Practical Experiences with real-world systems: Security in the World of Reliable and Safe Systems

Nuno Silva
Project Management Office - ASD
Critical Software S.A.
Coimbra, Portugal
nsilva@criticalsoftware.com

Rui Lopes
Aeronautics, Space and Defense
Critical Software S.A.
Coimbra, Portugal
rmlopes@criticalsoftware.com

Abstract— **Reliability and Safety have always been associated to Safety Critical Systems. Since the failure of a Safety Critical System may lead to loss of human lives or large economical effects, the standards that guide the development of these systems have always focused in these two aspects, independently of the domain applicable. By looking into Reliability and Safety independently and focused, one can design a system highly reliable and safe without Security concerns. However, Security plays a major role in the achievement of both Reliability and Safety. A system cannot be reliable and safe if it is not secure. Therefore, the current processes to certify a Safety Critical System also address Security aspects, together with Reliability and Safety. This work presents the activities that have been performed in the scope of the certification of a Safety Critical System in the railway domain and how Security is tackled without jeopardizing Reliability and Safety. The data collected and its importance for guaranteeing safety, reliability and security is presented and discussed. A relationship between the activities performed and the standards concerns is established and examples of architecture decisions that could provide more Reliability and Safety but less Security will be presented.**

Keywords-component; Reliability, Safety, Security, railway, Data Analysis, safety critical, signalling system

I. INTRODUCTION

Reliability and Safety are frequently associated to Safety Critical Systems. It is known that the failure of a Safety Critical System may lead to loss of human lives or large economical effects, by its own definition and by the nature of those systems, so, the standards that guide the development of these systems have always focused in these two important aspects, whatever the vertical market is.

When talking about safety-critical systems one can think about aeronautical systems, automotive control systems, medical devices, nuclear power plant systems, defense and homeland security systems, just to name a few. The growth of importance, usage, complexity of these systems has brought new challenges to the stage. Not only the safety part is important, but the security properties are having a more and more important role, especially with the "cloud" and the ubiquitous connection of systems (system to system, system to internet, etc). John Knight [1] had already identified the growing importance of Information Systems Security, taking into account the effects that security problems have on the systems (availability, information theft, service disruption, financial losses) and that in some cases these will end-up becoming safety related problems.

Just to provide an example of the importance of security related to safety, in 1982, a system controlling the trans-Siberian gas pipeline (allegedly implanted by the CIA) caused the largest non-nuclear explosion in history. The CIA, allegedly discovered that Soviet spies planned to purchase secretly a gas pipeline controller developed in Canada, and planted a Trojan horse (logic bomb) in the controller's software. Once it was installed on the pipeline, the controller ran a test of the pipeline's pressure gauges during which the logic bomb reset the gauges to the double of gas pressure in the pipeline. The resulting explosion was, then, the largest non-nuclear explosion ever seen from space.

As a more generic example, a railway signaling system is a system to control railway traffic in a safe way, especially to avoid train collisions on the track. These systems use train and track equipment information for supporting traffic management and infrastructure control. Since trains can only operate in fixed rails, cannot stop quickly and usually operate at a speed that will not easily let them stop at sighting distance, they become susceptible of collisions.

Several standards and regulations do exist to force requirements on implementation of signaling systems ([3], [4]). These systems must at least be able to implement Automatic Train Protection (ATP) functions, optional Automatic Train Operation (ATO) and Automatic Train Supervision (ATS) functions, as defined in the IEEE 1474 standard[2].

A signaling system is simply train control activities that involve movement authorization being passed from a responsible at each section of a rail network (for example, a signalman or stationmaster) to the train driving personnel. There is a set of rules and support from physical equipment used to accomplish these tasks.

These systems are based on the exchange of very precise and important information. They are safety-critical, but also quite "exposed" to security threats that might affect the data sent, transmitted and received and thus have a harmful effect on the decision taken, train movements, etc.

978-1-4799-0181-4/13/$31.00 ©2013 IEEE

A recent accident, where 40 people were killed and about 190 injured, occurred on 23 July 2011, two high-speed trains travelling on the Yongtaiwen railway line collided on a viaduct in the suburbs of Wenzhou, Zhejiang province, China. The official investigation blamed faulty signal systems which failed to warn the second train of the stationary first train on the same track, but also management failures on the part of railway officials in carrying out the proper procedures.[8]

II. RAILWAY CERTIFICATION

A safety-critical system is usually defined as "A system in which any failure or design error has the potential to lead to loss of life." [7], it is generally a computer or electronic system where a failure can have a negative effect such as cause injuries or kill human beings.

