Flexible Safety Systems for Smart Manufacturing

Dieter Etz[1,2], Thomas Frühwirth[1,2], Wolfgang Kastner[1]
[1]Institute of Computer Engineering, Automation Systems Group, TU Wien
[2]Research Department, Austrian Center of Digital Production, Wien
{dieter.etz, thomas.fruehwirth, wolfgang.kastner}@tuwien.ac.at

***Abstract*—Smart manufacturing is realizing the idea and potential of Industry 4.0 in reality. An essential part of smart manufacturing are production facilities that dynamically adapt to changing production needs. This brings completely new challenges to functional safety systems, which are mandatory for the protection of man, machine, and environment. Currently, functional safety systems are designed and certified in a static way. The safety design and the configuration are derived from the risk assessment which is performed during the design of a machine. Once the system is put into operation, the safety configuration is not changed anymore. This approach constitutes an impediment to flexibility which smart manufacturing production facilities require nowadays.**

This paper proposes the design of a self-organizing safety system with the objective to assist an engineer who operates a smart manufacturing facility by discovering all safety-related devices and generating automatically a suitable safety configuration. This configuration will be deployed to the system automatically after adaptation and validation by the safety engineer. The proposed self-organizing safety system, simplifies the safety configuration in a dynamically changing environment. Consequently, it would reduce engineering efforts and decrease machine downtime which improves profitability.

***Index Terms*—Smart Manufacturing, Industry 4.0, Functional Safety, Interoperability, Flexibility, Real-Time, Unified Communication, OPC UA, TSN**

I. Introduction

The transition from industrial automation (Industry 3.0) to Cyber-Physical Production Systems (Industry 4.0) implies a huge demand for connectivity and interoperability along the whole value chain. Smart manufacturing is realizing the idea and potential of Industry 4.0 in reality. An essential part of smart manufacturing are production facilities that dynamically adapt to changing production needs. This brings completely new challenges to safety systems, which are mandatory for the protection of man, machine, and environment. Factories, in this context, comprised of a heterogeneous array of machines from a multitude of vendors and manufacturers, have very specific demands on flexibility and interoperability which imposes higher requirements on functional-safety-related applications.

The increasing complexity of machinery in smart factories leads to very complex and time-consuming safety configurations. Production facilities in a smart manufacturing environment pose high requirements to flexibility because they have to dynamically adapt to changing production needs. Currently, functional safety systems are designed and certified in a static way. The safety design and the configuration are derived from the risk assessment which is performed during the design of a machine or production line. Once the system is put to operation, the safety configuration is not changed anymore. This approach constitutes an impediment to flexibility which smart manufacturing production facilities require. Automation technology in smart factories, together with high demands for flexibility and interoperability, entails a huge configuration effort of the indispensable safety system. There is an enormous contradiction between existing functional safety systems and the desired flexibility of production facilities.

This paper proposes the design of a self-organizing safety system with the objective to assist an engineer who operates a smart manufacturing facility by discovering all safety-related devices and generating automatically a suitable safety configuration. This configuration will be deployed, after adaptation and validation by the safety engineer, automatically to the system. The proposed self-organizing safety system, simplifies the safety configuration in a dynamically changing environment. Consequently, it reduces engineering efforts and decreases machine downtime which improves profitability.

This work has been partially supported and funded by the Austrian Research Promotion Agency (FFG) via the "Austrian Competence Center for Digital Production" (CDP) under the contract number 854187.

