

*Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria*

## Integration of safety and security in railway systems

Leonardo J. Valdivia a, Saioa Arrizabalaga b, Javier Añorga b, Jon Goya b, Iñigo Adin b, Jaizki Mendizabal b\*

<sup>a</sup>Universidad Panamericana. Facultad de Ingeniería. Prolongación Calzada Circunvalacion Poniente 49, Zapopan, Jalisco, 45010, México

<sup>b</sup>CEIT and Tecnun (University of Navarra), San Sebastian, Spain

### Abstract

Security is gradually taking center stage. Since traditional transport systems were based solely on mechanical or electromechanical devices and closed networks, today with an increasing number of information technologies and communications devices, systems are being migrated towards new communication technologies and open protocols. Although this has increased the efficiency and reduced costs to companies, the systems have become more vulnerable to external attacks. And railway is not an exception, its infrastructure is mainly based on computers that are interconnected via wired or wireless networks and it is highly distributed, therefore railway's infrastructure is difficult to protect and it is vulnerable to cyber-attacks.

This work shows an analysis about the standards used in security. A comparison with safety norms and the main reasons why security is currently not considered when developing safety critical devices are also described. Finally, an example of safety and security integration is presented.

**Keywords:** safety; security; integration; cyber-attacks, railway.

---

\* Jaizki Mendizabal. Tel.: +34 943 212800.  
E-mail address: jmendizabal@ceit.es

## Nomenclature

|      |  |
|------|--|
| CRC  | Cyclic Redundancy Check                                |
| ETCS | European Train Control System                          |
| IDS  | Intrusion Detection System                             |
| ISA  | International Society for Automation                   |
| ISO  | International Organization for Standardization         |
| IT   | Information Technology                                 |
| I&C  | Information and computation                            |
| RAMS | Reliability, Availability, Maintainability, and Safety |

## 1. Introduction

Safety is defined as “the degree to which accidental harm is prevented, detected, and reacted to” (Firesmith D. G, 2003). On the other hand, security is “the degree to which malicious harm is prevented, detected, and reacted to” (Firesmith D. G et al. 2003). An example of safety are the automatic doors, they open fast and close safely behind you. If you walk slower than the programmed time, built-in sensors will make certain that the door does not close on you, avoiding that you get hurt. Conversely, the passwords are a security example; they were created to avoid any unauthorized access to mail, bank accounts, PC accounts, etc. One component of security is cybersecurity that focuses on protecting, computer, networks and data from unauthorized access.

Railway is a safety critical application, as a failure has a relevant impact on human beings. To ensure safety in railways, a control system is required; signaling systems, such as European Train Control System (ETCS), fulfill that purpose. ETCS is a European standard created to develop a common interoperable platform for railways, authority and signaling systems. The creation of a common control system, ETCS, arises from the need of unifying and ensuring train interoperability regarding the train control and command systems.

The railway infrastructure is mainly based on computers systems that are interconnected via wired or wireless networks, which means that railway transport is vulnerable to cyber-attacks. The railway infrastructure is highly distributed, therefore it is difficult to protect, and it was designed before having to deal with threats and risks to sensitive data networks.

This research work has been carried out with two objectives: first, to analyze the current state and problems of security in the railway sector; second, to propose a solution to integrate a security mechanism such as IDS (Intrusion Detection System) with a safety critical application.

## 2. State of the art and current problems

### 2.1. Safety standards

Currently, all the railway signalling systems manufacturers dedicated to high speed in Europe have to be compatible with ETCS. The development of any railway product has to meet the standards and tests specified by ETCS. All devices designed following the ETCS norms must be safety critical, which means that errors must not occur and they must be fault tolerant.

The European EN-5012x family of railway standards govern the development of safety railway systems. These norms specify design rules and testing in order to attain a particular safety specification, which guarantees that the system continues to fulfill its safety requirements in case of random failure. Fig. 1 shows the EN-5012x standards and their main features:

- EN-50126 (EN50126, 2010): this standard defines a process, based on the system life-cycle and tasks within it, for managing Reliability, Availability, Maintainability, and Safety (RAMS).
- EN-50128 (EN50128, 2012): it specifies procedures and technical requirements for the development of programmable electronic systems, which are used in railway control and protection applications.

