Proceedings in Manufacturing Systems, Volume 20, Issue 3, 2025, pp. 103-109 ISSN 2067-9238

AS-INTERFACE: MODERN COMMUNICATION PROTOCOL IN INDUSTRIAL SAFETY SYSTEMS

Ştefan-Claudiu MUREŞAN[1,*], Adrian-Florin NICOLESCU[2]

[1)] Eng., Dep. of Robots and Manufacturing Systems, National University of Science and Technology POLITEHNICA Bucharest
[2)] Prof., PhD, Dep. of Robots and Manufacturing Systems, National University of Science and Technology POLITEHNICA Bucharest

Abstract: *With the development of industrial automation solutions and the level of automation required in the manufacturing facilities there has been a challenge in offering a well-rounded safety system, capable of dealing with all the possible safety-related scenarios that can occur in a day-to-day industrial environment. More than that, a complex safety system implies high costs with raw materials such as cables, wire ducting, connection points and manual labor, which lead to deficiencies in the project-budget with little to no direct revenue in exchange. This study focuses on developing a test-stand for a modern approach to the problem of cost and time saving in the process of integrating the safety system, maintaining the safety standards required by international associations. The results of this study can represent the beginning point for further large-scale integration in industrial fields of such solutions, leading to a decrease in budge funds reserves.*

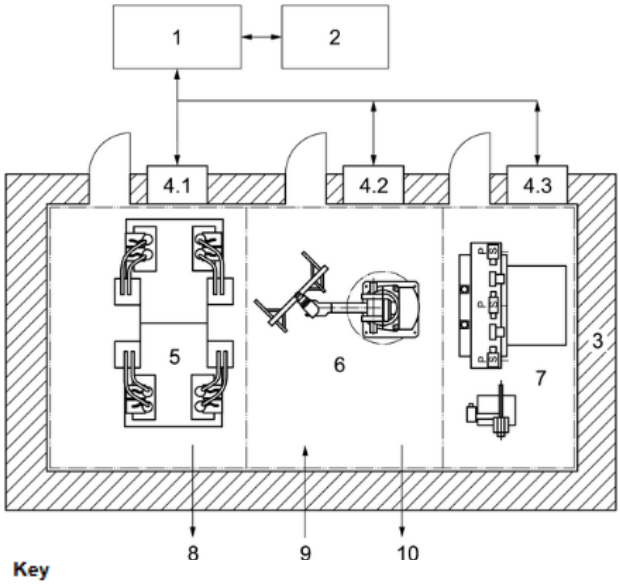
Key words: *AS-Interface, Safety, Industrial Automation, Communication, Control Systems.*

1. INTRODUCTION

From the beginning of time, human safety represented a principal concern in the eyes of world-wide leaders and organizations. With the rapid evolution of manufacturing facilities and the growing demand for automation, the safety requirements that automated systems must satisfy to obtain the necessary certifications have become increasingly stringent.

Safety standards have been developed and constantly improved during this period, with standards such as ISO 11161:2007 and EN ISO 13849-1 being considered state-of-the-art for every solution integrator. A clear set of hardware and software elements required for proper safety integration has been defined, including fencing and interlocking systems, segregated safety zones, hazard-control devices, and dedicated safety controllers equipped with specific safety functions and memory capacity (Fig. 1) [1].

The development of these standards has automatically implied an increase in the cost requirements needed in the project budgeted to assume proper safety development and integration. More materials needed to be acquired, and the classic wire-based point-to-point methods showed their limitations, which led to the necessity of new and durable solutions capable of maintaining the safety requirements but also helping in the process of cost reduction. With that, the spotlight was oriented to the communication protocols used in the basic signals exchange, wanting to integrate them to be capable of handling both the normal process tasks but also the safety-related tasks. For that, dual processor control units were developed, with a dedicated processor for the main process tasks and one separate processor only for the safety control tasks. It was crucial to permit the signal exchange between the two separate domains with the usage of special-dedicated intermedial data-blocks with restricted one-way communication.



Key

1	control	6	hazard zone B
2	operator pendant	7	hazard zone C
3	safeguarded space	8	scrap and expendables flow
4	local controls	9	raw material flow
5	hazard zone A	10	finished goods

Fig. 1. Configuration of an IMS according to ISO 11161:2007 [1].