II. Functional Safety

The concept of safety of machinery considers the ability of a machine to perform its intended function(s) during its life cycle where risk has been adequately reduced [1]. Safety is the "freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment", IEC 61508 [2]. Functional safety is defined as the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. It is the detection of a potentially dangerous condition which results in the activation of a protective or corrective device or mechanism in order to prevent hazardous events, which in turn provides mitigation to reduce consequences. This means that functional safety relies on active systems. The behavior of a machine whose failure can result in an immediate increase in risk is described by a safety function. It is a measure taken to reduce the likelihood of an unwanted event occurring and to exposing any potential hazards. The determination of safety functions and their implementation is described in ISO 13849-1 [3] and IEC 62061 [4]. Figure 1 shows an example of a safety function which consists of several Safety-Related Parts of a Control System (SRP/CS). The safety chain comprises the input actuated by opening of the guard (SRP/CS a), the control

978-1-7281-8956-7/20/$31.00 ©2020 IEEE

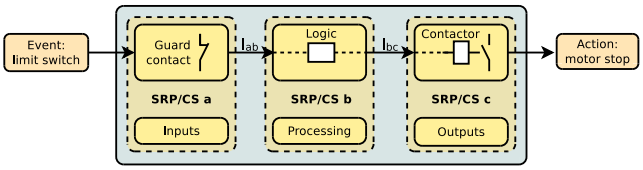

Fig. 1. Safety Function Example

logic (SRP/CS b), the power output that controls a motor (SRP/CS c), and the connections (I_{ab}, I_{bc}) [5].

III. Related Work

The challenges of safety in Industry 4.0 were recognized by Liggesmeyer et al. in [6]. The authors analyzed uncertainties of production systems originating in the central element of Industry 4.0 defined as "network of autonomous, situational self-controlling, self-configuring, knowledge-based, sensor-supported, and spatially distributed production resources". These uncertainties are in conflict with the safety certification process, which expects a deterministic and predictable system behavior. For this reason, safety could easily become a bottleneck in the transition to Industry 4.0 because – despite its high economic potential – innovation must never be at the expense of safety. A concept based on a modular safety verification procedure is proposed.

In his paper "Functional safety and Industrie 4.0", Meany explores some of the implications of functional safety for Industrie 4.0 [7]. The publication explains the design principles of Industry 4.0, such as interoperability, virtualization, decentralization, real-time capability, service orientation, and modularity followed by a short summary of the three important key aspects networking, security, and robots. After that, functional safety is put into context with these three key aspects as well as with software and integrated circuits. The paper addresses the implications and challenges of functional safety in Industry 4.0 without providing further solutions.

While Liggesmeyer et al. and Meany identify the challenges of safety in Industry 4.0 and propose only organizational or conceptual solutions, this paper proposes an assistive technology which actively supports the safe, flexible, and quickly changeable composition of machinery.

IV. Flexible Safety System Design

In order to address the needs of a machine, production line, or smart factory regarding safety, a solution is proposed which provides a self-organizing safety system based on vendor-neutral technologies to ensure interoperability between devices of various manufacturers. The aim is to design a self-organizing safety system based upon existing and vendor-neutral technologies. Data transport as well as unified communication is the foundation for seamless machine-to-machine (M2M) communication. Two vendor-neutral technologies, which are gaining acceptance in the industry, are very promising candidates to serve as communication platform: Time-Sensitive Networking (TSN) and OPC Unified Architecture (OPC UA) including the recently released OPC UA Safety "Part 15 OPC UA Core Specification".

A. Base Technologies

The used technologies should be standardized, vendor-neutral, support interoperability, and industrially mature. Therefore, two candidates where chosen to serve as foundation: Time-Sensitive Networking (TSN) and Open Platform Communications Unified Architecture (OPC UA) [8] [9] [10].

TSN is a set of IEEE 802 Ethernet sub-standards that are defined by the IEEE TSN task group. Each of these standards offers a different set of functionality that can be applied to IEEE 802 networks, including the well-known 802.3 wired Ethernet and 802.11 wireless local area network (WLAN). Standards, such as IEEE 802.1AS-Rev (Timing and Synchronization), IEEE 802.1Qbv (Enhancements for Scheduled Traffic), and IEEE 802.1Qbu (Frame preemption) provide extensions for wired and wireless Ethernet in order to enable deterministic real-time communication [11]. Additionally, a fault-tolerance mechanism called Frame Replication and Elimination for Reliability (FRER) offers highly reliable communication for time-triggered traffic [12].

