certMILS eases security certification of railway systems

The certMILS project aims to protect critical infrastructure against cyber-attacks by compositional security certification to deliver a certified Multiple Independent Levels of Security (MILS) platform. But how can this be applied to railway systems? The project's Technical Leader, *Sergey Tverdyshev*, explains more.

THE RAILWAY safety standards (CENELEC – EN 50128, EN 50129, EN 50126) have introduced uniform requirements for the development of safety-related electronic systems consisting of software and hardware. EN 50128 and EN 50129 define generic (software) applications and generic (hardware) products that can obtain independent certification for railway applications. When building a complex safety system, such commercial off-the-shelf (COTS) products can be reused, including their existing certification artefacts. With this approach, safety-relevant electronics can be assembled from pre-certified software and hardware modules. However, while the EN standards ease safety certification of COTS-based systems in the railway industry, they do only in part deal with security which is becoming more and more important, as closed systems are giving way to networked environments with wired and wireless connectivity. Safety-related systems in trains and signalling need to be protected from cyber-threats in order to guarantee both integrity and availability. Security certification of critical railway systems therefore moves into the focus of developers and operators alike.

In contrast to safety, security certification of complex systems to medium-high assurance levels is not solved today. The existing monolithic approaches cannot cope with the complexity of modern cyber-physical systems (CPS). Such systems are characterised by safety-critical nature, complexity, connectivity and open technology. A common downside to CPS complexity and openness is a large attack surface and a high degree of dynamism that may lead to complex failures and irreparable physical damage. The legitimate fear of security or functional safety vulnerabilities in CPS results in arduous testing and certification processes. Once fielded, many CPS suffer from the motto: Never change a running system.

In order to ease CPS security certification in the railway and other industries, the EU-funded certMILS[1] project is currently developing a compositional security certification methodology to complex composable safety-critical systems operating in constantly evolving hostile environments (see ***Figure 1***). As part of this initiative, certMILS develops composable industrial CPS pilots for both railway and subway systems, certifies security of critical re-useable components, and ensures security certification for the pilots by certification labs in three EU countries with involvement of the authorities. While developing and applying the security certification methodology, certMILS will respect and complement the existing safety certification processes.

certMILS objectives

The certMILS project's main objectives are to transfer know-how in compositional safety certification to security certification and to make certification of composed systems affordable. It is also specifically designed as a European project in order to reduce dependence on U.S. technologies. The aim is to increase the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety and security certification of composable systems.

The project employs a security-by-design concept originating from the avionics industry: Multiple Independent Levels of Security (MILS), which targets controlled information flow and resource usage amongst software applications. certMILS reduces certification complexity, promotes re-use, and enables secure updates to CPS throughout its lifecycle by providing certified separation of applications, i.e. if an application within a complex CPS fails or starts acting maliciously, other applications are unaffected.

The MILS architecture

According to MILS, systems are separated into three horizontal levels with different rights and levels of trustworthiness (see ***Figure 2***). The lowest level is the hardware with further platform and security modules. Level 2 contains the separation kernel, which controls all communication in the system and allocates computing time and memory access to the individual applications. Only it is privileged for hardware management access and is considered trustworthy with regard to security. All other modules of the second level system software are also trustworthy, but not privileged for direct hardware management access. They are used to configure and organise the overall system and monitor its functionality. All applications running in user mode are considered untrustworthy and are assigned to the third level.

The MILS concept formulates the consistent and uniform implementation of several security policies for the separation kernel in order to secure and maintain the trustworthiness of the system. The separation kernel is the element which enables compositional security certification. The separation kernel itself shall be certified to be able to enforce these security policies with the required assurance (e.g. Evaluation Assurance Levels of ISO/IEC 15408). These security policies of the separation kernel are enforced by security functions whose implementation is reduced to an absolute minimum so that their evaluation and certification remains possible. They include, but are not limited to:

- Information flow: The separation kernel must enable and control the information flow between hardware, system software and applications
- Data isolation: The separation kernel isolates the memory areas and resources allocated to each application
- Clean CPU registers: The separation kernel deletes all entries in the CPU registers before another application can use the CPU
- Limitation of damage: The separation kernel limits malfunctions of an application to its partition. All other applications, the system software and the separation kernel itself are not affected.