* Corresponding author: Splaiul Independenței 313, Bucharest 060042
Tel.: 0731299201
E-mail address: *stefan.muresan@upb.ro* (S.C. Muresan)

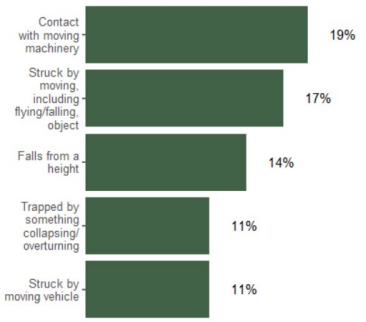


Fig. 2. HSE industrial workplace fatal accidents statistics [10].

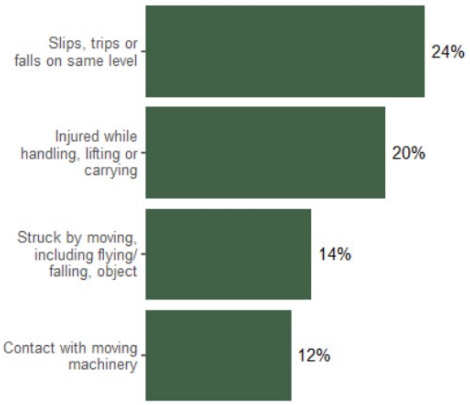


Fig. 3. HSE industrial workplace severe non-fatal accidents statistics [11].

The necessity of high-responsive and fail-safe communication protocols has increased during the previous years due to more complicated, fast demanding and more delicate manufacturing systems in the modern factories. Based on recent studies conducted by the Health Service Executive (HSE, Fig. 2) showed that the highest percentage (19%) of fatal workplace accidents in factories occur because of human contact with moving machinery and equipment [6]. Additionally, 12% of non-lethal but severe workplace accidents happened in the same scenario (Fig. 3). With such alarming statistics, new and durable safety protocols and channels had to become a priority in the field of industrial networks research [7].

Driven by academic research, the Internet of Things has gone beyond basic enabling technologies for the interconnection of smart devices, and researchers are increasingly focusing on the higher-level interoperability of Internet and Web-enabled devices and their services: one of the core challenges for ubiquitous computing research, today, is supporting users toward creating meaningful combinations of physical services for intelligent systems. One of the most critical non-functional aspects of workflow planning, particularly with respect to human agents in HRC settings, is ensuring the safety of the workers involved: any job performed in the workspace may have potential hazards that can affect the human workers or the workspace as a whole [5].

In the rapidly advancing realm of manufacturing, the concept of the “smart factory” has emerged as a groundbreaking innovation, transforming traditional production methods through the use of cutting-edge technologies and automation. Smart factories leverage digitized systems to enhance efficiency, reduce waste, improve product quality, and boost operational agility. However, safety management in these modernized facilities presents significant challenges due to the complexity and automation inherent in contemporary manufacturing processes. One major challenge is the integration of advanced machinery, robotics, and interconnected systems, which can lead to risks such as system failures, errors in human–machine interactions, and hazardous operating conditions. Traditional safety mechanisms, often reliant on manual oversight, struggle to identify and address potential dangers in real-time, particularly in fast-paced and high-risk manufacturing environments. Another critical issue is human error, which remains a primary cause of workplace incidents. Actions such as neglecting safety protocols, failing to use protective equipment, or engaging in unsafe behavior pose serious risks that conventional systems are not well-equipped to handle proactively. To overcome these challenges, advanced safety strategies must be implemented, including real-time hazard monitoring and swift response measures, as traditional approaches often prove insufficient in such dynamic settings.

This paper presents an implementation of a modern communication protocol developed for cost reduction in material and labor and its potential of sustaining strict safety regulations according to recent workplace environments. More than safety process control, the security of user access and control is mandatory for any communication protocol with safety functionalities in order to qualify in the actual requirements. Certain actions and routines should be permitted to trained personnel which has the corresponding credentials for different roles (administrator, service engineer, etc.) [8].

2. INDUSTRIAL COMMUNICATION PROTOCOLS

One of the common communication protocols most used in day-to-day automated processes is Profinet (CBA and IO), a state-of-the-art protocol developed by Siemens AG. Profinet CBA (Component Based Automation) is based on the definition of an object oriented environment in which the relationships between objects (PROFINET components) define the variables that are exchanged on the network. Profinet IO allows to implement a very fast data transfer between controllers and field devices. The protocol is designed to satisfy the most critical requirement of the device level in terms of both periodicity and real time [2].