OPC UA presents a platform independent service-oriented architecture for M2M communication. The components of OPC UA include transport mechanisms, information modeling capabilities, and services. The transport mechanisms support one-to-one, one-to-many, and many-to-many communications. Information modeling defines the rules and building blocks required to expose managed data with OPC UA. Services allow clients to interact with the application and information model on OPC UA servers [13]. OPC UA companion specifications map domain knowledge and concepts to standard models for representation in the OPC UA domain. The specification for the interoperable communication standard for functional safety – OPC UA Safety "Part 15 OPC UA Core Specification" – explains the relevant principles of functional safety for communication with reference to the IEC 61508 series as well as IEC 61784-3 and others and specifies a safety communication layer based on the OPC Unified Architecture. OPC UA Safety supports the assignment of Safety-IDs to machines and allows for dynamically changing the communication partner during runtime. These are prerequisites for modern production processes with batch size one, where machines or machine parts must be re-grouped frequently. OPC UA Safety uses a monitoring number, a timeout, a set of IDs and a cyclic redundancy code for the detection of communication errors which may happen in the underlying OPC UA communication channel. These measures offer a probability of failure per hour (PFH) and a probability of failure on demand (PFD) sufficing to build safety related applications with a safety integrity level of up to SIL4 (IEC 61508) or PL e (ISO 13849-1) [14].

B. Concept

The overview shown in Figure 2 illustrates how a self-organizing safety system can be integrated between different safety domains in order to enable safe communication across domains.

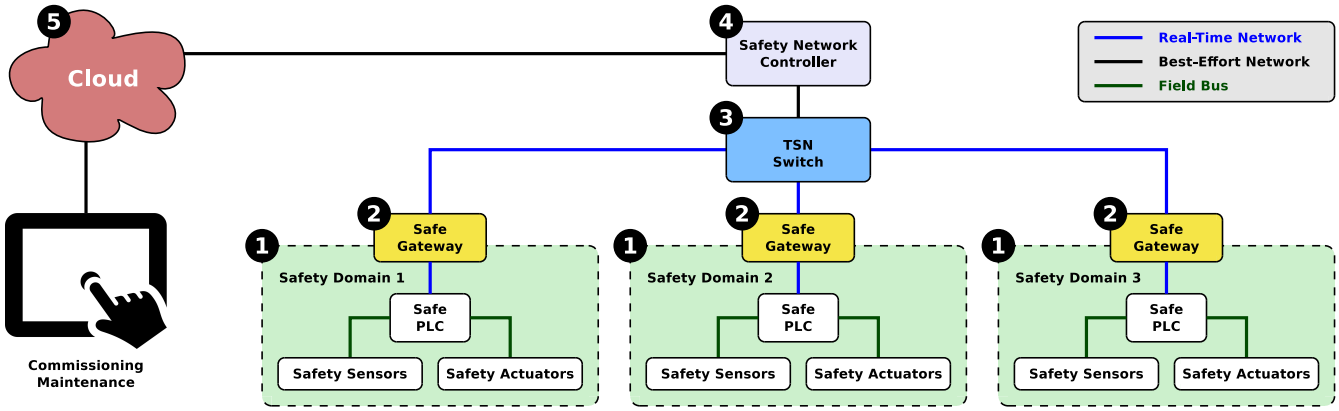

Fig. 2. Self-Organizing Safety System Concept Overview

At the core of the proposed safety system, there are five main components:

1. **Safety Domains** including safety sensors, safety actuators, and safety PLCs.
2. **Safety Gateways** serving as interfaces to different safety domains using 'Safety over OPC UA'.
3. **Data Transport** using TSN as real-time network providing the black channel for safety data transmission.
4. **Safety Network Controller** with the tasks to configure and monitor the TSN network, the OPC UA communication, and the safety configuration in the safety gateways.
5. **Cloud-based user interface** providing the tools for configuration as well as monitoring of the safety network.

