New lift safety architecture to meet PESSRAL requirements

Ayoub Soury, Denis Genon-Catalot, Jean-Marc Thiriet

New lift safety architecture to meet PESSRAL requirements

Ayoub Soury*†, Denis Genon-Catalot† and Jean-Marc Thiriet*‡
*Univ. Grenoble Alpes, Gipsa-lab, F-38000 Grenoble, France
†Univ. Grenoble Alpes, LCIS, F-26000 Valence, France
‡CNRS, Gipsa-lab, F-38000 Grenoble, France
Email: {ayoub.soury, denis.genon-catalot}@lcis.grenoble-inp.fr; jean-marc.thiriet@gipsa-lab.grenoble-inp.fr

***Abstract* — Industrial control and automation systems are evolving towards infrastructures more connected. Its component's interconnection makes them more dependent on the networks and communication protocols used. On the one hand, high performance, low costs and real-time capabilities are generally required to cope with more and more demanding application requirements; while on the other hand, security solutions are often needed in an increasing number of communication attack scenarios. As part of new lift control generation, we will analyze a transition case from an electrical/electro technical component to network of communicating electronic components as part of the safety displacement system. This paper will describe the analysis of dependability requirements for the next electronic lift control.**

I. Introduction

Nowadays, there are many industrial Ethernet protocols, which could act as fieldbus functionality. The introduction of Ethernet techniques in industrial communication allow to reduce the infrastructure costs. In this way the replacing cables by field bus has evolved from simple protocols such as Modbus (ASCII format) to Internet Protocol standard. The lift domain design has undergone same evolutions as the automotive domain; manufacturing cost, wiring reduction, energy optimization and meet a new norms constraints.

Nowadays, the lift safety chain based on interconnected electromechanical elements with interconnecting wireline cables. Therefore it requires a large number of cables that have a direct impact on the product cost and its installation complexity and thus its installation costs. So, in order to reduce these costs (installation cost, maintenance, certification, etc.) we will perform safety functions. This is done by means of a programmable electronic system to achieve some standardization requirements and not with electromechanical devices. We make an original approach in the lift eco-system, which uses a deterministic operating system [1] from Krono- safe Company (spin off CEA). To ensure the safety of people transportation, system availability should be considered behind the relevant safety. The deterministic lift control system is one of the ADN4SE project demonstrators (BGLE project). The global aim is to design and develop new lift safety functions supported on deterministic kernel and associated tools in accordance with the required lift-safety standard in order to achieve product certification.

The main contribution in this paper is an analysis case of the adopted standard IEC 61508 requirements specification targeting the development of a new safety chain for lift control system that allow to achieve SIL3. In addition, we propose a new lift safety architecture using a deterministic kernel to improve the safe real-time communication within the safety chain, in accordance with the safety standard. The challenge that is especially addressed is having a product certifiable PESSRAL with the integration of a deterministic core in electromechanical safety chain, i.e. transition from an electrical/electro technical component to network of communicating electronic components while respecting the business application specifications.

The remainder of the paper is organized as follows. In section II we present the existing architecture of the actual lift system, and we identify some problems in this architecture. In section III we analyze the safety requirements specification in the lift control system generally. Section IV describes a study case of existing fieldbus in lift eco-system, and we identify the bus limits in relation to the described standard safety. In section V and VI, we present our proposal. We describe the industrial communication over Ethernet with a classification for real-time communication. We propose how an Ethernet-based industrial communication can reach SIL3 and can be supported by deterministic kernel. Finally in Section VII we represent our conclusions.

II. The safety challenge in the lift application control

Fig. 1 shows a lift demonstrator with a safety chain as currently running on the majority of lifts. Range of serial contacts whose purpose is to allow the displacement lift car control compose this safety chain. The displacement lift car is only possible if all the contacts are closed. However, the behavior of these elements is not identifiable, which complicate the safety chain control. It will be more difficult to identify the failed contact in the actual chain. We cannot neglect the mechanical maintenance costs of the safety chain. So, making the safety chain smarter is a business need. But without forgetting the security level required in this type of application because that will direct influence on human life. The applicable standards for lift safety system design are defined in EN 81-1 (Specification of the safety requirements for the design and installation of electric lifts), PESSRAL (Programmable Electronic components and Systems in Safety Related Applications for Lifts)

