Security Certification of Cyber Physical Systems for Critical Infrastructure based on the Compositional MILS Architecture

Andreas Hohenegger,[1] Gerald Krummeck,[1] Janie Baños,[2] Alvaro Ortega,[2] Michal Hager,[3] Jiri Sterba,[3] Tomas Kertis,[4] Petr Novobilsky,[4] Jan Prochazka,[4] Benito Caracuel,[5] Ana Lourdes Sanz,[5] Francisco Ramos,[5] Holger Blasum,[6] Mario Brotz,[6] Rudolf Fuchsen,[6] Guillaume Fumaroli,[7] Jan Neškudla,[8] Jan Rollo,[8] Lisa Burgstaller,[9] Martina Truskaller,[9] Klaus-Michael Koch,[9] Reinhard Hametner,[10] Sandro Rauscher,[10] Peter Tummeltshammer,[10] Frank Golatowski,[11] Thorsten Schulz[11]

(1) atsec information security GmbH, (2) DEKRA, (3) Elektrotechnický zkušební ústav s.p. (EZU), (4) Q-Media s.r.o., (5) Schneider Electric, (6) SYSGO GmbH, (7) SYSGO SAS, (8) SYSGO s.r.o., (9) Technikon, (10) Thales Austria, (11) Universität Rostock

Abstract— **We describe compositional architectures and certifications in the research project certMILS. Compositional architectures enable re-use of certified COTS (commercial off-the-shelf) components with a well-defined delegation of responsibilities between component developers and system integrators during cyber physical system design and certification. We show how we used a Common Criteria certified MILS (Multiple Independent Levels of Safety / Security) platform for compositional designs and IEC 62443-4-1/62443-4-2 security evaluations and certifications for composed systems from the domains of smart grid, railway, and subway, that are safety- and security-critical.**

I. Introduction

Previously isolated physical systems have become connected to the Internet. For instance, in transportation, for passenger comfort as well as operational efficiency, almost all means of transportation (airplanes, trains, cars, ships) are networked.

In the domain of such real-time and networked embedded computing, the certMILS project ("Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats") has developed compositional designs based on MILS ("multiple independent levels of safety / security" [1]), using compositional security certification to re-use a certified COTS product. For evaluation of the approach, project partners Q-Media, Schneider Electric and Thales Austria implemented demonstrations (pilots) for each of their domains in subway, smart grid and railway, acting as system integrators. Research questions comprise: (1) understand via learning-by-doing re-use of existing safety experience / artifacts for security and the effort still needed; (2) understand how a separation kernel and its Common Criteria certification can ease IEC 62443 certification. Here we address question (2); question (1) had been focus of a previous publication [2].

Section III describes the setting: how we built the architecture of the pilots for mixed-critical systems, their commonalities and the underlying MILS design. Section IV reports on how certifications for the pilots and a MILS separation kernel have been achieved, utilizing the MILS separation kernel's resource management and information flow control. We conclude with related work, summary of results, and lessons learnt.

II. Systems and their (Mixed-Critical) Compositions

All three use cases embody a safety-critical system as an asset: (1) in the smart grid use case this was a remote terminal unit (RTU) regulating electrical grid voltages and current flow, (2) in the railway use case a railway platform for on-board and off-board (e.g. signalling) systems, (3) in the subway use case a restricted network. We provided (further) networking of these systems, consisting of (1) an isolated monitoring access in the smart grid RTU, (2) a security firewall for the railway platform, and (3) a security gateway securely connecting an open network to a restricted network. We needed to show is that each networked safety-critical system preserved its existing safety properties under security threats arising from the network access, that is that the safety-critical properties were preserved. This is a mixed-critical architecture, where the safety system is of a high criticality and the additional networking is of a lower criticality: network functions shall not impact safety functions. The MILS architecture is a software/hardware architecture for designing, implementing and certifying these mixed-critical systems. A MILS platform is a hardware platform exclusively controlled by system software (separation kernel) providing secure execution environments called partitions [1].

