Self-Configuring Safety Networks

Dieter Etz[1,2], Thomas Frühwirth[1,2], Wolfgang Kastner[1]

[1]Institute of Computer Engineering
Automation Systems Group
TU Wien
{dieter.etz, thomas.fruehwirth, wolfgang.kastner}@tuwien.ac.at

[2]Research Department
Austrian Center for Digital Production
Wien

Abstract. In the context of Industry 4.0, production lines as part of Cyper-Physical Systems (CPS) have specific demands for interoperability and flexibility. Machinery, being part of these production lines, has additional requirements in terms of functional safety and real-time communications. The re-configuration of functional safety systems, which is characterized by high manual configuration efforts, leads to time-intensive and expensive downtimes. This paper presents the requirements on and the concept of self-configuring safety networks, which reduces the engineering efforts and allows the operator of production lines convenient re-configuration of safety functions and devices. The proposed concept is based on the vendor-neutral technologies Ethernet, Time-Sensitive Networking (TSN), and OPC Unified Architecture (OPC UA).

1 Introduction

The transition from industrial automation (Industry 3.0) to Cyber-Physical Production Systems (Industry 4.0) implies a huge demand for connectivity along the whole value chain. This chain encompasses vertical and horizontal communication from the sensor/actuator level up to Enterprise Resource Planning (ERP) systems and further to applications residing inside the cloud. Factories, in this context, comprised of a heterogeneous array of machines from a multitude of vendors and manufacturers, which are integrated as a singular production line, have their own specific demands on flexibility, interoperability, and real-time. Existing vendor agnostic technologies such as OPC UA and TSN try to address these demands. However, so far no specification exists which covers the need for interoperability, discovery, and automatic configuration in the field of functional-safety-related applications [EFIK18].

Machinery, which poses a risk of physical injury or damage, has additional requirements in terms of functional safety. A common way to address these challenges is to deploy dedicated cables that have to be installed separately to guarantee safety requirements of various machines in a production line. Additionally, these cables require monitoring for open-circuit and short-circuit problems, in

J. Jasperneite, V. Lohweg (Hrsg.), *Kommunikation und Bildverarbeitung in der Automation*,
Technologien für die intelligente Automation 12, https://doi.org/10.1007/978-3-662-59895-5_17

order to assure proper function of their safety features. Such a discrete wiring solution is simple, but every change in a production line results in a huge effort of re-cabling and re-configuring. Over the past several years, industrial communication systems have emerged that address safety features based on Industrial Ethernet to simplify cabling for functional safety applications.

Today, several safety transport protocols based on Industrial Ethernet are established in the industry. However, there is no system on the market which offers discovery of safety devices and automatic configuration of the safety network.

This paper describes a method of how to use existing technologies in order to achieve self-configuring functional safety connectivity which minimizes the effort required due to system changes. The proposed solution is based on Ethernet, TSN, OPC UA, and openSAFETY, combining them into an integrated architecture which enables self-configuring safety networks.

2 Functional Safety in Cyber-Physical Systems

The objective of functional safety is "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" [IEC05a]. The most important functional safety standard in continental Europe is IEC 61508. It is a generic standard that can be used as a template for application-specific standards, or it can be applied directly. Furthermore, two international standards, namely ISO 13849-1 and IEC 62061, use the concept of functional safety by specifying safety requirements in terms of functional requirements and by defining the amount of risk reduction.

A safety-related electrical, electronic and programmable electronic control systems consists of several Safety-Related Parts of Control Systems (SRP/CS) such as sensors, logic, actuators, and the connections in between.

2.1 Discrete Wiring Solution

The classic approach for building a functional safety system is to connect safety devices using cables with line monitoring. This discrete wiring concept involves efforts in wiring each sensor and actuator to safety relays or a safety Programmable Logic Controller (PLC). It is an inflexible solution as every change in the safety configuration implies a change in cabling, which leads to a long downtime of the machine or production line.

