem arises when environmental conditions exist that were unknown to the module manufacturer. Instead of the definition of some intended use, an attempt is made to facilitate the determination of a safe networked system through a combination of dy-

namic releases of individual modules and a dynamic interface assessment. Because of the unknown environment, the proposal suggests evaluating the condition-dependent risks in the modules as well as at the interfaces between modules by means of additional interface risk reduction agents. These can be defined by the machine manufacturer and can eliminate the need to have a safety profile on file for certain conditions (cf. Chapter 5).

4.3 Data sources and semantics of risk reduction agents

The data required for a validation comes from several data sources. First, each CPPS must have a digital twin[3] in its administrative shell for storing process and safety data. This ensures the manufacturer's defined parameter ranges as well as the safety profiles are available. The manufacturer must also define the risk reduction agents for dynamic release in the development phase. In this way, all possible risks are defined with SI level and integrated in the decision tree. Enabling communications with the different risk-reduction agents requires that the possible risks and the safety profiles also be semantically defined. Manufacturer-independent semantics need to be created for this purpose that allow the manufacturer to refer back to the nodes of the decision tree. The interface agents described in Chapter 4.2 serve as an additional database for the interactions within the environment that were not known during development. The output from these interface risk reduction agents can be compared to those risks that have no valid safety profile stored within the module.

5 Use-Case SmartFactory^{KL}

To illustrate the SmartSafety concept within S*martFactory*^{KL}, the following use case is helpful:

5.1 Use case description within SmartFactory^{KL}

As described in articles for HM18, S*martFactory*^{KL} uses an autonomous guided vehicle transport system (AGV) called "Robotino" to transport the work pieces between the various production stations. This use case describes the interaction of the AGV with the docking station and the interaction between the docking station and an adjacent production station, the "spring module". In the context of the white paper for HM18, all modules are considered inherently safe. As shown at the 2018 industry fair, the AGV is dynamically assigned to the emergency circuit of the line in its next immediate proximity. This use case expands on this to describe how the safety-related verification of the interaction between AGVs and docking stations can be carried out using the concept described in Chapter 4.

[3] Explaining the role of the digital twin: This is a digital representation of the machine with cinematic descriptions/ functions. The administrative shell contains the digital twin plus additional data, for example, the documents required under the Machine Directive.

5.2 Dynamic approval for the spring module

The following parameter range is used for simplicity within the spring module:

- "Speed of axial robots"
  - 0-4 m/s
- "Conveyor speed"
  - 0-2 m/s
- "Status of the transfer gate"
  - "open" vs. "closed"
- "Status of the safety door"
  - "closed" vs. "open"
- "Status of the safety door lock"
  - "enabled" vs. "disabled"

The parameter ranges are stored in the "spring module" digital twin and updated on the basis of real-time events. They serve as a database for the "spring module" risk reduction agent. The decision tree executed within the agent would appear as shown in Figure:

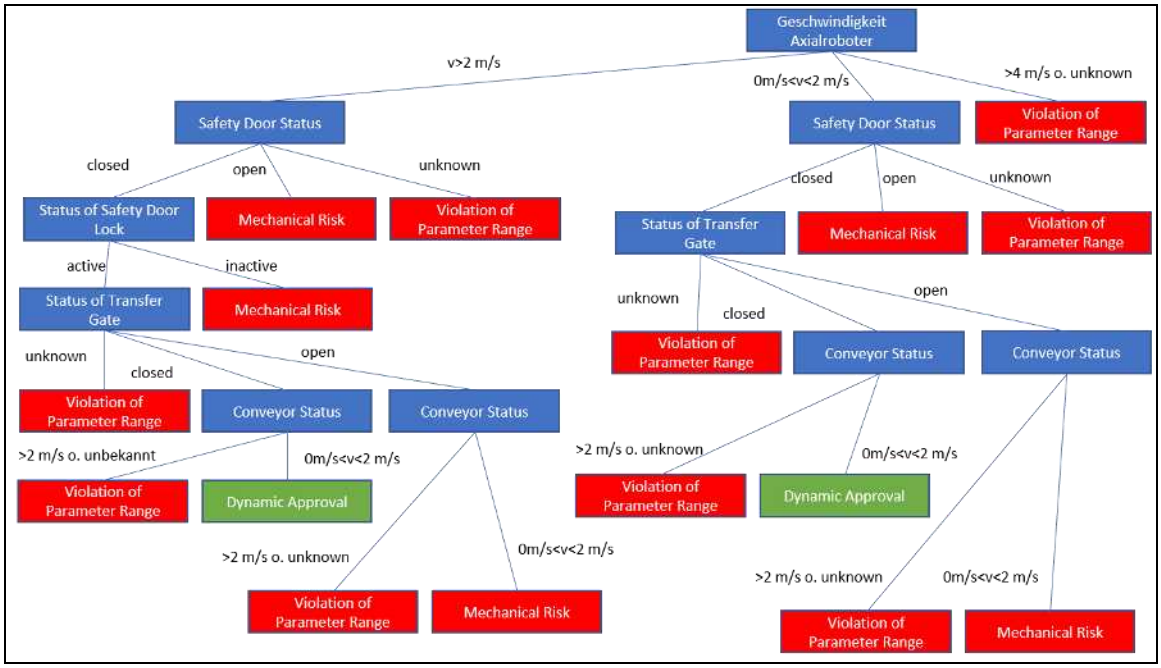

Figure2: Spring module decision tree

As shown by the decision tree, there are only two parameter configurations in which the module can be safely operated. Any violation of the parameter range as described in Chapter 4 leads to an immediate failure in the dynamic approval. If the decision tree ends in a risk due to an interaction with the environment, it is possible that this risk can be eliminated with the help of a dynamic interface certificate.

5.3 Dynamic approval of the docking station

The docking station has two opposing conveyor belts to either move the work piece carrier from the adjacent station to the end of the production line or from the end of the production line to the adjacent station. The belts are designed to move the work piece carrier in one direction only. A sensor at the end of each conveyor belt detects the arrival or departure of the work piece carrier. The following parameter range is used for simplicity within the spring module:

- "Conveyor speed"
    - 0-2 m/s
- "Work piece detects exit"
    - "Yes" vs. "No"
- "Work piece detects entrance"
    - "Yes" vs. "No"

The decision tree executed within the agent would appear as shown in the figure below:

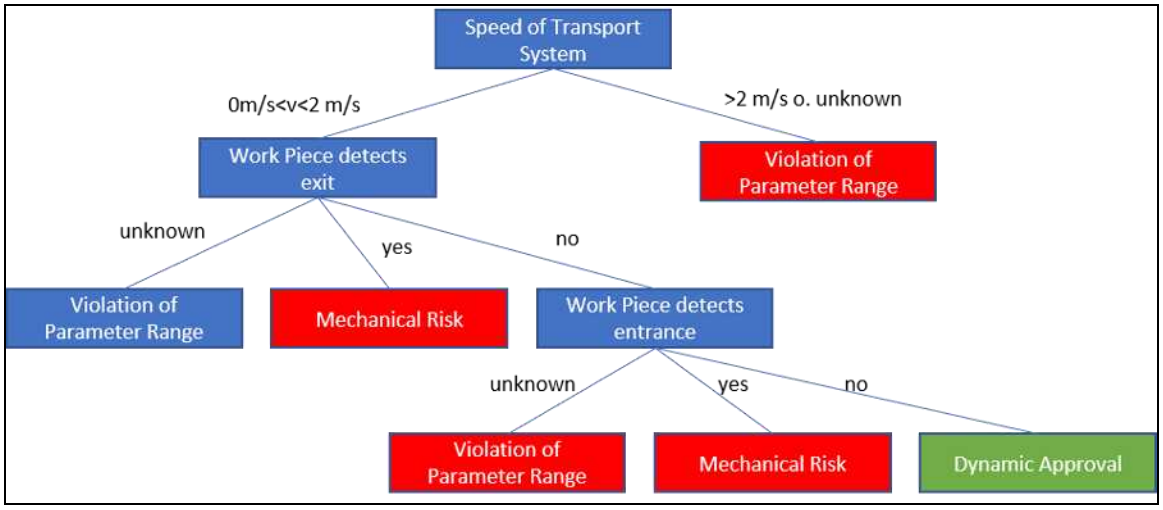

Figure 3: Decision tree - docking station

The operation of the module, in the case, in the form of conveyor belt motion – the docking station is only enabled when no work piece carrier is detected on the belts. For operational purposes, when a single operation of the docking station is not possible, all existing risk is interface risk.

5.4 Dynamic approval of the autonomous guided vehicle transport system

Since AGV operations are essentially designed for the safety of people, we consider only the process-related structure of the AGV system here. This system also consists of two opposing conveyor belts. The conveyor belt is designed for receiving the work piece carrier. At the end of the assembly, the workpiece carrier is re-directed over to the opposing conveyor and is detected by sensors located at the end of the conveyor belt. The parameters are simplified below in contrast to the docking station:

- "Conveyor speed"
    - 0-2 m/s
- "Work piece detects exit"
    - "Yes" vs. "No"

The decision tree would appear as shown below:

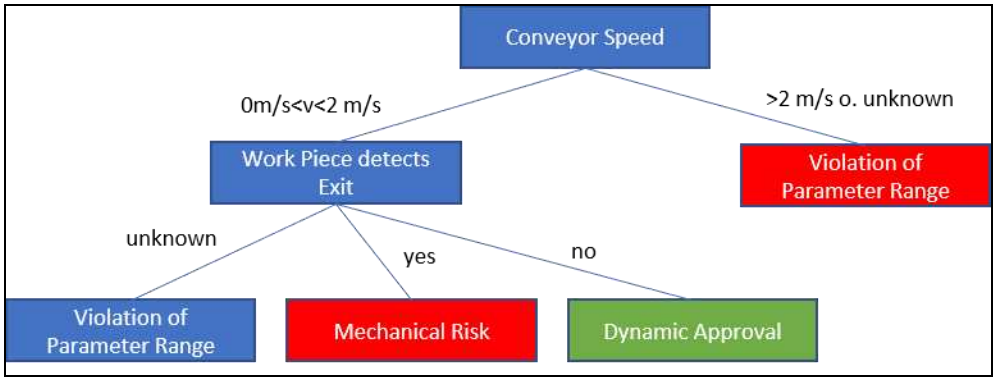

Figure 4: Decision tree - AGV system

Based on the results of the analysis of the docking station decision tree, an approved operation of the conveyor belts of the AGV is only possible for the case when no work piece is being transported. Consequently, for the transport of a work piece, an inspection of the environmental conditions is required.

5.5 Dynamic interface approval

The decision tree for the "spring module" reveals 5 scenarios that can be checked by risk reduction agents. The scenarios are:

- Operation with safety door open and robot speed <2 m/s
- Operation with safety door open and robot speed 0 m/s < v < 4 m/s
- Operation with door lock disabled and robot speed 0 m/s < v < 4 m/s

- Operation with transfer gate open and robot speed 0 m/s < v < 4 m/s and conveyor belt speed 0 m/s < v < 2 m/s
- Operation with transfer gate open and robot speed <2 m/s and conveyor belt speed 0 m/s < v < 2 m/s

The docking station reveals 2 scenarios:

- Operation with work piece detecting entrance with a conveyor belt speed of 0 m/s < v < 2 m/s
- Operation with work piece detecting exit with a conveyor belt speed of 0 m/s < v < 2 m/s

The AGV system reveals the following scenario:

- Work piece detecting exit with a conveyor belt speed of 0 m/s < v < 2 m/s

The tasks of the agent for dynamic interface approval are 1) to assign the risks of the interface that can be seen from the decision trees of the individual modules and 2) to find a parameter configuration in which the detected risk from the interactions with the environment can be eliminated.

5.5.1 "Spring module"/"docking station"

The first interface check relates to the operation of the spring module with the transfer gate open, a conveyor speed of 0 m/s < v < 2 m/s, and a robot speed that conforms to the parameter range, in addition to the operation of the docking station upon detection of a workpiece at the entrance with a conveyor belt speed 0 m/s < v < 2 m/s. The interface agent requires precise information about the mechanical risk and the mechanical structure of both modules.

To ensure a positive interface check in a risk assessment by the risk reduction agent, it is necessary that the design compliance of the conveyor belts as well as the relative speeds are known and checked.

5.5.2 "Docking station"/"AGV system"

The second interface check relates to the operation of the docking station with a work piece detected at the exit and a conveyor belt speed of 0 m/s < v < 2 m/s, in addition to the operation of the AGV with a work piece detected at the at the exit and a conveyor belt speed TRUE initial 0 m/s < v < 2 m/s.

A positive interface check in a risk assessment demands the risk reduction agent check the direction of the conveyor belts in relation to one another. A vision system on the docking station of the AGV checks not only the direction of the conveyor belts, but also checks the orientation of the AGV by means of an environmental recognition system. The approval is then given after a corresponding interface check showed a positive result.

6. Sources

[WIKI19]: https://de.wikipedia.org/wiki/Komplexes_System

[STÜTT02]: Manfred Stüttgen: Komplexe adaptive Systeme - oder: was wir von der Komplexitätstheorie für die Organisation von Unternehmen lernen können. In: Peter Milling (Hrsg.): Entscheiden in komplexen Systemen. Berlin 2002, ISBN 3-428-09365-8, S. 333–348

[LIGG17]: P. Liggesmeyer, M. Trapp, "Safety in der Industrie 4.0: Herausforderungen und Lösungsansätze", in Handbuch Industrie 4.0 Bd.\, 1: Produktion, 2 ed. B. Vogel-Heuser, T. Bauernhansl, M. ten Hompel, Eds., Berlin: Springer, 2017, pp. 107-123.

[SF18]: Safety an modularen Maschinen; Whitepaper SF-3.1: 04/2018

[VDI/VDE 2653 Blatt1]: Agentensysteme in der Automatisierungstechnik - Grundlagen