A MILS platform must be non-bypassable, evaluable, always invoked and tamperproof (NEAT) in order to provide the required high level of security.

MILS in railway applications

In railway applications, communication systems usually follow the CENELEC EN 50159 standard which defines safety-related communication in transmission systems. It also contains some security elements by defining cryptographic techniques as well as cryptographic architectures required for open network communication. Currently, the CENELEC EN 50129 standard, defining mostly safety-related electronic systems for signalling, does not explicitly contain security elements or quality metrics but still, the integrity of system is paramount due to safety requirements. In this sense, security can be interpreted equivalently through ensuring the integrity of the system.

However, there exists relevant emerging standards on security in railway, such as VDE 0831-102 and VDE 0831-104 – both being still in pre-phase, as well as the emerging IEC 62443. Still, up to now customers must provide their own security requirements which are usually formulated at a high level. This effect generates very diverse security requirements throughout the railway

After joining SYSGO AG, **SERGEY TVERDYSHEV** has focused on real-time operating systems for high-critical applications. In this context he has worked in safety certification for avionics and later moved to security certification of RTOS PikeOS. Sergey has German accreditation for evaluation for Common Criteria standard. At SYSGO Sergey has initiated product security, product security certification and PikeOS security portfolio and he is the Director of their Research and Technology (R&T) Department. In this role he defines, maintains and manages the company portfolio of R&T projects. He regularly initiates European level research projects on high-assurance architectures for cyber-physical systems. Sergey regularly authors scientific papers on virtualisation platforms, security, safety, certification, energy consumption and formal verification. He is also actively contributing to standardisation of the MILS technologies: he has initiated an annual workshop on MILS and launched the 'MILS Community'.

FIGURE 1

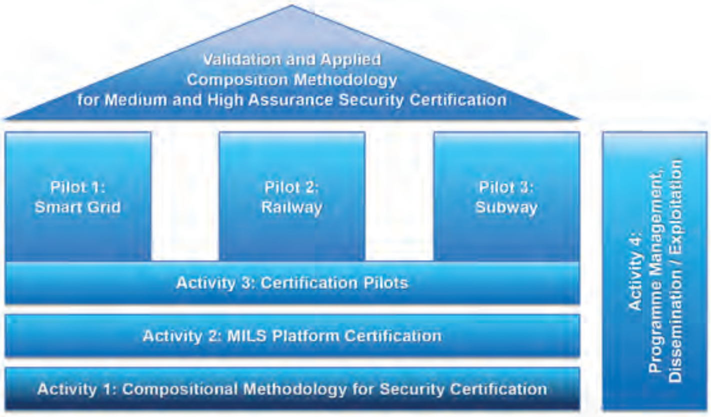
Validation and Applied
Composition Methodology
for Medium and High Assurance Security Certification
Pilot 1:
Smart Grid
Pilot 2:
Railway
Pilot 3:
Subway
Activity 3: Certification Pilots
Activity 2: MILS Platform Certification
Activity 1: Compositional Methodology for Security Certification
Activity 4:
Programme Management,
Dissemination / Exploitation