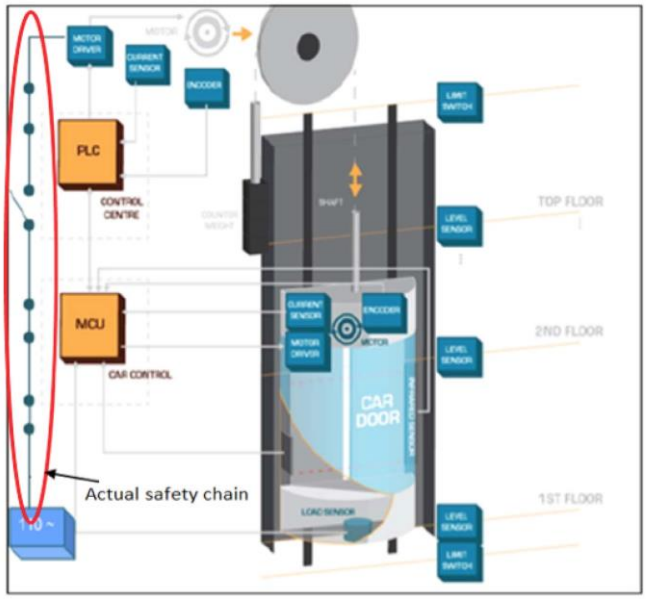

Fig. 1. Actual safety chain in the lift architecture.

and ISO022201: 2008 (Standard relating to programmable electronic systems integrated in the safety chain of a lift).

The main objective of the project is to design new lift demonstrator that is, applying the IEC 61508 standard, using SIL 3 certified safety bus, simplifying the certification phase, reducing testing effort and hosting (reassemble) critical and non-critical functions on the same micro-controller. The demonstrator must be capable to integrate third-party non-critical functions without undermining the certification of critical functions. To minimize failures and maintain the dependability to a certain level, in electrical, electronic and programmable electronic systems, the IEC 61508 [2][3] specifies 4 safety integrity levels in terms of dependability (SIL1, SIL2, SIL3, and SIL4) [4]. These cover features security systems and requires from its conception to meet and satisfy certain criteria and safety conditions [5]. Automatic electronic architectures need to perform more and more functions that are mapped onto different electronic components because of their different safety level or different application domains. For our application demonstrator domain (Lift), we would reach IEC 61508 SIL3 level. To achieve this safety integrity level, our system must satisfy specific requirements for the lift application control. The PESSRAL, derived standard from IEC 61508 and specific lift application domain, details these requirements and identify business requirements and hardware requirements standard, and the digital management system of the lift must be consistent with this requirements. The PESSRAL standard is based on the guidelines provided by IEC 61508 and EN81 (CEN). It specifies dedicated hardware and software requirements to ensure SIL 3 integrity level [4]. But it did not assign roles to implement responsible.

The functions relating to the lift safety (51 functions, which allow the system to meet the SIL3 requirements) must not be less than SIL1 and not more than SIL3 [6]. These functions are implemented in order to bring the system into safe state or maintain the system on its safe state according to the specific random events. The features and functions associated with the integrity level SIL3 must meet performed in the communication layer [5]. The designers must list the customer requirements and describe the secure states in the lift system. These states depend primarily on the responses of safety functions applied. There is some requirement identification:

- Hardware requirements: 09 PESSRAL requirements.
- Software requirements: 16 PESSRAL requirements.

III. Analysis of Requirements Specification

In this project we aim to design and develop lift dependability functions for electronic systems using deterministic kernel ”Kron-OS” and its tools that are safety by construction [7]. These functions must be PESSRAL certified. Each client requirement must have a structure that brings together and combined among the normative, functional and temporal requirements as shown in Fig. 2. In the next sentences will describe each requirement and we assign an identifier relative to that of the root requirement, for example:

- Root requirement:
  - Description: Protection against the excessive speed of the car uphill.
  - Security requirement: YES.
  - Risk covered: fall of the cabin.
- Functional requirement:
  - Description: A traction lift must be provided with a device for protection against excessive speed of the car uphill. The device including a supervisory and speed reduction unities, must detect an uncontrolled movement of the car uphill at a speed of at least 115 of the nominal speed. The device must act on the cabin, counterweight, the cable system (suspension or compensation) or the traction sheave.
- Temporal requirement:

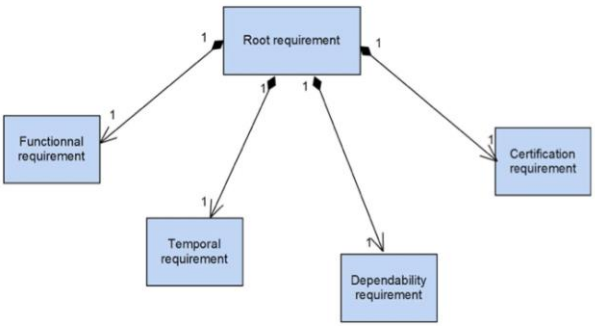

Fig. 2. Requirement composition and definition -ADN4SE document project.

  - Description: system reaction time $\leq$ 100ms.
- Certification requirement:
  - Description: Lift-safety function (id 12) (among 51 functions).
- Dependability requirement:
  - Description: this function must be SIL2.

Achieving PESSRAL links four partners for this demonstrator in the ADN4SE project:

- LCIS: specialized dependability in industrial communication.
- SPRINTE: for the provision of the lift specifications.
- Krono-safe: for providing the real-time software solution.
- Schneider Electric: expert in the development of critical systems.

To ensure the safety integrity level SIL3 over the whole lift safety chain, which must be ensured with a single communication channel, we will use an important means of communication certified SIL 3 [8]. With a view to simplification, the bus must transmit critical and non-critical messages.

IV. Existing fieldbus in lift eco-system

According to its original purpose, CAN, using bus topology, is strongly established in the automotive industry to reduce cable harnesses in vehicles. It is not suitable for transmission of data over long distances with a high rate (for an indicative maximum length of 40 m it's 1 Mbps) [9]. This one is particularly suitable for located systems with distributed intelligence and high reliability constraints [10]. His main objective was reliability with a low cost. Mercedes-Benz was the first automaker to equip his vehicles with CAN protocol. Since many manufacturers use it such Intel, Philips, Siemens, Motorola, NEC and Texas Instruments, were the first to implement the protocols in micro-controllers. The CAN protocol is a multi-master contention type (any master station can initiate a frame as soon as the bus is free allowing the production and consumption of information transmitted by diffusion thereof. This is a CSMA protocol with access collision inhibition (Carrier Sense Multiple Access with Collision Resolution CSMA/CR) for priority frame by bitwise arbitration. Each node performs this bitwise arbitration. Any anomaly detected during the arbitration allow transmitter node to stop immediately its transmission. It is not possible to calculate a maximum reaction time, because CAN is not as deterministic except possibly for the data to have always the highest priority [10].

In the automation world, an international users group and manufacturers defined a subset of CAN protocol in the Can in Automation (CiA 04). The CiA group specified the application layer of the protocol stack over CAN bus: physical, data link and application. CANOpen based profiles are only software solution. The CanOpen application layer protocol supports synchronous and asynchronous channels shared. The synchronous transmission cycle is defined by the cyclic transmission of a synchronization frame (SYNC frame priority). The CANOpen profile applicative specifications describe the virtual devices (12 VD) for lift control system.

The virtual controllers (Call Controller, Controller car door, car drive controller) perform control functions dedicated to the lift application. In this application, all the control functions can be implemented in a single CANOpen device. Although in other applications, control functions must be implemented in different and various CANOpen devices. Virtual devices are implemented each in a CANOpen device as they can be combined in one or more devices CANOpen-Lift (Cia 417) and allows it to be a simple and sophisticated application. The virtual devices set are: Call- Controller, Car-door-Controller, Car-drive-Controller, Input- panel-Unit, Output- panel-Unit, Car-door-Unit, Light-barrier-Unit, Car-drive-unit, Car-position-Unit, Load-measuring-Unit, Remote-data-transmission-Unit, and Power-measuring-unit. The CAN protocol introduces object-oriented communication. In- deed, the CANOpen protocol uses the objects dictionary. It defines all the objects that can be exchanged in the network. Each object is addressed using a 16-bit index and a sub- index of 8 bits. Each node must have an object dictionary through which data transmission will be possible as shown in Fig. 3. While Can is largely adopted in industrial processes automation, it has disadvantages that limit its use as follows [11]:

- Transmission rate: It can reach as maximum throughput 10 Mbps, which is relatively, low (with FTT-Can version).
- Limited frame format: the CAN bus is dedicated for industrial communication systems that limit transmitted information types.