2.2 Ethernet-Based Real-Time Safety Control Networks

In recent years, automation networking technologies, in particular those dedicated to the industrial automation domain, have been enriched with safety features. An industrial network, as the platform for all communications within a production line, must also support deterministic real-time traffic as well as best effort traffic. The pre-requisite of a safe and stable operation of a functional

safety protocol within a system is the deterministic transmission of data, which includes low latency, minimal jitter, and minimal packet loss.

Black-Channel Principle The black channel principle, recommended by IEC 61784-3 [IEC16], is based on the requirement that the transmission of safety data is performed independently of the characteristics of the transmission system. Therefore, an additional layer – the safety layer – is placed on top of the application layer. The safety layer considers that safety data is subject to various threats, and for each one a set of defense measures is defined in order to protect this data [WI16, chapter 46.1.2].

Ethernet-Based Safety Protocols IEC 61784-3 defines common principles for the transmission of safety-relevant messages among participants within a distributed system using control network technology in accordance with the requirements of IEC 61508 series for functional safety.

Although all safety protocols and profiles defined in IEC 61784-3 are transport layer agnostic using the "black channel principle", almost every Industrial Ethernet protocol comes with its own safety protocol. Some of the most prominent protocols are listed in Table 1.

Table 1. Industrial Ethernet and Safety Protocols

Ind. Ethernet	Safety Protocol	IEC Norm	Org.
EtherNet/IP	CIP Safety	61784-3-2	ODVA
PROFINET	PROFIsafe	61784-3-3	PNO
EtherCAT	Safety-over-EtherCAT	61784-3-12	ETG
POWERLINK	openSAFETY	61784-3-13	EPSG

The choice of an Industrial Ethernet solution almost always determines the safety protocol which has to be used within a machine. But the advantage of a well integrated safety protocol entails difficulties when it comes to interoperability of machines of various manufacturers within a production line.

Safety Configuration Procedure for Ethernet-Based Systems The commissioning and re-configuration process of a safety system is usually assisted by an engineering tool supported by the manufacturer of that system. The safety engineer provides all necessary information to that tool, which compiles the needed configuration and transfers it to the safety system. The configuration procedure, according to the E/E/PE system safety lifecycle phase 10 in IEC 61508-1, includes the following steps: create a safety application; compile and transfer the safety application to the safety system; at initial commissioning or hardware change, the safety modules have to be validated by the safety engineer.

2.3 Safety Connectivity in Production Lines

Heterogeneous production lines, comprised of machines from various manufacturers in an Industry 4.0 environment, are placing a new range of demands on communication, interoperability, and flexibility. Although, machine manufacturers already use proprietary Ethernet-based safety protocols inside their machines, it is still common today to implement functional safety connectivity among machines within a production line using a discrete wiring solution. The lack of interoperability between different safety protocols of various manufacturers implies therefore limitations in flexibility.

Figure 1 illustrates a production line consisting of 3 machines and an external emergency stop button. Safety connectivity is carried out with dedicated cables between the machines. Non-safety critical communication includes real-time and non-real-time data transmission. Real-time data is utilized for process data using Industrial Ethernet solutions such as PROFINET or POWERLINK. Applications with no need for real-time such as Human Machine Interface (HMI), Manufacturing Execution System (MES), ERP, or cloud services are connected via a best effort network to the production line.