Safety-critical applications place high demands on communication and on the underlying data transmission system. Therefore, a combination of three building blocks is used to address these safety specific demands. First, deterministic transport of data is ensured by features of TSN (e.g. IEEE 802.1Qbv traffic scheduling). Second, security will be handled by functionality included in OPC UA, such as application layer security (e.g. authorization, authentication) and Transport Layer Security (TLS) (e.g. UA secure conversation, WS secure conversation). Cloud connectivity for the network controller can be based on several protocols such as Constrained Application Protocol (CoAP), MQ Telemetry Transport (MQTT), or Advanced Message Queuing Protocol (AMPQ). These can be secured using TLS, Datagram Transport Layer Security (DTLS), or Secure Socket Layer SSL. Third, safety related aspects of safe data transmission will be covered by the OPC UA specification 'OPC UA Safety' [14]. The configuration is accomplished using a safety network controller which discovers the safety devices, generates a configuration, and deploys it after acknowledgment from the operator into the system. The deployment includes the configuration of the real-time network as well as the safety configuration. The safety gateways act on one side as a safety endpoint in their safety domain, on the other side they expose certain safety inputs and outputs via the OPC UA information model for external use. This can be compared to a discrete wiring solution where terminals in the control cabinet are prepared for external components (i.e., when the external part is not used, the terminals are short-circuited with a jumper wire). At the safety gateway, an input can be connected to an output (1:n) on a different gateway and vice versa. If an input is not connected it can be short-circuited with a "software jumper". An example for such safety connections is illustrated in Figure 3. This safety connectivity on a software level brings maximum flexibility and enables the operator to change the safety configuration with no hardware or wiring change, even during operation. In the long term, the safety gateway should become no longer necessary as manufacturers of Safety PLCs will integrate OPC UA Safety directly into their devices.

The preparation of a safety connection requires the configuration of the participating safety gateways and the TSN network. These tasks are handled by the safety network controller during configuration deployment. It also includes safety device discovery, configuration generator, configuration validation, and plausibility check.

Fig. 3. Safety Connections

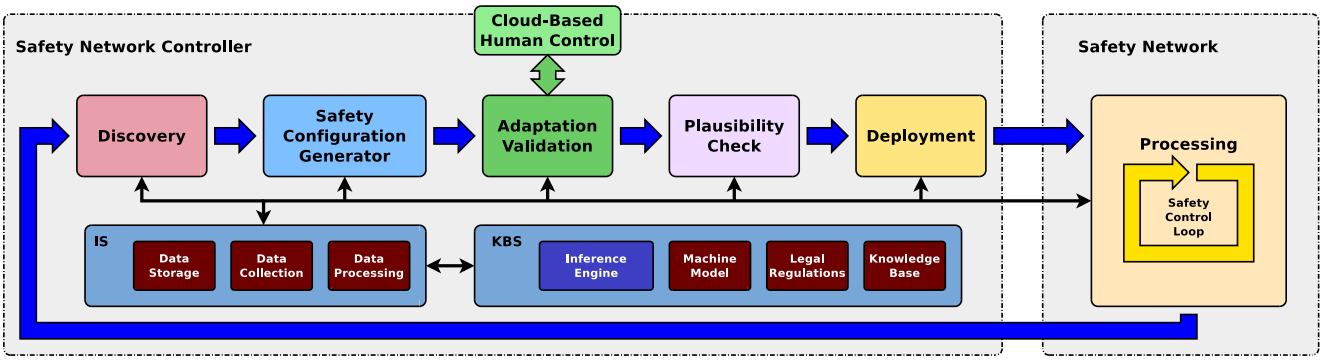

Fig. 4. Self-Organizing Safety System Model

An information system (IS) and a knowledge-based system (KBS) are located at the core of the safety network controller. All other components build on or around these. An IS refers to a collection of components for collecting, transporting, storing, and processing data. A KBS is an application that reasons and uses a knowledge base to solve complex problems. It has two characteristic features which are a knowledge base, a technology used to store complex structured and unstructured information, and an inference engine, a component that applies logical rules to the knowledge base to derive new information.