Profinet IO is a high-speed stable communication protocol which comes with a variety of derivatives of it, with two of the most common being: ProfiDrive, made specifically for controlling frequency drives, and ProfiSafe, dedicated for integration of safety functionalities in an all-in-one controller. Even though Profinet seems to have solved the problem of centralized control unit, it remains the problem of material cost, being necessary separate wires for power supply and signal exchange. Even though Profinet came with a significant material reduction on the signal exchange side, from the classic point-to-point wire transmitted

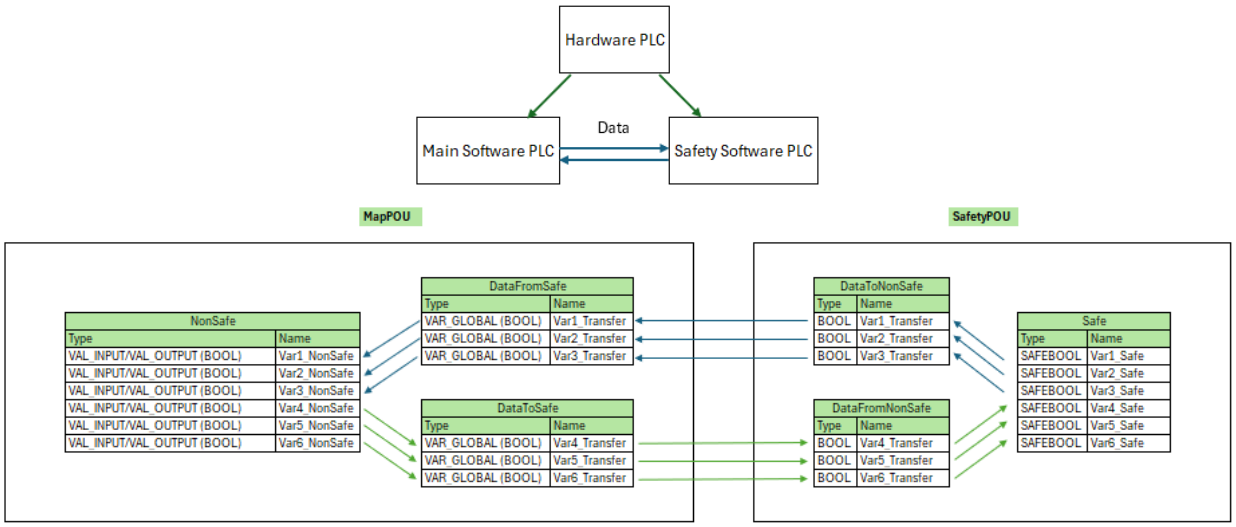


Fig. 4. Configuration of Safety PLC.

signal, to a byte-oriented mono-cable signals exchange, the need for separate power supply for both the control modules and each individually field device.

A new communication protocol comes to solve even this problem. Known as Actuator Sensors Interface or simply AS-Interface, it is a late 90s' communication protocol developed by a group of German companies meant to be integrated in linear and arborescent systems, which integrates both the power supply and the signal exchange on the same cable. It is possible to maintain such capabilities due to usage of Alternative Pulse Modulation phenomena. The APM process has some positive properties that make the use of AS-Interface easy and efficient: the frequency range from 50 kHz to 300 kHz was selected for AS-Interface data transmission, the modulation takes place in the baseband (no carrier frequencies required), the modulation process is DC-free (modulation onto the energy supply possible), the signal is relatively narrow band (good suitability for the transmission properties of the AS-Interface cables), the signal only radiates to a small extent (standard limit values for permissible radiation are safely adhered to without additional shielding) [3].

AS-Interface's mechanical characteristics consists of a specially profiled cable for both the signals and the power supply (in the limit of maximum power of 30 V) of field devices and the specific system architecture required to achieve a correct integration. Because of its common cable for both the signals and the power supply network length is limited by the modulation of the signal appeared with its travel through the cable. Therefore, the reflexion of the signal within the cable increases with the increase of the cable length. For eventual network length increase repeaters can be used to receive the signal and transmit a copy of it further to the network programmable logic controller – PLC. Here the network is limited to the pass of a signal between two repeaters, a higher number leading to severe signal modulation and obtaining *ghost* signals.