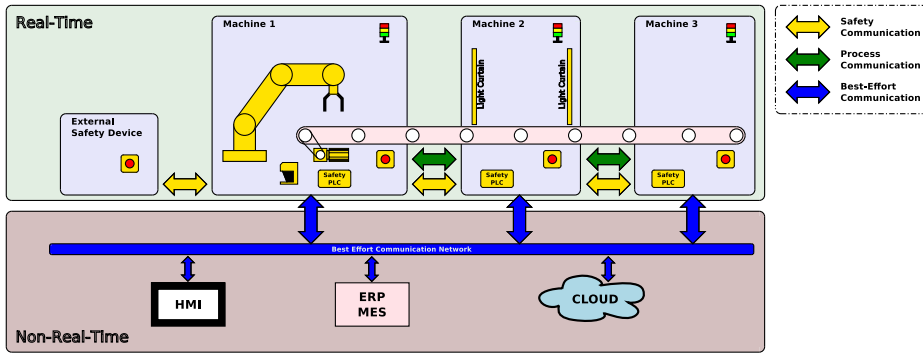

Fig. 1. Production line with hard-wired safety connectivity

3 Requirements for Self-Configuring Safety Networks

The set of requirements that needs to be satisfied by an industrial communication solution spreads out over three different areas: the communication network, the Machine-to-Machine (M2M) communication protocol, and functional safety. Each of these areas provides capabilities which serve as foundation for a self-configuring safety solution.

3.1 Communication Network

The foundation of a unified data transport platform places requirements on the network capabilities. The deterministic transmission of data is a prerequisite for a safe and stable safety protocol in a Cyber-Physical System (CPS). Process data transmission as well as safety communication requires deterministic real-time network capabilities which includes low latency, minimal jitter, and minimal packet loss rates (**Req.C1: Periodic real-time traffic**).

Furthermore, there is also the demand for non-real-time capabilities on the same infrastructure. Applications such as HMI, ERP, or cloud services as well as configuration and diagnostic are not time-critical, and therefore can be based on a best-effort type of traffic (**Req.C2: Best-effort traffic**).

3.2 Machine-to-Machine Communication

The current trend towards reduced lot sizes and more flexibility re-inforces the need for a unified Machine-to-Machine (M2M) communication infrastructure. Devices or machines as part of such a unified infrastructure must be able to describe and advertise their capabilities (**Req.M1: Self-description**), and to discover capabilities of other devices (**Req.M2: Discovery**).

In an industrial environment such as a production line, communication is based on two paradigms. First, sporadic data transmission upon request such as configuration, data logging, and analysis should be available. This paradigm uses a Client/Server communication model in which the client sends a request, and the server returns a response (**Req.M3: Client/Server**). Second, the transmission of data in an event-based manner (e.g for the transmission of change-of-values) is mandatory. This kind of communication is best handled by a publish/subscribe communication model in which the sender of messages, called publisher, does not send the data to a specific receiver but rather uses a dedicated stream identifier. Receivers, called subscribers, can then use this identifier to subscribe to the data stream (**Req.M4: Publish/Subscribe**).

A comprehensive M2M communication platform must provide mechanisms to maintain a secure channel ensuring confidentiality, integrity and availability of data and services. It therefore has to support common security features including user authentication, user authorization, message authentication, and encryption (**Req.M5: Security**).

3.3 Functional Safety

Functional safety certification is widely considered to be an essential tool to control and mitigate risk, particularly in those cases where a failure could lead to serious injury or death. Compliance with international standards such as IEC 61508 [IEC05a] is driven by legislation, regulations, and insurance demands. IEC 61508 is a basis for sector-specific standards including process industry (IEC 61511), nuclear industry (IEC 61513), machinery industry (IEC 61061 and ISO 13849), and rail industry (EN 50126).

The machinery-sector-specific safety standards IEC 62061 [IEC05b] and ISO 13849-1 [ISO15], therefore, require the user to assess the risks by calculating the average probability of a dangerous failure per hour (PFH). IEC 62061 assigns the PFH to Safety Integrity Levels (SIL) which range from 1 to 4. ISO 13849-1 uses Performance Levels (PL) from "a" to "e" instead. A common communication platform in machinery, consequently, has to support safe and standard applications in order to get a safety certificate (**Req.S1: Safety Certification**).

IEC 61784-3 [IEC16] defines common principles for the transmission of safety-relevant messages among participants within a distributed system using control network technology in accordance with the requirements of IEC 61508 series for functional safety. The "black channel principle", recommended by IEC 61784-3, is based on the requirements that the transmission of safety data is performed independently of the characteristics of the transmission system. Therefore, an additional layer, the safety layer, is placed on top of the application layer (**Req.S2: Black Channel Principle**).