V. Deterministic fieldbus

The industrial communication protocols, as well as fieldbus must meet the constraints of industrial communication [9][12]

- Robust to the industrial environment (physical layer).
- Deterministic (ensuring the data refresh in cycle time) (Data Link Layer).
- Interoperable (exchanging information among all types of industrial equipment) (Application Layer).

Interoperability is the term most sensitive in terms of cost. New industry communication concepts progress after some problems in fieldbus network classic (determinism, reaction time, throughput, portability...). IEC TC65 has launched a new standardization project for industrial communication. Set the real-time Ethernet in the industry seems a logical consequence of the Ethernet introduction in industrial automation.

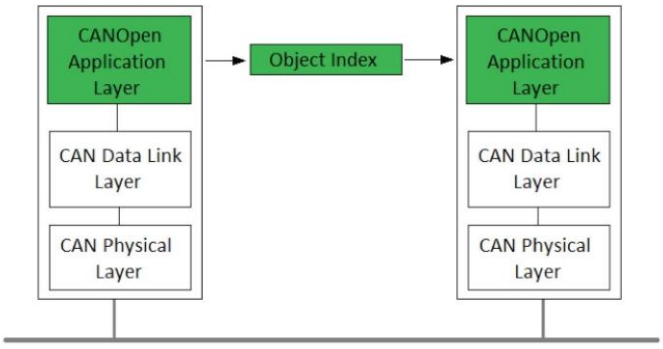

Fig. 3. Exchange principle of objects in CANOpen.

Researchers continue to propose solutions to the Ethernet specifications to meet the criteria of real-time. There are those who offer solutions for quality of service, devices synchronization or packet processing/modification to resolve Real-Time constraint [13].

After that, Ethernet has positioned itself as standard solution for industrial communication replacing classical fieldbus as CAN. Ethernet Real Time (RTE) resolves some existing problems in industrial control system [14][15] as; rate transmission (high rate about 1Gbps), over Ethernet, different kinds of data can be transmitted (Audio, Video...) and using Ethernet allows integrating different applications.

Considering the reaction time for the Ethernet-based real-time solutions, we can classify their protocols into 3 classes as shown in Fig. 4.

- Class 1: Top of transport layer (over TCP/UDP); low speed class, reaction time 100ms, moderate efficacy (e.g. Ethernet/IP).
- Class 2: Top of Ethernet layer; required by automate (PLC, control PC), reaction time < 10ms, hardware implementing to reduce the TCP/IP stack (e.g. PowerLink, Profinet RT).
- Class 3: Modified Ethernet (most challenging); required by Motion Control, reaction time <1ms, high synchronization precision (e.g. EtherCAT, Profinet IRT).

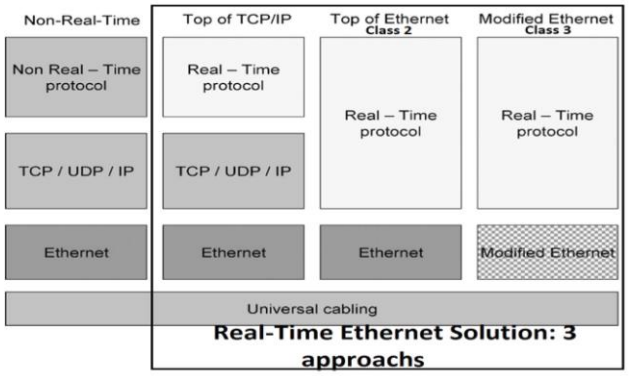

Fig. 4. Real-time Ethernet classification.

These solutions will be implemented over deterministic kernel safe by construction, which requires specific criteria to accelerate and ensure communication in the industrial system. Besides the reaction time, the communication model has to guarantee SIL3 safety level in communication phase to ensure the portability capacity of the deterministic operating system in embedded environments constrained. In this work, we are relying on actual architecture of safety chain in lift control system, improving it components behavior by introduction of controllers node network communicated instead of electric contact. Fig. 5 depicts the considered system with our modifications in safety chain. However, in our approach we are introducing network-based safety chain with communication network to transfer sensor measurements and control data using Ethernet based real time protocol.

We are replacing electric contacts with tow node kinds: Controlled node (CN) and manager node (MN). These new safety chain components are connected through an Ethernet network and the data frames are encapsulated in Ethernet PowerLink (EPL).

