A Platform Approach for Fusing Safety and Security on a Solid Foundation

Reinhard Hametner
Thales Austria GmbH
Handelskai 92
1200 Vienna, Austria
reinhard.hametner@thalesgroup.com

Stefan Resch
Thales Austria GmbH
Handelskai 92
1200 Vienna, Austria
stefan.resch@thalesgroup.com

ABSTRACT
This paper presents the concept example of how to integrate safety and security using a platform approach. The TAS Control Platform is a SIL4 vital computing platform for railway applications developed within Thales to support many different safety-critical applications. Using common standards, MILS concepts and building up on a generic safety concept, enables the integration of safety and security with TAS Control Platform, while still providing support for legacy applications. With this platform approach many applications can benefit from the consistent safe and secure basis.

Keywords
Multiple Independent Levels of Security, Dependable Systems, Safety, Security, Embedded Systems, Safety-critical Systems

1. INTRODUCTION
Integrating safety and security is a key challenge for vital distributed systems.

With respect to safety Thales started development of the TAS Control Platform [1] more than 20 years ago. It is a generic fault-tolerant computing platform developed for railway applications with a safety integrity level of up to SIL4 according to the applicable CENELEC standards for the railway domain [2-5].

The TAS Control Platform consists of components off-the-shelf hardware and operating systems, as well as a safety-critical middleware that is a software layer which provides fault-tolerance and communication services to the applications. Providing such services for safety and availability as a platform enables the reuse of these by many different railway applications within Thales. The layered approach with the safety-critical middleware allows adapting to changing hardware and software environments without changing the business logic of the safety-critical applications, which typically have a very long life time in the order of 20 to 30 years.

As we see more and more requests for the support of "category 3" networks according to CENELEC EN 50159 [5], the integration of a common security approach in the TAS Control Platform, that also enables the support of secure railway applications, is the next logical step. With the above presented mechanisms, TAS Control Platform is a good foundation for the implementation of a cyber-secure ecosystem to run vital applications, since it already provides the abstraction of hardware, operating system and the separation of business logic and redundancy. In its current version TAS Control Platform is based on the Linux kernel and open standards, which allows integration of state-of-the-art security measures from an already well established community in the security domain.

In the next section we first present the foundation of our security approach. Section 3 shows our concept to separate the safety and security life cycles, followed by the summary in Section 4.

2. A SOLID APROACH TO SECURITY
The standard series ISA 62443 provides a systematic approach to security for industrial automation and control systems and is used in the CENELEC security standardization community as one of the potential security standards for the railway domain. The chosen approach for security in TAS Control Platform follows the corresponding industrial standards of ISA 62443 part 4-1 [6] and part 4-2 [7] for components. We are currently in the process of finalizing and improving the combination of our security and safety processes such as threats-, risk- and hazard-analysis with guidance from [8], [9], and [10].

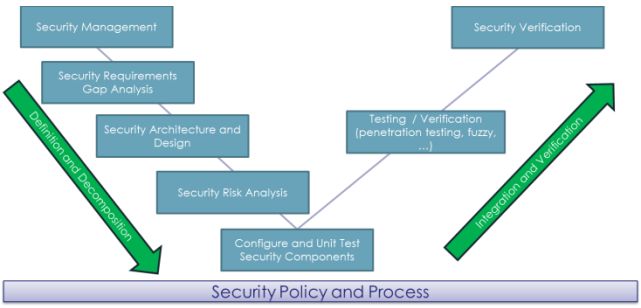

Figure 1 Security development process for TAS Control Platform.

Figure 1 illustrates the approach and activities that comprise the security management for the TAS Control Platform project. With this lifecycle all security activities and aspects are tracked in order to support a security assessment of each TAS Control Platform version. Additionally a periodically analysis of the Common Vulnerability [11] is performed in order to detect and react on potential security issues in the TAS Control Platform. The next section presents the security architecture and design that enables a light weight integration of security patches.

3. SEPARATING LIFE CYCLES
The ISA 62443 standards, like all other reasonable security standards, require patch management to react on detected vulnerabilities of the products in the field. Development, certification, and deployment of safety-critical products usually are performed in the order of several months, while fixes for security vulnerabilities should be provided and deployed within at most days. This illustrates the essential difference concerning safety and security life cycles.

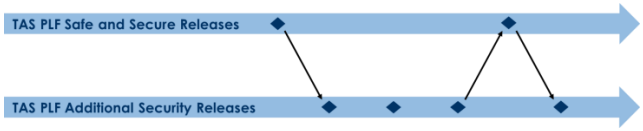

Figure 2 Separating safe and secure and secure releases for TAS Control Platform.