For the railway signaling systems implementation, where an error can cause injury or death of people inside or outside the train, there are international standards that intend to guide the implementation and certification prior to operation. The objective of these standards is not only to have a uniform way of implementing but also a uniform high level of resilience, and thus safety and security.

The CENELEC standards for railway safety and dependability are composed by the following three main standards:

- EN 50126 / IEC 62278 (Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability and Safety (RAMS))
- EN 50128 / IEC 62279 (Railway Applications - Communications, Signaling And Processing Systems - Software For Railway Control And Protection Systems)
- EN 50129 (Railway Applications - Communication, Signaling And Processing Systems - Safety Related Electronic Systems For Signaling)

These standards are today mandatory in Europe, and they define a probabilistic approach for railway systems safety engineering and systems operations. Their worldwide equivalents are ISO-IEC standards, basically with the same requirements. They provide for example detailed information about the requirements for the life-cycle approach, safety management and RAMS. These standards cover the systems, applications, software and hardware safety properties of railway systems.

Railway systems certification needs to follow the requirements specified in these standards, and this is taken very seriously with quite formal evidences reviews, meetings, gap analysis, safety cases, etc. The system's developers must provide evidences of clear and effective Engineering Safety Management systems, and specific proof regarding the development and demonstration of safety properties/requirements and performance targets.

The activities proposed by the CENELEC standards are in-line with the ones proposed in other domain safety critical standards. Hereafter are described the main activities that must be performed.

A. *Failure Modes and Effects Analysis (FMEA)*

The FMEA analysis is rather common in Safety Critical certifications or qualifications since it provides a complete assessment of all possible failure modes of the system components and their effects at system level. Following a bottom-up approach, the output of the analysis is a worksheet containing the end effect of a failure in each system component, based on a predefined list of failure modes. The following list presents a set of generic failure modes that are usually considered in a FMEA analysis:

- Function fails to perform;
- Function performs incorrectly;
- Function performs prematurely;
- Function performs belatedly.

Other failure modes shall be considered in a case by case approach, whenever applicable and relevant. The following table provides an example of a possible FMEA worksheet fields.

Table II-1: FMEA worksheet example

Field Name	Description
FMEA ID	An unique identification number, assigned for traceability purposes.
Component ID / Function	The identification of the component being analyzed. A concise statement about the function performed by the item (component).
Failure Mode	Identification and description of all potential failure modes of the item or function under analysis.
Failure Cause	Identification and description of the most probable cause associated with the assumed failure mode.
Local Effects	The impact of the failure mode on the operation, function, or status of the item identified in the second column (Component ID).
End Effects	The final effect of the failure mode on the system. The data contained in this field refers to the failure mode effects before the implementation of the compensating provisions.
Compensating Provisions	Recommendations proposed in order to mitigate the propagation and occurrences of component failures. These recommendations intend to mitigate or eliminate the probability of a catastrophic end effect.

Note that some tailoring can also be performed in order to better address the system being analysed. The importance of this activity in the scope of security will be described in later sections of this paper.

B. *Fault Tree analysis (FTA)*

The FTA analysis also aims to identify failure events that lead to top level (i.e. system level) feared events. Following a top-down approach, a set of top level feared events is identified, leading to the production of fault trees. The fault trees are composed by all the lower level failure events that lead to the feared top level event.

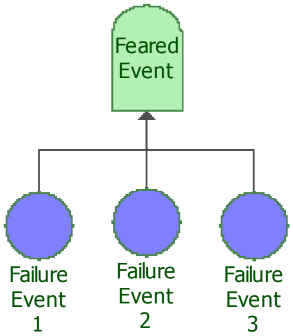

Figure II-1: Fault tree example

The importance of this activity in the scope of security will be described in later sections of this paper.

III. Case Study

The system analysed in the scope of this paper is an interlocking control system for the railway industry (this is a very common type of signaling system). This system has been designed from the beginning, including the electronics boards that constitute the system and its main function is to ensure safe interlocking management and control. The system shall be deployed in the railway track and interface with other identical interlocking systems deployed on adjacent interlocks. The system also interfaces with external controlled inputs (e.g. railway signals) and the centralized Traffic Control Centre.