3. EXPERIMENTAL STAND

For the purpose of testing and validating a suitable solution for integrating AS-I communication into safety

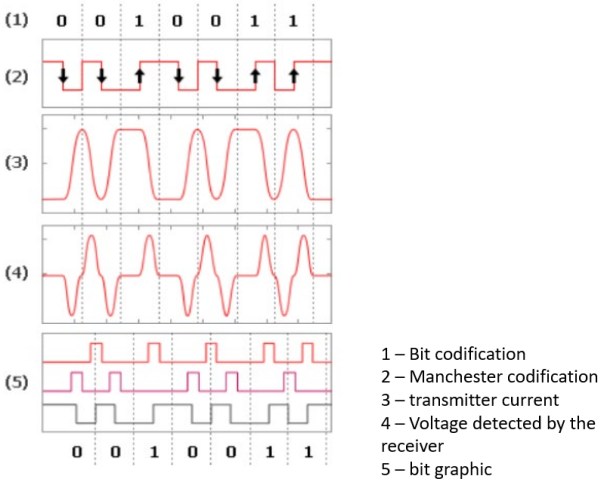


Fig. 5. Variety of signals graphs.

3. EXPERIMENTAL STAND

For the purpose of testing and validating a suitable solution for integrating AS-I communication into safety control systems, an experimental stand has been developed with a series of modern devices. The system is divided into two components: the control cabinet, which has the purpose of controlling and managing all the processes, and the filed devices.

3.1. Cabinet components

The main two devices installed in the control cabinet are the fail-safe PLC with a dual-channel AS-Interface and the dedicated AS-I power supply. In each AS-I system it is required to use a special power supply with the capability of generating an automatic range selection output voltage of maximum 30 V, variation established based on the architecture of the system. For the control part of the system, a fail-safe PLC capable of managing at least one AS-I network was mandatory to achieve all the performance targeted. For that, the AS-I power supply AC1216 and the Fail-Safe PLC with two AS-I networks AC422S were considered to be suitable for the requirements of the system.

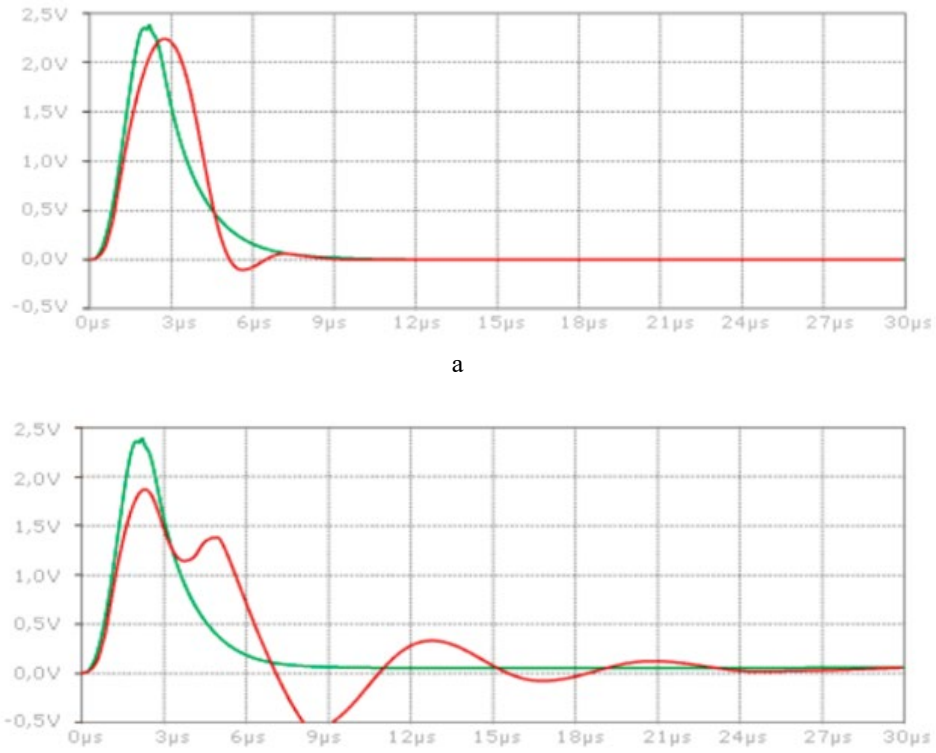


Fig. 6. Signal perturbation: *a* – AS-interface signal in a 100 m network; *b* – AS-interface signal in a 200 m network.