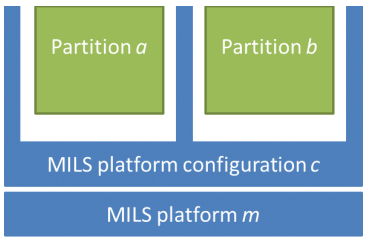

Figure 1: MILS platform

Naming components, behaviours and safety properties explicitly (Figure 1), computational systems have often been described as state machines, a transition function and invariants. For instance, take a critical system a with transition function q_a, and a less critical system b with transition function q_b. Then the combined system ab has transition function q_{ab}. If we add a MILS platform m, and its configuration c then the combined system $mcab$ using that MILS platform has transition function q_{mcab}. What we typically want to ensure in safety-critical systems is that safety property i_a, always holds on sys-

tem a, meaning that it is preserved by the initial condition of a and under the transition function q_a. A safety or security property that always holds is also called an invariant. For the compositional system *mcab*, this means that an invariant i_{mcab} is always preserved by the initial condition of system *mcab* and transition function q_{mcab}. In a mixed-critical case, the invariant i_{mcab} consists of the safety properties i_a for its component a plus safety and security properties for the MILS platform itself i_m, and its appropriate configuration i_c that determine its transition function and initial condition, but do not depend on i_b. In a compositional certification context, i_m is shown by the base separation kernel certification, and i_c is shown by the certification of the composed system. Moreover, for security properties not originating from the separation kernel, these need to be shown from invariants of system a (i_a) or (if non-critical) system b (i_b) in the compositional certification.

III. Compositional Architecture

A. MILS architecture and separation kernel

The Multiple Independent Levels of Security (MILS [1]) architecture is based on using a separation kernel. The separation kernel is a special kind of operating system, that is optimized for providing strong separation between the execution environments ("partitions" see Figure 1). The separation kernel has a small code base, so that it can be inspected for safety and/or security certification, to establish the invariant that it does not bypass its configuration (i_m). As safety- and security-critical embedded systems do not change during run-time, a separation kernel allows to configure the system's definition of partitions and allocation of resources during integration time when the system binary is assembled. It provides separation by default and allowing controlled information flow only by configuration (i_c). The separation kernel thus greatly simplifies the system's transition function q_{mcab}, because interactions between partitions only happen when this is explicitly requested. Unlike a separation kernel with its static and always enforced configuration, in comparison, a desktop operating system such as Windows or Linux in addition would at run-time dynamically reallocate memory between processes, creating non-desired and non-controllable interference between processes. Of course, the transition function q_{mcab} does not have to be computed or written down explicitly as a whole, rather for certification we ensure that no transition of q_{mcab} violates i_{mcab} given by the separation kernel. For a separation kernel, with its design for "no communication or interference unless allowed", q_{mcab} is limited to explicitly allowed communication, thus i_{mcab} is stronger and easier to verify than a desktop operating's system i_{mcab}.

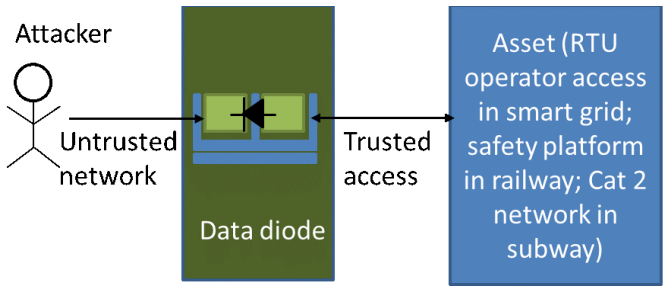

Figure 2: Use of MILS platform for controlled information flow (e.g. data diode functionality)

B. Description of security architectures in compositional pilots

The three project pilots in the smart grid, railway and subway domain have in common that they are safety- and security-critical embedded systems. From a threat analysis point of view, they operate in a mixed-criticality operational environment interacting with less trusted domains, protecting assets from attackers [3]. In all three pilots, the separation kernel is used either for a data diode [4] or at least control of network functionality in the pilots as shown in Figure 2. As the separation kernel's behaviour is determined by its configuration (i_c), we used security architecture templates [5] to allow to describe the chosen configuration in text form. Structuring the architecture description around the separation kernel's configuration also gave better comparability of the architecture descriptions produced for each pilot in an early stage of the project.