Communication platforms intended for safety data are equipped with several mechanisms to prevent potential errors from occurring during data transmission. These errors are replicated data, data loss, inserted data, incorrect data sequences, corrupt data, and transmission delays (**Req.S3: Safe Data Mechanisms**).

It can be very costly to stop a production line for each change in the safety configuration. Therefore, it is essential that the safety layer offers seamless configuration changes (**Req.S4: Seamless Configuration Change**).

4 Building Block Technologies

The aim of this paper is to design a self-configuring safety network based upon existing technologies. Deterministic data transport as well as unified communication combined with a safety protocol is the foundation for a real-time safety network.

Three technologies, which are gaining acceptance in the industry, were chosen as a basis: Time-Sensitive Networking (TSN), OPC Unified Architecture (OPC UA), and openSAFETY.

4.1 Time-Sensitive Networking

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 for Time-Sensitive Applications), IEEE 802.1Qbv (Traffic Shaping), and IEEE 802.1Qbu (Frame preemption), provide extensions for wired and wireless Ethernet in order to enable deterministic real-time communication [SPG+16]. IEEE 802.1Qcc (Stream Reservation Protocol) is focused on the definition of management interfaces and

protocols to enable TSN network administration. The fully centralized configuration model, which is used for this paper, is illustrated in Figure 2.

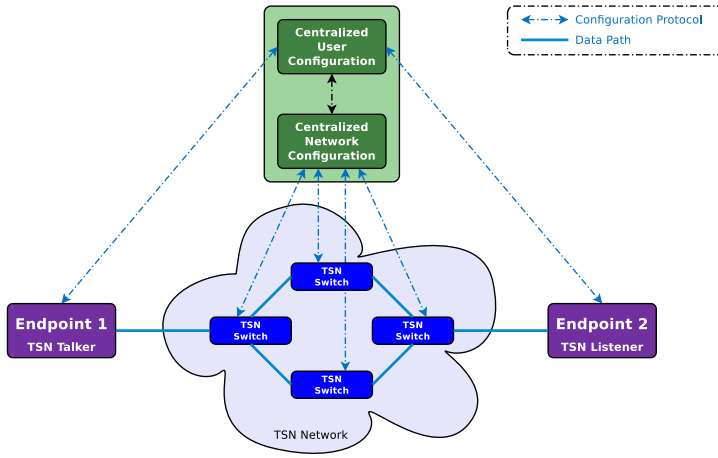

Fig. 2. Fully Centralized Configuration Model from IEEE 802.1Qcc

Configuration or rather re-configuration takes places in several steps. The Central User Configuration (CUC) takes a request from an endpoint and hands it over to the Central Network Configuration (CNC), including information about the talker and the listener. The CNC, which has full and global knowledge of network resources and topology, calculates a path that fits the communication requirements. On successful completion, the path is configured in the network and a positive feedback is sent via the CUC to the endpoints.

From a technical perspective, any real-time capable protocol which fulfills the requirements discussed in Section 3.1 or analyzed in [DJF15] could be used as transport platform. TSN was chosen du to the fact that it is the only candidate which is vendor independent, offers converged networks, and allows large and flexible network topologies.

4.2 OPC Unified Architecture

OPC UA is 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 communication. 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 [MLD09].

Information Model OPC UA uses nodes as a fundamental notion to represent the data and behavior of an underlying system. The nodes can be of various classes including variables, objects, and methods. Nodes can be organized using references that represent the relationships between them. Thus, an information model may be constructed to expose data and metadata for consumption by clients. OPC UA companion specifications exist that map concepts and technologies to standard models for representation in the OPC UA domain.

Communication Concepts OPC UA supports two communication models. A client/server model for one-to-one communication, and a publish/subscribe (PubSub) model for one-to-many.