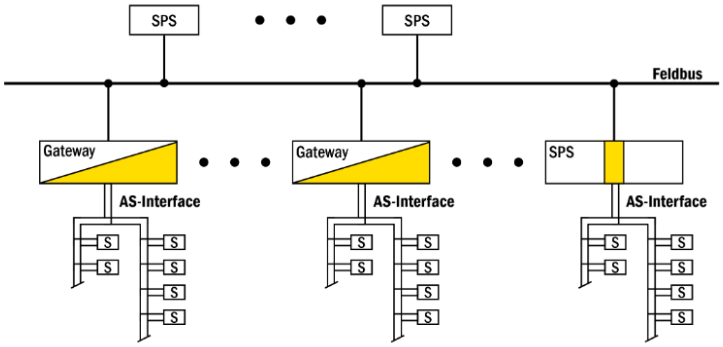


Fig. 7. Basic AS-Interface system architecture.

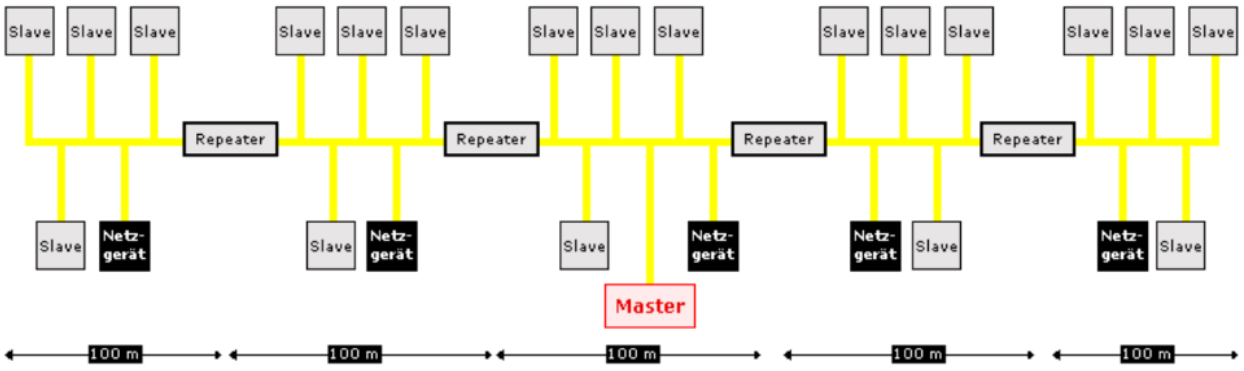


Fig. 8. Extended AS-Interface system architecture.

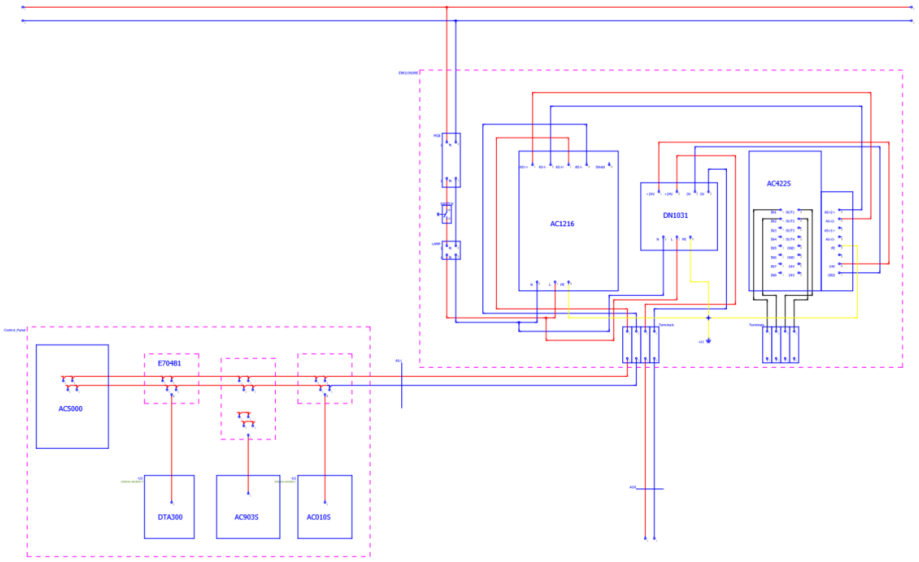


Fig. 9. Electrical Diagram of the system.

Fig. 10. Cabinet components.