Figure 2 illustrates our approach to separate the safety and security life cycles by having different safety and security releases of TAS Control Platform. Safe and secure releases are verified and assessed according to safety and security standards, while security releases are only verified according to the security process. This enables us to provide up-to-date secure versions with a justifiable effort.

Concerning the integration of these versions in the field on a single computing board is then achieved by building up on the MILS approach. Key requirements we have concerning this approach are:

- Separation of secure software components from safe software components must be provided,
- The performance and resource usage by the secure software components must be restricted and predictable,
- Availability must be achievable through redundancy (independent boards, communication links, etc.), and
- The safety-critical functionality must always be provided with redundancy.

Especially the performance restrictions are necessary for supporting the real-time requirements of the safety-critical applications.

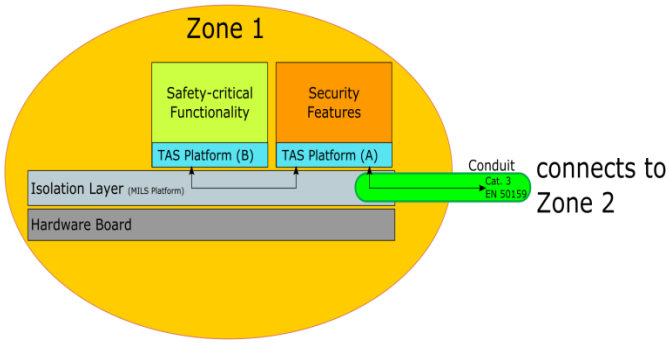

Figure 3 Integrated safety and security architecture example by using a MILS platform.

Figure 3 shows the concept of how the safety-critical and secure versions of TAS Control Platform can be integrated by using a MILS platform for separating the software components. This approach decouples the different life cycles of safety and security. Subsequently security patches can be included without complete retesting of the safety-critical application and platform. A major part of known vulnerabilities can be addressed with such a security partition especially if one includes secure-gateway functions in the security component, see Figure 3 TAS Platform (A). When combined with an automatic vulnerability management system that is linked to the CVE database [11], the platform approach enables regular and efficient patching with low additional efforts. This way zero-day vulnerabilities can be patched quickly once known and thus, minimizing the time of potential open critical security vulnerabilities significantly.

4. Summary

The platform approach shows how we combine safety and security for TAS Control Platform based on industrial standards for safety and security. A generic safety case approach is the basis for enabling the use of a MILS platform which supports the separation of the safety and security life cycles. The exchangeable security partition enables a fast security update without re-certification of the safety part of the system.

5. ACKNOWLEDGMENTS

CERTMILS Contract No: 731456: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731456.

6. REFERENCES

[1] Gerstinger, Andreas, Heinz Kantz, and Christoph Scherrer. "TAS Control Platform: A Platform for Safety-Critical Railway Applications." ECRIM NEWS, no. 75 (2008), pp. 49-50.

[2] CENELEC, "EN 50126-Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," European Committee for Electrotechnical Standardization, 1999.

[3] CENELEC, "EN 50128-Railway Applications: Software for Railway Control and Protection Systems," European Committee for Electrotechnical Standardization, 2011.

[4] CENELEC, "EN 50129-Railway Applications: Communication, signalling and processing systems - Safety related electronic systems for signalling," European Committee for Electrotechnical Standardization, 2003.

[5] CENELEC, "EN 50159- Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems", European Committee for Electrotechnical Standardization, September 2010.

[6] ISA99 Committee, "ISA 62443-4-1: Security for industrial automation and control systems - Product Development Requirements," Edition D3E11, 2017.

[7] ISA99 Committee, "ISA 62443-4-2: Security for industrial automation and control systems - Technical security requirements for IACS components," Edition D4E1, 2017.

[8] Department of Transport, Rail Executive, "Cyber Security Informed Safety Cases for Rail Industry: Code of Practice," Frazer-Nash Consultancy Limited, Bristol, UK, March, 2016.

[9] International Electrotechnical Commission, "Draft Guide 120: Security aspects – Guidelines for their inclusion in standards," Edition 1, 2017-06-02.

[10] International Electrotechnical Commission, IEC TC 65, "Industrial-process measurement, control and automation-Framework for functional safety and security," IEC TR 63069, Edition 1, August 2016.

[11] Common Vulnerability Enumeration (CVE) management of NIST; https://nvd.nist.gov, visited on 11.04.2018