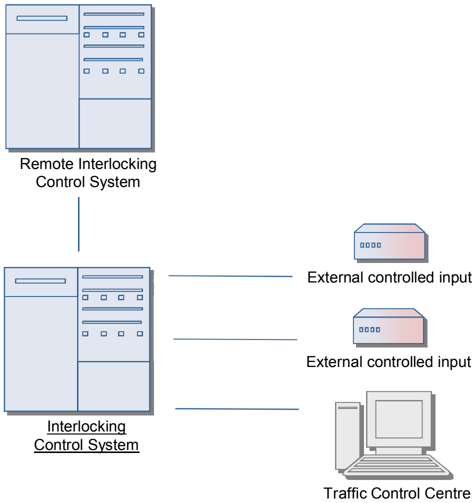
Remote Interlocking Control System
External controlled input
External controlled input
Interlocking Control System
Traffic Control Centre

Figure III-1: Interlocking Control System interfaces

The Interlocking Control System must be certified according to the CENELEC standards referred in the previous section. Since the system is composed by both hardware and software, certification on both areas is applicable. The following system characteristics allow to have an idea of the size and complexity of the Interlocking Control System:

- Composed by 6 electronics boards;
- Defined by 130 system requirements;
- Designed into 25 system functions;
- Implemented by 25000 lines of code.

Since the failure of an interlocking system may lead to loss of lives, its development is ruled by the standards described in the previous section. The main top level feared events of the system are:

- Collision between trains;
- Collision with non-railway traffic;
- Derailment of trains.

These feared events are the main subject of analysis of the safety assessments. However, the same feared events shall be considered in the scope of the security assessment. The approach followed was to integrate safety and security in the same analysis, by defining both safety and security failure modes.

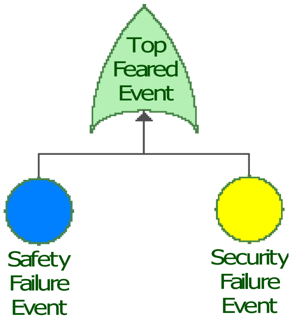

Figure III-2: Integrated Safety and Security analysis

The following activities have been performed in the scope of the system certification under CENELEC standards:

- Functional Analysis;
- RAM Prediction;
- FMEA;
- FTA.

The results of these analyses in the scope of Security and Safety integrated assessment are presented in the following section.

IV. Results

The results of the Reliability and Safety analysis are hereafter summarized:

- Four main FTAs have been developed, representing a total of around 80 events analysed.
- Around 130 FMEA lines have been produced;
- RAM Prediction has been performed based on the modeling of a total of 16 equipment units.

Several security failure modes and failure events have been identified throughout the certification process and included in the Reliability and Safety analysis. The results of these inclusions had significant impact on design decisions. The following high-level security failure events have been identified:

- Unauthorized on-line access;
- Unauthorized on-site access.

The following figure presents a section of one of the FTAs developed in the scope of this project in which is clearly visible the way security concerns have been integrated in the safety FTA:

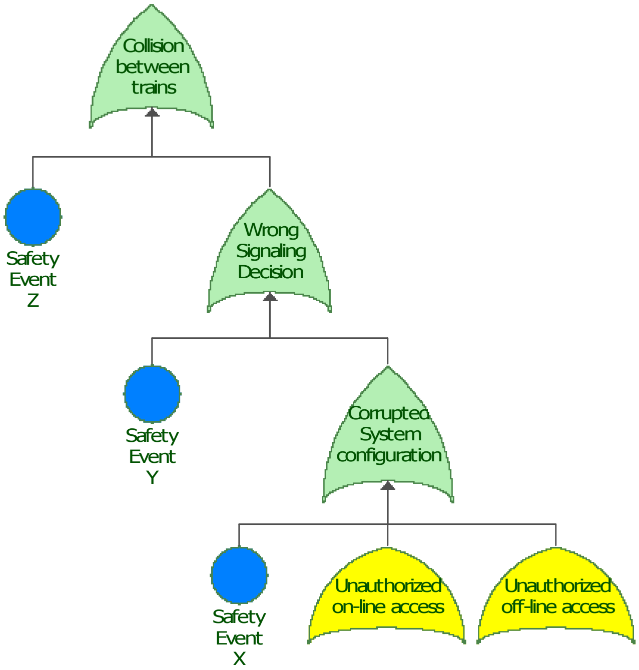

Figure IV-1: FTA section with security failure events

These security failure events have been broken-down into lower-level failure events that have been added to the Safety FTAs:

- Unauthorized on-line modifications to the Interlocking System configuration;
- Unauthorized on-site modifications to the Interlocking System configuration;
- Unauthorized on-site corruption of input signals from external controlled input equipment;
- Unauthorized on-site corruption of output signals to external controlled input equipment.