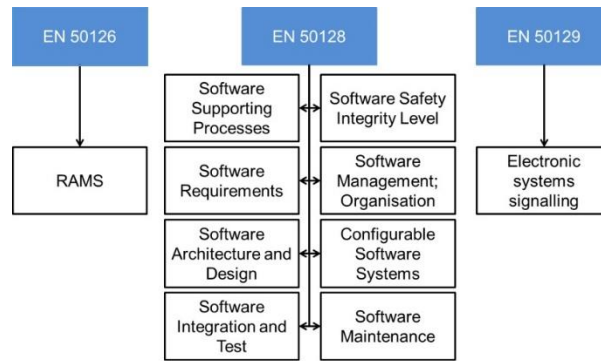


Fig. 1 Safety standards for railway industry

- EN-50129 (EN50129, 2010): this standard applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete signalling systems.

## 2.2. Security standards

The evolution of traditional information and communication technology has created a new technological age. These advances have improved companies' efficiency; however, they also bring new challenges and expose the systems to cyber-attacks. In order to enhance security, some standards provide design recommendations to avoid attacks. Fig. 2 shows the relationship among the security standards, they are separated by publisher, International Organization for Standardization (ISO) or International Society for Automation (ISA).

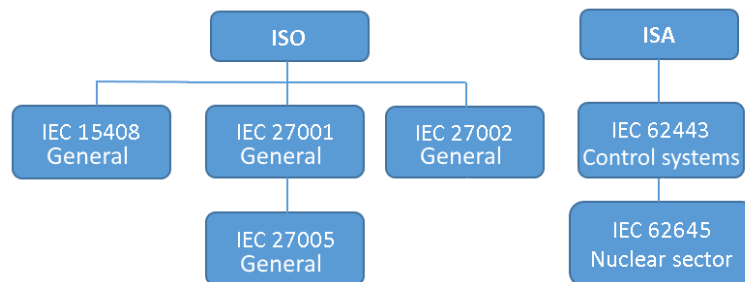


Fig. 2 Relationship among the security standards

- IEC-15408 (IEC 15408, 2009): it is an international standard that established the general concepts and principles of Information Technology (IT) security, it is also called "security common criteria". This standard is used as the basis for evaluating the security properties of IT products. It addresses the assurance levels applied to security management and the related criteria for evaluating such assurance levels.
- IEC-27001 (IEC 27001, 2005) and IEC-27002: they are international standard for Information Security Management Systems (ISMS). They specify the requirements for establishing, implementing, maintaining and improving an information security management system. These standards are the top-level documents of a series of standards that includes IEC-27005 (IEC 27005, 2008), which specifically addresses information security risk management.
- IEC-15408 (IEC 15408, 2009) and IEC-27001 (IEC 27001, 2005): are generic standards, i.e. they state how to apply security but in general, they are not focused to a specific sector or industry. Alternatively, the IEC-62443 (IEC 62443, 2013) (also known as ISA-99) is a series of security standards for industrial automation and control systems. Fig. 3 details all the standards of the IEC-62443 (IEC 62443, 2013) family (most of the standards are under development).
- IEC-62645: it establishes requirements and provides guidance for the development and management of effective security programmes for I&C computer-based systems for nuclear plants.

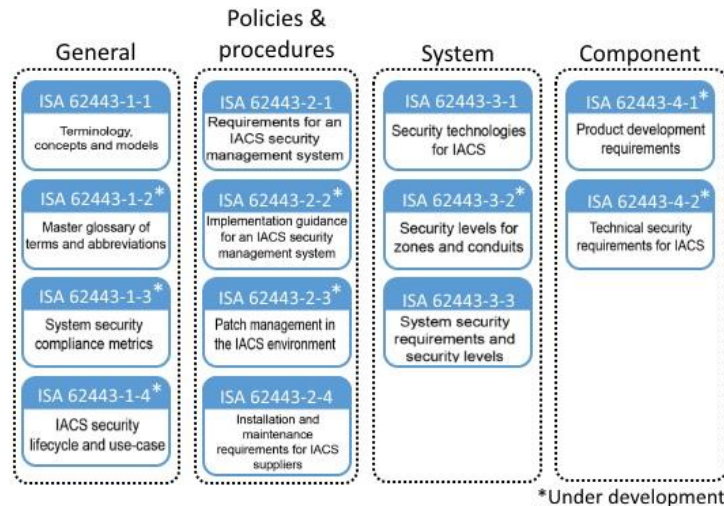


Fig. 3 ISA-62443 work products

### 2.3. Current issues

There are many reasons why security is not implemented or even considered in railway industry, some of these reasons are explained below:

Currently, if any manufacturer wants to implement its product in railway industry, it is necessary to meet the required safety level, so manufactures need to follow the safety standards in order to design railway equipment. However, it is not necessary to meet any SL to implement the equipment in railway, thus railway manufactures do not necessary follow the security standards.