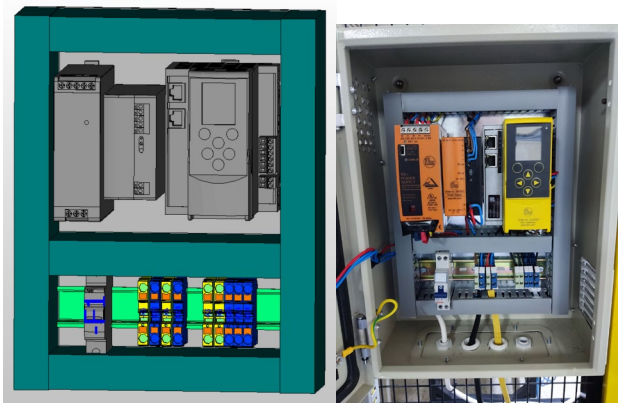


Fig. 11. Digital twin and physical cabinet.

3.2. Field components

For the field devices the selection was made based on the functionalities wanted: an interlock device to prevent the unwanted access in the safety zone (AC903S), an RFID head reader to detect de users IDs and to segregate the personal based on their access rights (DTA300), a dual-confirmation of interlock reactivation to assure no unintentionally interlock activation (AC5000) and a safety emergency device for hazardous situations (AC010S).

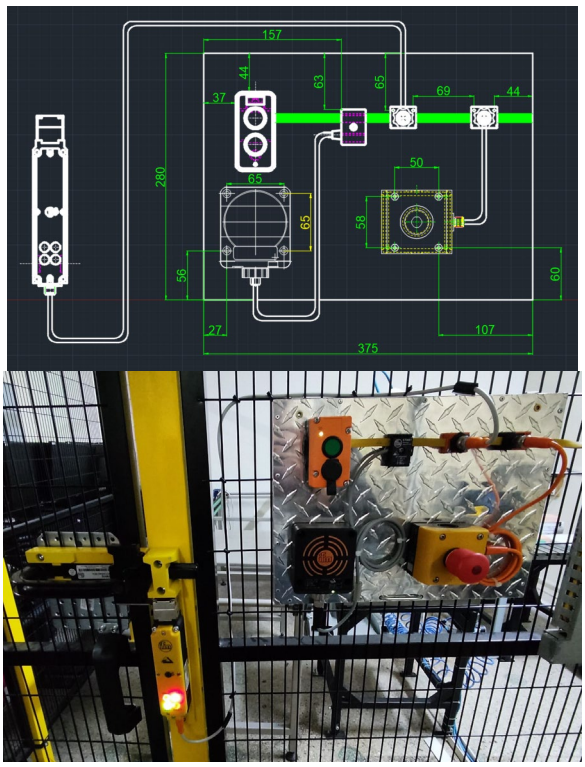


Fig. 12. Digital twin and physical field layout.

4. SYSTEM PROGRAMMING AND MAPPING

4.1. IO Mapping

First and foremost, to be able to do logic programming there is necessary to properly define the signals mapping in the address memories. The AS-I network has its characteristic IO mapping, consisting of a maximum of 64 addresses, denoted as 0A-31A and 0B-31B, correspondingly to each individual device in the network, according to its data exchange size. For example, a basic IO device requires one memory address (for example: 1A), while a complex device which requires more data addresses might occupy a whole slave domain (for example: both 1A and 1B, usually encrypted as S-slave).

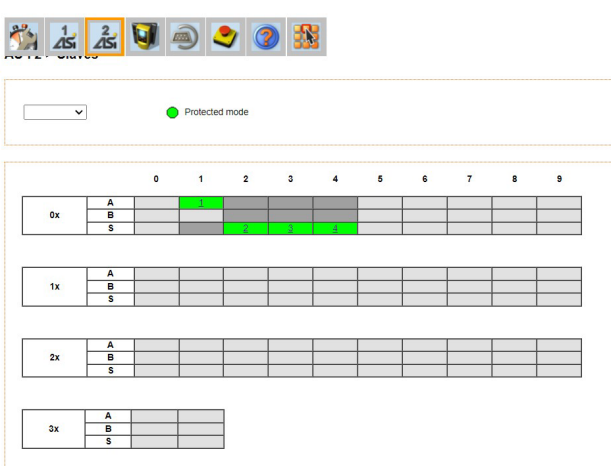


Fig. 13. Slaves IO mapping.