These failure events have been added to the Safety FTA. Also, the following failure modes have been considered in the Safety FMEA, whenever applicable:

- Function performs incorrectly after unauthorized access.

Due to the inclusion of security related failure events and failure modes in the FTA and FMEA analysis, the following design constraints have been defined:

- Protection from on-line unauthorized accesses:
  - Interlocking system connected to a segregated network. No access to the internet.
  - Not possible to modify configurations remotely. Authorized personnel must go on-site and upload new configuration.
- Protection from on-site unauthorized accesses:
  - Railway tracks protected by security infrastructure: no non-authorized personnel are allowed in the premises.
  - Interlocking system placed in secure room with access control.

Other design constraints identified by the nominal safety analysis could also be traced to security failure events and failure modes, demonstrating the importance of considering security concerns in Safety Critical Systems certification process. Without the design constraints referred above, the lack of security could have led to the triggering of a top level feared event, jeopardizing the safety of the system.

V. Conclusions

Safety-Critical systems, such as railway signaling applications/systems, besides being intrinsically safety oriented, might also suffer from security threats and vulnerabilities. The security issues, when explored by malicious entities, end up in severe safety effects. Not only security exploration leads to loss of money, unavailability of systems, disruption of service, stealing important and sensitive information, but they also cause severe problems that can endanger humans by hurting or killing.

In this specific case, following a certification process, based on mature international standards is essential. This leads to the usage of appropriate processes, methods and tools, and to the creation of evidences that all safety, security and reliability properties/requirements are met and/or exceeded. The objective is to achieve a resilient architecture that will not end up by harming neither passengers, nor operators, nor other external entities.

Due to the particular nature of the security issues, and the specific impact they might have towards safety and dependability, we recommend that these analysis are always performed in conjunction with safety experts and included in the process explicitly. Security experts must be involved in the safety-critical projects, certainly not alone, but they can have a very important contribution towards guaranteeing safety.

The strategy followed for this case study was to perform an integrated safety and security approach, by integrating security related failure modes into FMEA and failure events into FTA. The results obtained by integrating security concerns into these analyses lead to the identification of design constraints that would not have been derived from safety concerns. The approach has proven to be useful and adequate to the system at hand. Other systems may require different approaches, based on their core design goals.

The case study presented in this paper has demonstrated that Safety cannot be achieved without Security. Therefore, it is essential that security concerns are incorporated in certification process of Safety Critical Systems. Different approaches may be followed to perform safety and security assessments, whether in a more integrated or segregated perspective. Nonetheless, there is no question that security shall play a major role in the design of the future Safety Critical Systems.

ACKNOWLEDGMENT

This work has been partially supported by the European Project FP7-2012-324334-CECRIS (CErtification of CRItical Systems).

REFERENCES

[1] John C. Knight, “Safety Critical Systems: Challenges and Directions”, ICSE '02 Proceedings of the 24th International Conference on Software Engineering, pp 547-550, ISBN:1-58113-472-X, 2002.

[2] IEEE Standard for CBTC Performance and Functional Requirements (1474.1-1999). IEEE Rail Transit Vehicle Interface Standards Committee of the IEEE Vehicular Technology Society, 1999.

[3] Regulation of Railways Act 1889, UK.

[4] EN 50126 / IEC 62278 (Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability and Safety (RAMS))

[5] EN 50128 / IEC 62279 (Railway Applications - Communications, Signalling And Processing Systems - Software For Railway Control And Protection Systems)

[6] EN 50129 (Railway Applications - Communication, Signalling And Processing Systems - Safety Related Electronic Systems For Signalling)

[7] JOHN DAINTITH. "safety-critical system." A Dictionary of Computing. 2004. *Encyclopedia.com.* 28 Mar. 2013 <http://www.encyclopedia.com>.

[8] Wikipedia, “Wenzhou train collision” http://en.wikipedia.org/wiki/Wenzhou_train_collision, visited 22 April 2013.