In addition to the problems, professionals who develop safety railway modules are often not aware about the security issues, so if any security technique is implemented, this is done after the development of the system or module. And this can be also translated to safety: many of the security experts do not deal with safety. This lack of mutual understanding between safety and security complicates the implementation of security.

Moreover, as Fig. 2 shows, the ISO security standards are generic, and only the IEC-62645 is designed for a particular sector (nuclear). Even the IEC-62443 (IEC 62443, 2013) is for automation and control systems for all industries, i.e. there are not security standards for railway industry. The railway sector should use general standards, so it is possible and probable that each sector interprets the norms differently. This does not happen with safety, where there are specific standards for almost all sectors including railway.

Finally, even if a manufacturer decides to consider security in the development of a safety device, there are technical problems. These problems are listed below:

- Any hardware or software that performs safety critical functions needs to be safety certified. If security and safety modules are integrated, it is very difficult to achieve the certification, as security modules are not designed with respect to safety standards.
- Even if the safety certification is achieved including a security system, there is another issue, new cyber threats appear daily (ENISA, 2016), so security modules need to be updated to ensure protection. If any change is applied to a safety certified system, it must be certified again. Therefore, it is unfeasible to certify each time that the security module is updated.
- Some safety protocols (as PROFIsafe) recommend the usage of encryption and authentication solutions, however there is not an obligation. Then, there are multiple devices working with unencrypted protocols. If security is added, these protocols need to accept encrypted messages, which adds processing time (encryption, decryption) that can significantly affect real-time tasks (K. Hansen, 2009).

### 3. Safety design approaches

With the problems explained in the previous section, it is clear that any security module that is used in railway should not perform critical tasks (to avoid safety certification) and must be able to be update. To achieve this, the

security module should be physically separated from safety modules, i.e. the security functions are isolated from safety functions.

Additionally, safety standards allow two design approaches, black channel and white channel. In the white channel approach, entire communication channel including its interfaces compiles with the requirement of safety standards. In the black channel approach, there is no available evidence of design or validation according to the safety standards (K. Hansen, 2009). However, the data and the connected elements must have built-in mechanisms to detect any interference (A. Elia et al. 2016). Hence, the EN-50129 (EN50129, 2010) states that if a layer with safety built-in mechanisms is added to the communication protocol, safety certified devices and non-certified devices can share the same network. Fig. 4 shows this architecture.

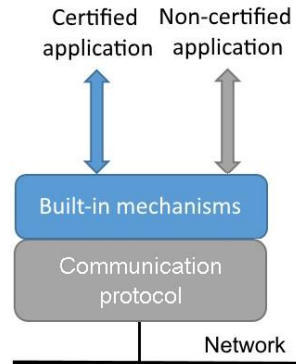


Fig. 4 Black channel architecture

### 3.1. Built-in mechanisms

The built-in mechanisms or safety measures that should be added to the communication protocol in order to use the black channel approach are mentioned below (A. Elia et al. 2016):

- **Cyclic Redundancy Check (CRC):** it is common that other layers already contain a CRC but they are not valid, an extra CRC have to be used.
- **Time stamp:** a time value is added to all the messages, normally this value is the message transmission time, but it is possible to use other reference.
- **Sequence number:** a consecutive number is appended to the protocol and it is incremented from message to message.
- **Timeout:** the message has to be received between two times, not before and not after.
- **Acknowledgment:** an echo is send to the source of the message to confirm the reception.
- **Authenticity:** a unique identifier for the sender and receiver has to be added.

Table 1 shows how the built-in mechanism added to the top of the communication protocol help to prevent different kind of failures, although the main objective of the mechanisms is to ensure safety, the security is also improved. For example, a sequence number is added to each message, if any external attack injects messages without the correct number, they will be ignored.

Table 1 Built-in mechanisms for failure detection

| Failure          | CRC | Time stamp | Seq. Number | Timeout | Echo | Authenticity |
|------------------|-----|------------|-------------|---------|------|--------------|
| Insertion        |     |            | X           |         | X    | X            |
| Wrong sequence   |     | X          | X           |         |      |              |
| Loss             |     |            | X           |         | X    |              |
| Delay            |     | X          |             | X       |      |              |
| Repetition       |     | X          | X           |         |      |              |
| Wrong addressing | X   |            |             |         |      | X            |
| Masquerading     |     |            |             |         | X    | X            |
| Corruption       | X   |            |             |         | X    |              |

#### 4. Safety-security integration

Safety and security, although distinct, share the main objective, reduce and if possible eliminate risk. To achieve certain level of safety it is necessary to follow EN-50129 (EN50129, 2010). If an electronic module needs to be used in a critical application, it is necessary to certify that module following the safety standards, but these standards do not consider security in their scope. Therefore, there is no guide to include security in a safety module.