VI. Open Safety

The industrial communication in deterministic networks is far from being secure, it guarantees perfect synchronization among devices, and meets the temporal requirements imposed by the deterministic kernel, or the standard but not wholes safety requirements. To strengthen the security in this communication networks, we need to add a security measures at the top of application layer. OpenSAFETY is an application layer communication protocol. It ensures the security of the transmission frames. It allows creating communication systems requiring SIL 3 (Safety Integrity Level) according to IEC61508. OpenSAFETY is a set of components offering services and security mechanisms for secure data exchange via networks unsecured [16]. For example:

- Time stamp: This timestamp mechanism allows associating with each frame the time and date of transmission in order to avoid duplication of frames.
- Time monitoring: This time monitoring can predict moments of frame arrival and thus can detect losses and delays.
- Identification: Each frame is identified by a unique identifier to prevent and detect any kind of integration.
- Cyclic Redundancy Check (CRC): To ensure the integrity of messages sent and to avoid the alteration and modification of data, OpenSAFETY uses the CRC.
- Frame format: Using different frame format allows the distinction between the standard frame and the Open SAFETY frames.

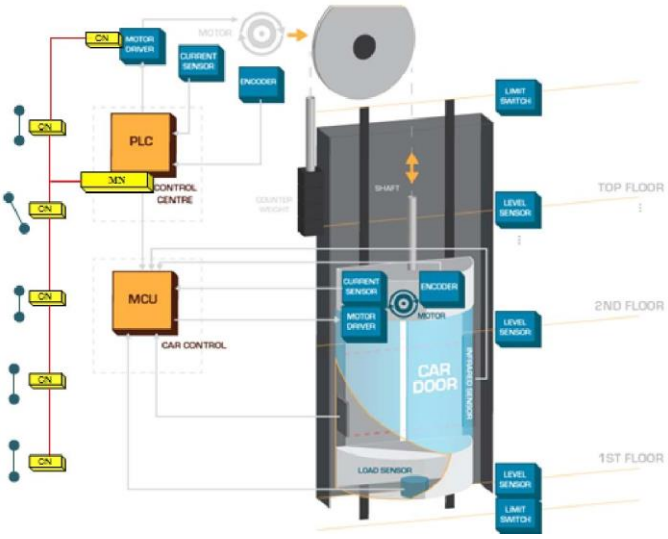

Fig. 5. Modified safety chain in lift control system.

OpenSAFETY operates at the application layer independently from real time Ethernet protocols used in the lower layers as shown in Fig. 6.

VII. Conclusion

The analysis and proposal for the new lift control are mandatory by new security level requirements. The innovative aspect of this collaborative project was the capacity to replace the safety chain electromechanical components (serial electric contacts) by dedicated fieldbus network. In this research project, we identified an adapted IP protocols to support dependability constraints for lift applications control. The IEC 61508 requirements for the performance machines applied to lift application have been regrouped into PESSRAL specifications. The paper summarizes the necessary criteria to achieve in the protocols selection to ensure the integrity of the PESSRAL standard. The mixed methodology allows integrating the communication architecture in the development in order to ensure the time performances based on deterministic operating system and safety by construction. Our contribution will allow to perform a safety chain analysis which is impossible to diagnose at this time. After specifying safety constraints required in the lift application, the next task will be devoted to the modeling of a safe communication. This modeling will be included in the modeling of a deterministic core used in the ADN4SE project. At least, this strategy will allow displacements command of the lift cabin in safe conditions clearly identified, which greatly simplifies the maneuver that today requires human intervention locally.