This approach of using a separation kernel that allows to establish safety and security invariants by its configuration (i_c) means that we have a clearer interface for breaking down the composition task. I.e., the security guarantees that are provided by the technical component separation kernel are quite well understood. In certMILS, we gained strong support from a public survey among stakeholders [6]. From a logical perspective this means, that for finding a good compositional architecture, our approach is not just a purely top-down search for the optimal fulfilment of external requirements. Instead, it also has a strong bottom-up part by using a well-understood component, the MILS separation kernel. Thereby, the multiple use of the well-understood MILS architecture is our approach for reducing the search space [7]. While our discussion here focuses on the pilots' common basis, they still differ for example on how they address each specific operational environment.

IV. Compositional Certifications

A. Choice of standards

We selected IEC 62443-4-1 [8] and IEC 62443-4-2 [9] to certify the pilots and Common Criteria (CC) [10] to certify the separation kernel: The security certification landscape is characterized by the generic CC on the one hard and application-domain specific standards on the other hand. Because the CC is quite generic, rigorous, and also involves a governmental authority, it has been considered more suitable for a small, stable and well re-usable systems/products [11], in our context the MILS separation kernel.

For industrial automation and control systems (IACS), the standard IEC 62443 has been created to improve the security of entire production facilities, whose life-cycle includes frequent changes that need to be made to a plant, which is reflected by life cycle processes: For example, risk assessment is continuously repeated to cover IACS evolution. Two of three demonstrators in certMILS are about rail systems (railway and subway), including their track-side networks (e.g. for control command and signalling). Because in effect, these distributed systems are similarly complex as IACS, CENELEC's prTS 50701 [12] is largely based on the IEC 62443 standard in the field of cyber-security. The next choice was about the certification schemes where IEC 62443 has different options such as (1) IECEE certification body (CB) Industrial Cyber Security

Table 1: Example of CC requirement provided by separation kernel: access control to memory FDP_ACF1.2/MA

Requirement in security target [40], FDP_ACF.1.2/MA (excerpt)	Access to physical memory M of type <VM_MEM_TYPE_ROM>, <VM_MEM_TYPE_RAM>, <VM_MEM_TYPE_IO_MEM>, or <VM_MEM_TYPE_IO_PORT> is allowed to a subject in partition PA if: • M is specified in a <MemoryRequirement> MR in the <MemoryRequirementTable> contained within the <Partition> P and the attribute <IsPool> is set to <false> AND • the access operation is read or write or execute and the access mode <AccessMode> of MR matches <VM_MEM_ACCESS_RD> for read, <VM_MEM_ACCESS_WR> for write, and <VM_MEM_ACCESS_EXEC> for execute correspondingly […] OR • M is specified in a property file system <prop_memmap> node PN AND • the <FileAccessTable> element of PA has an element of type <FileAccess> where the <AccessMode> attribute is AM and attribute <FileName> matches the PN AND • a subject in partition PA has successfully performed open operation (vm_open) on the property node name PN with access flags AF including <VM_O_MAP> and AF being subset of AM, resulting in a file descriptor FD AND • a subject in partition PA has successfully performed a property memory mapping (vm_prop_mem_map) operation with the file descriptor FD AND • the access operation is read or write or execute and compatible with AF
Functional specification	The functionality is documented in the design artefacts and user guidance, e.g., all parameters at the separation kernel configuration interface (example above: <VM_MEM_TYPE_ROM>) as well as to run-time system calls (in the example above: vm_open at runtime for files) must be explained. For this, we used available requirements specification from safety.
System design	System design describes in which subsystems (kernel subsystem and CPU architecture-dependent subsystems) and which modules the memory management functionality resides. At the module level, system calls, e.g., for memory mapping tend to stay within the memory-mapping module, where the security functional requirement (SFR)-enforcing functionality is. In addition, memory mapping calls involving access control have some SFR-supporting functionality with finding out which subject the current invoker of the system call is, which is needed to decide for the source of the invocation. The evaluator ensured that all functionality (SFRs) can be traced to the design.
Security architecture	The security architecture explains how memory separation contributes to maintaining different security domains; how memory management unit (MMU) initialization happens (e.g., different stages of memory setup at initialization steps of kernels and system services); how the intended memory setup cannot be bypassed at run-time (e.g., explaining how exceptions, such as page faults, are triggered on behalf of the MMU) and how calls to vm_open obey the configuration.
Testing	Functional testing of positive and negative tests that memory access is allowed / denied when it is configured by the system integrator. The evaluator checks that SFRs have tests in the CC test coverage work unit ATE_COV, which also lists the test cases that cover that the configuration is enforced at run-time. Fuzz testing of memory-related system calls.