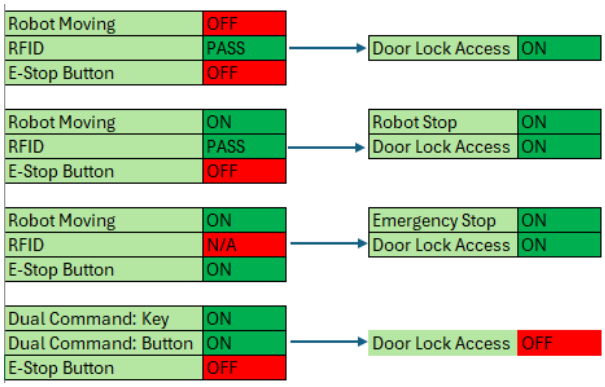


Fig. 14. Cause-effect diagram.

4.2. Logical structure

After the correct device mapping it is necessary to establish the functionality logic to assume proper cover in case of different possible scenarios that can occur during the functionality of the system. For that, a basic cause-effect diagram can check the proper coverage of the system.

4.3. User access

Smart manufacturing systems are an attractive target for cyber attacks, because they embed valuable data and critical equipment. Despite the market is driving towards integrated and interconnected factories, current smart manufacturing systems are still designed under the assumption that they will stay isolated from the corporate network and the outside world. This choice may result in an internal architecture with insufficient network and system compartmentalization. As a result, once an attacker has gained access, they have full control of the entire production plant because of the lack of network segmentation [9].

4.4. Safety programming

A correct programming method starts with the definition of safety functionalities and the integration of safety functions. Due to its fail-safe characteristics, the PLC comes with predefined safety functions such as Emergency Stop STO function or the Guard Locking function. These functions respects all the requirements mentioned in international standards, such as dual-channel monitoring, acknowledgement requirement and self-integrated diagnostics. In addition, the correct correlation between safety and non-safety tags is necessary to perform, to optimize the user-access features and to optimize the cycle-time of the processor.

For the proper access permission of personal, it is necessary to encrypt the access tags with suitable RFID codes based on their access levels. Through this, a database of all users was created and dedicated

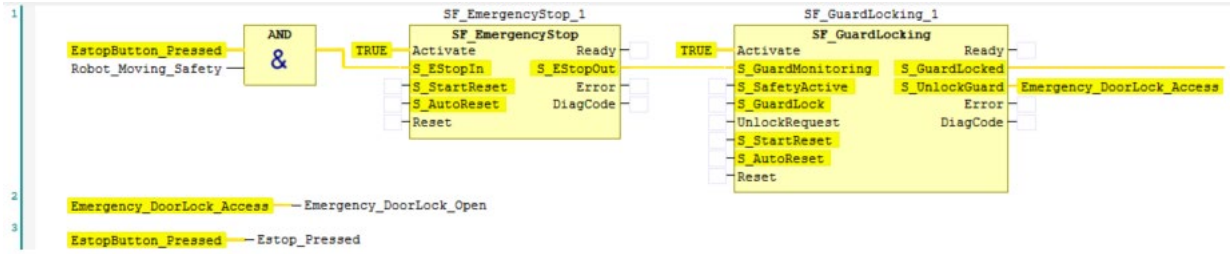


Fig. 15. Safety integrated functions.

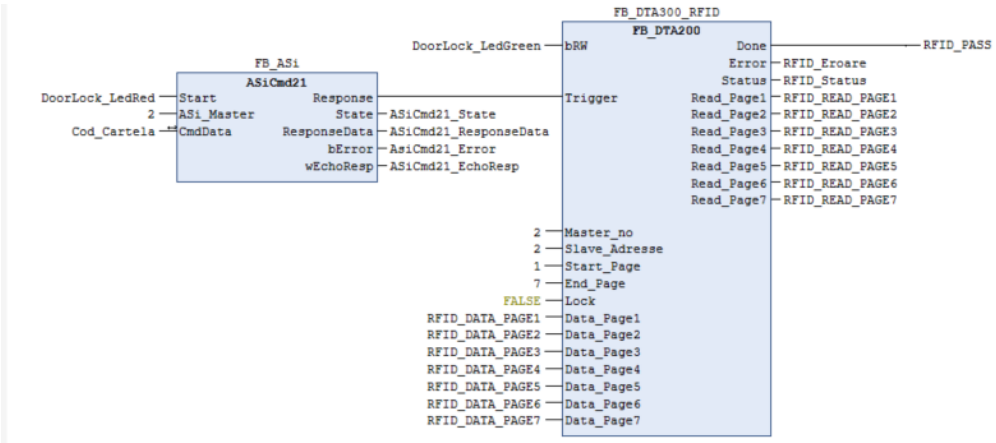


Fig. 16. User access function integration.

functions were used to compare the current user requirements with the database access roles and determine the system modification based on the user's access level.