When using the client/server principle, a client establishes a channel and an actively maintained session with a server. Client requests (service calls) are sent to the server, which in return is required to respond. The client may subscribe to nodes in the information model. Changes to these nodes trigger notifications.

Using the PubSub mechanism, a publisher may use connection-less (broker-less) or connection-oriented (broker-based) transmissions to distribute messages to subscribers. The former uses multicast to deliver messages to subscribers. The latter uses a message broker and a standard message exchange protocol (e.g., MQTT, AMQP) for message distribution.

4.3 openSAFETY

openSAFETY is a bus-independent communication protocol defined in IEC 61784-3-13 used to transmit information that is crucial for the safe operation of machinery. It is a black channel protocol certified according to IEC 61508 and meets the requirements of Safety Integrity Level (SIL) 3 applications. IEC 61784-3 defines common principles for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. The openSAFETY stack is the only safety protocol with an open source implementation (mixed BSD/GPLv2 license).

Two communication models are applied within openSAFETY, the producer/consumer model for process data, and the client/server model for configuration and network management. Process data is transmitted in the way that a producer node sends data identified by a specific Safety Address (SADR). Any Safety Node (SN) within the Safety Domain (SD) may receive this data. Configuration data as well as network management data uses client/server communication where the Safety Configuration Manager (SCM), as the client, sends requests to a SN which acts as a server. The SN replies with a response. Both messages, request and response, include server and client addresses.

5 Self-Configuring Safety Machine-to-Machine Communication

Two of the major obstacles to functional safety M2M communication in a production line are the lack of interoperability and a complex, time-consuming safety configuration. This paper proposes a concept that addresses interoperability and flexibility by using TSN for deterministic real-time transport, OPC UA as communication platform, and openSAFETY for functional safety communication. The concept provides an automatic re-configuration procedure, assisting the system operator on configuration changes and consequently reducing machine downtime.

5.1 Concept

The traditional approach in production line communication is to separate real-time and non-real-time related system parts on a hardware level as shown in Figure 1. In the real-time domain, there is a process communication network and a discrete wiring solution for functional safety requirements. For applications in the non-real-time domain such as HMI, MES, and ERP as well as connectivity to cloud-based services, a best effort communication network is used.

In our concept, the distinction between real-time and non-real-time domain is accomplished on a configuration level using features of TSN instead of using separate communication networks. As illustrated in Figure 3, all communication in the production line is based on one comprehensive communication platform, replacing all the cabling for various hardware interfaces by a single networking technology.

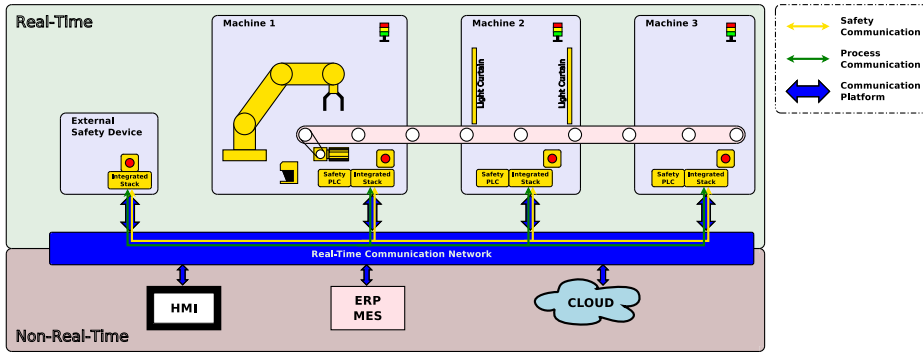

Fig. 3. Production line with a comprehensive communication platform

Each system change in the production line entails re-configuration in all parts of the communication stack, including the safety protocol and safety application.

In order to keep the re-configuration effort for the system operator as small as possible, this concept defines an automatic procedure for re-configuration.