FIGURE 1: The certMILS methodology

FIGURE 2

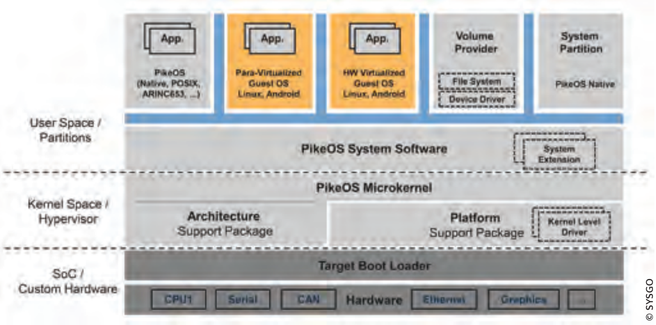

FIGURE 3

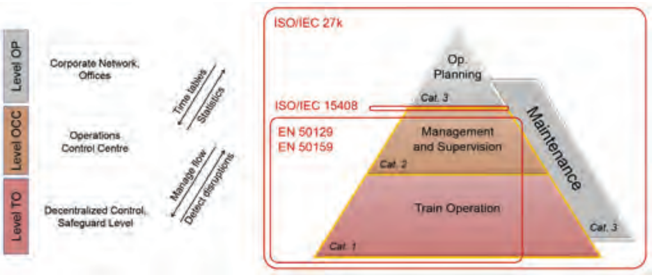

FIGURE 2: The MILS architecture distinguishes three security zones

FIGURE 3: Model of subway cyber-security

market, which can be problematic for suppliers as well as certification authorities.

While originally developed and applied in military and avionic applications, the MILS concept is also entirely suitable to ease that pain in the railway industry. One of the main targets of certMILS is to apply relevant security standards in the railway domain to foster conformity of security requirements and help customers provide a similar level of security in their products. Just like in the safety domain, the goal is to provide guidance for security building blocks, which can be integrated into complex systems using secure gateways for communication. In this way, the integrity of the system can be ensured from a security point of view. Furthermore, security gateways based on certified MILS Platforms will demonstrate modular security and reach high security levels.

> *One of the main targets of certMILS is to apply relevant security standards in the railway domain to foster conformity of security requirements and help customers provide a similar level of security in their products*

certMILS and subways

Subway management today is based on a three-level model per the EN 62290 standard (see ***Figure 3***). These levels are Operation Planning (OP), Operation Management and Supervision (OCC) and Train Operation (TO). An operator is responsible for the system operation and security of the critical infrastructure. The security requirements, at this global level, are satisfied by applying ISO/IEC 27k. The supplier is responsible for the system security at the OCC and TO levels. The safety requirement mandates application of EN 50159 and EN 50129. Commissioning of the metro line depends on acceptance of the 'Evidence of Safety' (EN 50129, Chapter 5) that shall also include cyber-security evidence. The interface between the corporate network (OP level) and OCC level shall be designed to meet both safety and security requirements (ISO/IEC 15408). The interface must be approved and included in the 'Evidence of Safety'. In case of change of the security relevant part, the approval process must be repeated.

In case of construction and inclusion of a new track section, it is necessary to prepare a security analysis of the complete system that will include the old and new parts of the line. If the newly constructed section of the track contains other than the original supplier's equipment, fundamental problems may arise in providing information relating to the system security, since the required detailed information is part of the supplier's know-how and typically kept secret. Thus, there are fundamental problems for cyber-security: How to integrate the new track-side equipment into the original system while preserving its security. There are no standards for integration of approved interfaces that comply with the relevant requirements without revealing/sharing the know-how of involved suppliers.

The certMILS approach to modular design, assurance and certification will foster heterogeneous systems without revealing commercial secrets while increasing security assurance and decreasing costs for IEC 62290 compliance for system interoperability and expandability. certMILS will create a Target of Evaluation (ToE) for certification in the subway domain, using ISO/IEC 15408 and the current interpretations of IEC 62443 within the context of security functionalities certified to EN 50129, EN 50126, EN 50159, IEC 61375. certMILS will demonstrate how a system based on MILS platform decreases both maintenance and incremental certification costs to future modules, while improving reaction on emerging security threats. certMILS will improve standardisation by contributing pilot results into security working groups of IEC and CENELEC.

Conclusion

certMILS will dramatically reduce the complexity of the certification of cyber-physical systems by use of a trustworthy MILS platform within the cyber-physical system, which is simple, small and certified for the highest level. Such a platform enables compositional security certification, which is applied in different pilots, including railways. To be marketable as a product for a large scope of ICT/cyber-physical systems, the platform has a powerful API configuration, supports open common and domain specific APIs (e.g. POSIX, ARINC) as well as consistently addresses existing domain safety standards/regulations.

REFERENCE

1. www.certmils.eu