5. RESULTS

The first validation necessary to be verified is the safety functionality, where different emergency scenarios had to be simulated in order to validate the system, the scenarios were created based on the cause-effect diagram presented in Fig. 14. Besides the usual functionality of the overall system, an important parameter that had to me monitored was the response time of the system, which according to ISO 13849-1 the Performance Level (PL) should in the range 10–50 ms. During multiple attempts a response time was obtained between 20–35 ms, which is validated according to the standard [4].

From the economic point of view, if in the control cabinet the cable cost does not suffer any significant change, on the field side, although, it can be observed a significant reduction in the necessary total length of cable. From a multi-conductor cable for each device (with a ranging length between 0.5 m to 2 m) with a total of around 6.5 m, it only came to a two-conductor profiled cable with a length of 2 m, resulting in a 69.23% cable reduction, representing a massive overall budget optimization.

6. CONCLUSIONS

Following the experimental testing, even though a variation of 41.67% in response time appeared, it still was validated due to presence of all the results in between the required limits, resulting in an up-to-standard system on the safety side.

Due to the modern worldwide economic problems such as increase in raw materials cost, labor shortage, increased delivery time and the severances of competition between companies, optimizing your costs doesn't represent only a matter of profit-margin increase, but a matter of surviving and remaining competitive in today's market. Integrating modern solutions that not only reduces the amount of materials needed to, but also decreasing the installation time and the labor resources allocated while offering a valid solution for integrating the safety functionality, removing any supplemental components such as safety-relay can represent a critical decision that leads to new horizons in a dynamic market.

Even though only a test stand was developed for this study case, it has high scaling potential, with large industrial systems that can easily be compatible with solutions of this kind, mainly in intra-logistics, warehouse management, food and beverage, automotive, etc.

In conclusion, the integration of systems comparable with the one tested aim to represent the switch from the classic multi-cable point-to-point safety systems to a more dynamic and customizable AS-Interface system, with multiple benefits both economically and functional.

REFERENCES

[1] ISO 11161:2007, available at: https://www.iso.org/standard/35996.html, accessed: 2025-09-25.

[10] Specified, reportable injuries to workers, https://www.hse.gov.uk/riddor/specified-injuries.htm.

[11] LFS estimated annual average 2019/20-2021/22, https://www.hse.gov.uk/statistics/lfs/tables.htm.

[6] HSE Fataly Workplace Accidents, available at: https://ifr.org/downloads/press2018/2022_WR_extended_version.pdf, accessed: 2024-10-11.

[7] HSE Severe Non-Fataly Workplace Accidents, available at: https://www.hse.gov.uk/statistics/industry/manufacturing.pdf, accessed: 2024-10-11.

[5] A. Shafei, J. Hodges, S. Mayer, *Ensuring Workplace Safety in Goal-based Industrial Manufacturing Systems*, Procedia Computer Science, pp. 90-101, Volume 137, 2018.

[8] Z. H. Haghighat, A. Islam, H. Karimipour, B. M. Fard, *An explainable big transfer learning approach for IoT-based safety management in smart factories*, Internet of Things, pp. 90-101, Volume 31, 018.

[2] P. Ferrari, A. Flammini, S. Vitturi, *Performance analysis of PROFINET networks*, Computer Standards & Interfaces, pp. 369-385, Volume 28, Issue 4, April 2006.

[3] AS-Interface Organization, available at: https://www.as-interface.net/, accessed: 2025-09-26.

[9] F. Maggi, M. Balduzzi, R. Vosseler, M. Rösler, W. Quadrini, G. Tavola, M. Pogliani, D. Quarta. S. Zanero, *Smart Factory Security: A Case Study on a Modular Smart Manufacturing System*, Procedia Computer Science, pp. 666-675, Volume 180, 2021.

[4] ISO 13849:2023, available at: https://www.iso.org/standard/73481.html, accessed: 2025-09-28.