5.2 Re-Configuration Procedure

Self-configuring safety networks can be realized by combining a functional safety protocol, deterministic real-time transport, and an integration platform with discovery and security capabilities to implement and execute a well-defined re-configuration procedure. This procedure has to be executed whenever the safety configuration changes, i.e. Safety Nodes (SNs) are added to or removed from the system setup. As illustrated in Figure 4, it follows four consecutive phases[1]: *Discovery*, *Validation*, *Plausibility*, and *Processing*.

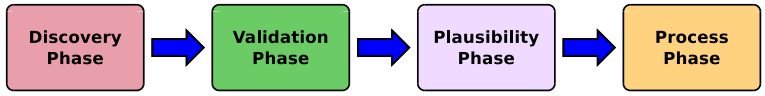

Fig. 4. Re-configuration phases

In the 'Discovery Phase', a new device advertises its functionality to the existing safety network and uses a discovery service to search for other nodes that offer safety functions. This phase is based on client/server communication using best effort traffic. Therefore, the requirements 'C2: Best-effort traffic', 'M1: Self-description', 'M2: Discovery', and 'M3: Client/Server' have to be met.

The next stage is the 'Validation Phase' where a check occurs to ascertain whether a device is new or already known to the ensemble. If a new device has entered the network and, thus, a safety configuration change is needed, the operator is prompted to verify and acknowledge the changes. Similar to the previous stage, the communication utilizes the client/server principle with best effort traffic. The addressed requirements in this phase are 'C2: Best-effort traffic' and 'M3: Client/Server'.

The new configuration is checked for potential issues and errors during the 'Plausibility Phase'. This phase involves device matching and network timing such as response and cycle times. The result of the plausibility checks are communicated to other entities in the system, either success or fail. In both cases, the subsequent client/server communication is based on best effort traffic. Thus, the requirements 'C2: Best-effort traffic' and 'M3: Client/Server' are necessary.

Upon successful completion of the first three phases, the 'Processing Phase' can start where the SNs transmit safety-related process data. This phase concludes the re-configuration procedure. Now, the network and the safety application are prepared, and safety-relevant process data is transmitted using the

[1] https://www.br-automation.com/en/products/innovations-2017/safe-line-automation/

publish/subscribe paradigm. Consequently the requirements 'C1: Periodic real-time traffic', 'M4: Publish/Subscribe', 'S2: Black Channel Principle', and 'S3: Safe Data Mechanisms' are needed.

Furthermore, there are some requirements which are demanded in all four phases. 'M5: Security' ensures the secure transmission of data during the whole operation. In order to keep machine down-time as small as possible, the configuration has to be applied seamlessly into the system, which explains the 'S4: Seamless Config. Change' requirement. Finally, the safety protocol has to be certified according to [IEC05a] which is reflected in 'S1: Safety Certification'.

5.3 Requirements Matrix

Implementation of the proposed concept requires the mapping of all requirements to the suggested technologies. Therefore, Table 2 summarizes all previously mentioned requirements and maps them to the technologies discussed in this paper.

Table 2. List of requirements

	M1: Self-description	
	M2: Discovery	S1: Safety Certification
	M3: Client/Server	S2: Black Channel Principle
C1: Periodic real-time traffic	M4: Publish/Subscribe	S3: Safe Data Mechanisms
C2: Best-effort traffic	M5: Security	S4: Seamless Config. Change
TSN	**OPC UA**	**openSAFTEY**
(a) Communication Network	**(b)** M2M Communication	**(c)** Functional Safety

The requirements matrix points out that the requirements on the communication network, the M2M communication platform, and functional safety protocol can be covered with the technologies TSN, OPC UA, and openSAFETY. Thus, these technologies are combined to achieve a comprehensive and integrated architecture.

5.4 Integrated Architecture

As basis for a self-configuring safety network serves an architecture which was proposed in [EFIK18] and is illustrated in Figure 5. This communication stack combines TSN, OPC UA, and openSAFETY in a way that it is capable of transmitting real-time and non-real-time as well as safety and non-safety relevant data.