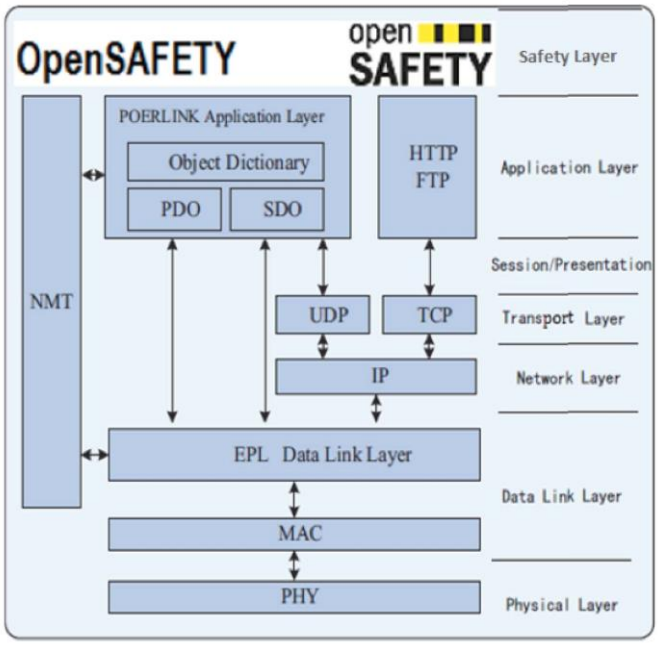

Fig. 6. OpenSAFETY over real-time Ethernet.

Acknowledgment

This research is supported by a grant of the BGLE-ADN4SE project (Atelier de Développement et Noyau pour (For) Systèmes Embarqués) supporting by the french industry ministry and lead by Sherpa and Krono Safe companies. The authors want to thanks the members of the work package lift for theirs analysis and specifications: Schneider, Sprinte, Itris automation.

References

[1] D. Chabrol, V. David, C. Aussagèues, S. Louise and F. Daumas, *"Deterministic Distributed Safety-Critical Real-Time Systems within the Oasis Approach"*, International Conference Parallel and Distributed Computing and Systems, 17th IASTED, 2005.

[2] E.M Marszal and W. Eric Scharpf *"Safety integrity level selection: Systematic methods including layer of protection analysis"*, Instrumentation, Systems, and Automation Society, 2002.

[3] D.J Smith and K. GL Simpson *"Safety Critical Systems Handbook: A straightfoward guide to functionnal safety, IEC61508 (2010 edition) and related standards, including process IEC 61511 and machinery IEC 62061 and ISO 13849"*, Elsevier, 2010.

[4] IEC 61508-2:2000, *"Functional safety of electrical/ electronic/ programmable electronic safety related systems" -Part 2:Requirements for electrical/ electronic/ programmable electronic safety-related systems.*

[5] E. Alberto, L. Ferrarini and C. Veber, *"Analysis of Ethernet based safe automation networks according to IEC 61508"* , Emerging Technologies and Factory Automation. ETFA'07. IEEE Conference on. IEEE, 2007.

[6] PESSRAL:2008 *"A lift design and development of programmable electronic systems in safety-related applications for lifts (PESSRAL)"*, 3rd ed. ISO/FDIS22201:2008, 2008.

[7] A. Soury, D. Genon-Catalot and J.M Thiriet *"La sécurité des ascenseurs avec des communications Ethernet-Based Real-Time"*, Edito 2 Historique - Comités du JNCT 2014.

[8] A. Soury, M. Charfi, D. Genon-Catalot and J.M Thiriet *"Perfomance analysis of Ethernet Power Link protocol around real-time operating system"*, International Conference on Industrial Informatics, IEEE, 2015, in press.

[9] N.P. Mahalik, *"Fieldbus technology: industrial network standards for real-time distributed control"*, Springer Science & Business Media, 2003.

[10] F. Corno, J. Perez, M. Ramasso, M. Reorda and M. Violante, *"Validation of the dependability of CAN-based networked systems"*, International High Level Design Validation and Test Workshop. HLDVT'12, IEEE, 2004.

[11] H. Xu, Y. Gao, K. Liu, B. Zhu and C. Zhang, *"Research on cross-communication based on real-time Ethernet POWERLINK"*, Control and Decision Conference (2014 CCDC), The 26th Chinese IEEE, 2014.

[12] J.D Decotignie, *"Ethernet-based real-time and industrial communications"*, Proceedings of the IEEE, vol. 93, no 6, p. 1102-1117, 2005.

[13] F. Max and T. Sauter, *"Standardization of industrial ethernet-the next battlefield?"*, International workshop on factory communication systems'06, IEEE, 2004.

[14] P. Neumann, *"Communication in industrial automation?What is going on?"*, Control Engineering Practice, vol. 15, no 11, p. 1332-1347, 2007.

[15] J. Juergen, M. Schumacher and K. Weber, *"Limits of increasing the performance of industrial ethernet protocols"*, Emerging Technologies and Factory Automation. ETFA'07. IEEE Conference on. IEEE, 2007.

[16] *"OpenSAFETY"*, version 1.4. June, 2014.