The self-organizing safety system model illustrated in Figure 4 includes four tools to assist safety engineers: the automatic discovery, the safety configuration generator, the plausibility check, and the deployment. These tools should simplify the workflow and operating process in order to allow quick, efficient, and correct configuration changes.

A functional safety system, which aims at protecting humans and environment, must meet the highest standards, as malfunctions can endanger human lives. Therefore, the self-organizing safety system model includes an adaptation and validation building block with a human control interface and a Human-Machine Interface (HMI). It ensures that a safety configuration can only be deployed if a human verified the completeness and correctness. Furthermore, the HMI allows the user not only to change the safety configuration of the production system but also to monitor and configure the safety network controller.

V. Conclusion and Work-in-Progress

The intention of the proposed safety system is to bring maximum flexibility to smart manufacturing facilities by enabling the operator to change the safety configuration without hardware or wiring change, even during operation. Additionally, the proposed system includes assistive tools such as discovery, configuration generator, and automatic deployment. These tools should simplify the workflow and operating process by relieving the operator from tedious tasks. Therefore, long and costly down times of production lines, due to safety configuration, can be avoided which can consequently help reduce costs and maximize profits.

Currently, the research focus is on the base technology components such as TSN configuration, development of an OPC UA information model, and an analysis of OPC UA safety features. The next steps will be the definition of interfaces between the participating components, followed by a proof-of-concept implementation. Furthermore, it is also envisaged to equip the system with an external interface for Enterprise Resource Planning (ERP) or Manufacturing Execution System (MES) in order to allow safety configuration changes from business process management software.

References

[1] ISO, "Safety of machinery – general principles for design – risk assessment and risk reduction," ISO 12100, 2010. [Online]. Available: https://www.iso.org/standard/51528.html

[2] IEC, "Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC 61508, 2005.

[3] ISO, "Safety of machinery – safety-related parts of control systems – part 1: General principles for design," ISO 13849-1, 2015.

[4] IEC, "Safety of machinery - functional safety of safety-related electrical, electronic and programmable electronic control systems," IEC 62061, 2005.

[5] D. Etz, T. Frühwirth, A. Ismail, and W. Kastner, "Simplifying functional safety communication in modular, heterogeneous production lines," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, June 2018, pp. 1–4.

[6] P. Liggesmeyer and M. Trapp, *Safety in der Industrie 4.0*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 107–123.

[7] T. Meany, "Functional safety and industrie 4.0," in *2017 28th Irish Signals and Systems Conference (ISSC)*, June 2017, pp. 1–7.

[8] D. Bruckner, M. Stanica, R. Blair, S. Schriegel, S. Kehrer, M. Seewald, and T. Sauter, "An introduction to OPC UA TSN for industrial communication systems," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 1121–1131, June 2019.

[9] L. Lo Bello and W. Steiner, "A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 1094–1120, June 2019.

[10] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, March 2017.

[11] W. Steiner, P. G. Peón, M. Gutiérrez, A. Mehmed, G. Rodriguez-Navas, E. Lisova, and F. Pozo, "Next generation real-time networks based on IT technologies," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 2016, pp. 1–8.

[12] M. Pahlevan and R. Obermaisser, "Redundancy management for safety-critical applications with time sensitive networking," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov 2018, pp. 1–7.

[13] W. Mahnke, S.-H. Leitner, and M. Damm, *OPC Unified Architecture*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[14] OPC Foundation and Profibus Nutzerorganisation, "OPC Unified Architecture Part 15: Safety," Industry Standard Specification OPC 10000-15, 10 2019.