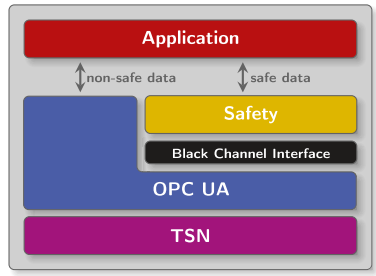

Fig. 5. Integrated Architecture handling safety and non-safety critical data

5.5 Prototype Implementation

In order to realize a prototype, the integrated architecture is chosen as building block for the proposed solution. It includes openSAFETY as the functional safety protocol, TSN for deterministic real-time transport, and OPC UA as integration platform.

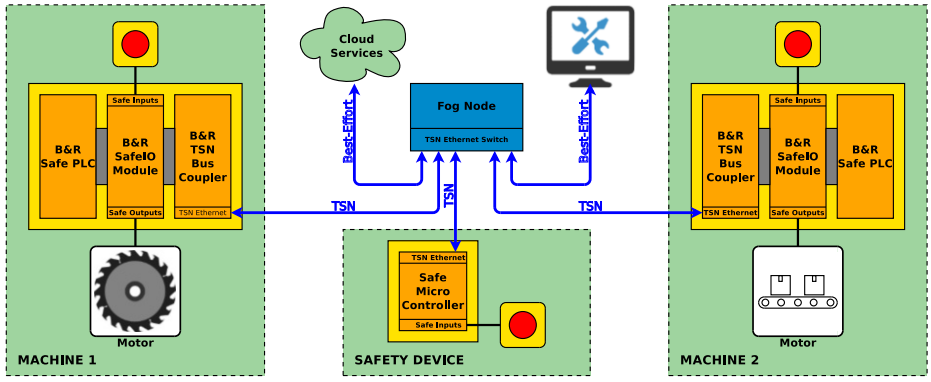

Fig. 6. Prototype schematic

Figure 6 illustrates the prototype setup including PLC components from B&R Industrial Automation, a TSN switch, and a Fog Node. The use-case assumes that Machine 1 and Machine 2 communicate via the TSN network. During operation, a new device, the safety device in the middle, will be connected to the TSN switch. After automatic execution of the re-configuration procedure and acknowledgment of the safety engineer, the newly added emergency button is able to stop the motor in Machine 1 and the conveyor belt in Machine 2.

6 Conclusion and Outlook

The presented solution of self-configuring safety networks can help to reduce the re-configuration effort and costs of production lines. Instead of re-installing separate cables to connect safety functions, the safety engineer simply re-configures the system and acknowledges the changes via the HMI on one of the corresponding machines. Additionally to the financial aspect, the introduction of an automated configuration can help to prevent configuration mistakes especially in stressful situations. The construction and configuration of the prototype presented in Figure 6 is currently in progress. The findings in setup and configuration of the prototype will help to identify necessary adjustments in communication relations, user interaction, and safety application.

Acknowledgment

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.

References

[DJF15] L. Dürkop, J. Jasperneite, and A. Fay. An analysis of real-time ethernets with regard to their automatic configuration. In *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, pages 1–8, May 2015.

[EFIK18] 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)*, pages 1–4, June 2018.

[IEC05a] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508, 2005.

[IEC05b] IEC. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems. IEC 62061, 2005.

[IEC16] IEC. Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions. IEC 61784-3, 2016.

[ISO15] ISO. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. ISO 13849-1, 2015.

[MLD09] Wolfgang Mahnke, Stefan-Helmut Leitner, and Matthias Damm. *OPC Unified Architecture*. Springer Publishing Company, Incorporated, 1st edition, 2009.

[SPG+16] 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)*, pages 1–8, Sept 2016.

[WI16] B.M. Wilamowski and J.D. Irwin. *Industrial Communication Systems*. ENGnetBASE 2015. CRC Press, 2016.