With the challenges explained in subsection 2.3, it is clear that the security module should not perform critical tasks and must be able to be updated. To achieve this, the security module should be physically separated from safety module, i.e. the security functions are isolated from safety functions.

Therefore, based on the black channel approach presented in the previous section, Fig. 5 shows the proposed solution. The security module is a IDS connected to the network to detect anomalies or intruders, the mechanisms added to the communication protocol allows to include a security module even if it is not safety certified.

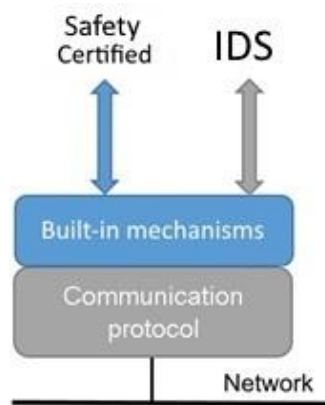


Fig. 5 Safety-security integration

The advantages of this architecture are mentioned below:

- Third party IDS can be used, and moreover multiple IDS with different features can be added to diversify security.
- The security module (IDS) is physically separated from the safety module, hence the security can be updated without affecting the safety certification (K. Hansen, 2009).
- The security module does not need to be safety certified and it does not affect the certification of the safety module.

The inclusion of the IDS in the presented system has been done following the safety standards. These standards allows sharing the communication network with non-certified systems as long as safety measures are added to the top of the protocol. Hence, the proposed redundant system integrates a security mechanism without affecting the safety certification. Another important feature is the possibility to update the security mechanism (IDS) without changing the safety submodule, and then the safety certification is not affected.

The integration of an IDS with a safety sub-module is the first step to achieve that safety and security coexist. There are many other security mechanisms that can provide a greater protection to a system, such as: data encryption, code, identity based networks, etc. However, these security techniques are not compatibles with safety certifications. E.g., if an encryption mechanism is added to a safety communication, the time to encrypt a message and the time to decrypted it, must be considered, and for real time systems this delay affects directly the performance and in consequence the safety certification is also affected.

## 5. Conclusion

Railway applications should be safe and secure. Which means that safety and security need to work together. Safety has general and specific standards to achieve the desired safety level of an electronic module that will be used in railway. Conversely, in cyber security there are only recommendations to follow and general norms. This means that each manufacturer should include their own criteria to follow or not the standards. It is very difficult to reach an optimum level of security, because the norms recommend different approaches, and if a manufacturer achieves an acceptable security level, it is very complicated to apply the same solution to other modules. Then, they cannot be applied to the whole railway system.

The proposed architecture shows how to integrate a security module to a safety certified system in order to improve reliability. By using the built-in mechanisms, the safety module can be certified and the security module does not need to be safety certified (which is time consuming and expensive, since security modules do not follow any safety standard). Furthermore, the security module can be updated (a very important feature, since new threats appear daily) in any moment and the safety module is not affected, so it does not required being re-certified. The integration of an IDS with a safety module is the first step to achieve the coexistence of safety and security.

## 6. References

- Firesmith D. G, 2003. Common Concepts Underlying Safety, Security, and Survivability Engineering, Carnegie Mellon.
- CENELEC. 2010. EN50126, Railway applications. The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
- CENELEC. 2012. EN50128, Railway applications. Communication, signaling and processing systems - Software for railway control and protection systems.
- CENELEC. 2010. EN50129, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling.
- International Organization for Standardization. 2009. IEC 15408, Common Criteria for Information Technology Security evaluation.
- International Organization for Standardization. 2005. IEC 27001, Information technology - Security techniques - Information security management systems – Requirements.
- International Organization for Standardization. 2008. IEC 27005, Information technology - Security techniques - Information security risk management.
- International Society for Automation. 2013. IEC 62443, Industrial Automation and Control Systems Security.
- ENISA. 2016. The cost of incidents affecting CII.
- K. Hansen. 2009. Security attack analysis of safety systems. IEEE Conference on Emerging Technologies and Factory Automation.
- A. Elia, L. Ferrarini, and C. Veber. 2006. Analysis of Ethernet-based safe automation networks according to IEC 61508. IEEE International Conference on Emerging Technologies and Factory Automation.