Program [13], (2) ISASecure IEC 62443 Certifications [14], (3) exida IEC 62443 Cyber Security Certification Programs [15].

One of our consortium members (EZU) plays a major role in IECEE CB development, and the ensured good understanding of the development of the emerging scheme was one motivation to go for this scheme. IECEE CB also has the advantage that the applicant can choose quite freely the requirements she claims to fulfil (the exact scope of the requirements selected is noted on the certificate).

B. *Separation kernel: Assurance provided by the separation*

The separation kernel was used to gain separation assurance. To give an example for a separation kernel property (i_m), the pilots rely on the fact that the separation kernel properly manages memory. For the separation kernel's CC certification documentation this means that the developer properly explains how the separation kernel sets up the memory for different partitions into different address spaces at initialization time using the MMU and how certain reusable objects (e.g., for thread data, task data) are managed during run-time, so that memory between partitions is kept separate. See Table 1 for an example that shows how the configuration and run-time use of separation kernel memory is described and evaluated for CC.

C. *Use of separation kernel CC assurance for IEC 62443 by pilots*

In a world with unlimited resources the separation kernel would also have undergone a broader IEC 62443 certification. But as separation kernels are general-purpose products, and not limited to industrial control systems from a market perspective, for a separation kernel vendor it is more meaningful to certify against CC. Hence, we argue that the CC process requirements are sufficient for a separation kernel to be used as a component.

A technical argument why a CC certification is sufficient for a MILS separation kernel to be used in an IEC 62443 context is that both frameworks share many common properties: For example, both do a threat analysis, based on the identification of assets, threats, adverse agents, security objectives and functional measures to achieve them. IEC 62443-1-1 explicitly adopted a threat model based on the CC model [IEC-62443-1-1, Section 5, Figures 2 and 3]. Formally, the separation kernel is a COTS component and according to IEC 62443-4-1 SM-9 "Security requirements for externally provided components", it is possible to evaluate according to similar software development lifecycle standards. Therefore, we conclude that a CC certification of a separation kernel suffices for use as subcomponent of a product under 62443-4-1/62443-4-2 certification.

For the certification, the separation kernel helps to fulfil certain IEC 62443-4-2 functional requirements, reusing assurance provided by the separation kernel, mainly in the IEC 62443 functional groups CR5 restricted data flow and CR7 resource availability, as well as CR3 system integrity [16]. In Table 2, evaluation arguments for some CR5/CR7 group functional requirements are shown across the pilots: The MILS platform's separation kernel is referred to as "MILS separation kernel" or "separation layer". We can see that for restricted data flow (CR5.1 shown for smart grid and railway, CR5.2/NDR5.2 for subway), the MILS separation kernel's information flow control property is used, and the separation kernel's per-partition resource management is relied on for CR7.2 resource management.

Table 2: Example of evaluation evidence for requirements involving the separation kernel: IECEE-4-2 CR5.1 Network segmentation / CR5.2 Zone boundary protection / CR 7.2 Resource management

Smart grid (CR5.1)	The manufacturer sent the equipment to DEKRA lab for performing the testing/pentesting. User manuals are also provided for the evaluators to gain experience in the use of the unit. The prototype has two separate networks: • Partition 1: ETH1 – trusted network (protocol communications). • Partition 2: ETH2 – untrusted network (web access) If partition 2 gets attacked by malicious traffic exploiting a vulnerability of the webserver, this traffic would not reach partition 1 hosting the critical functionality, since the information flow policy between the partitions is strictly enforced by MILS. The manufacturer provides guidance (both documentation and online support) on how to configure for fulfilling the above-mentioned functionality. Once the configuration is applied, the evaluators conduct (pen)testing to confirm that the network segregation feature cannot be bypassed.
Railway (CR5.1)	The separation layer incorporates a technique called IOMMU (Input–Output Memory Management Unit) to hand-over the only used network interface (which connects to Zone 2) of the hardware board from the separation layer to TAS-Platform (A) and directly map it into TAS-Platform (A)'s memory. The interface is only accessible to this instance after a successful start-up and verification of the used exec-images. In case of an attack on the device itself, TAS-Platform (B), which runs all safety-related software is never affected due to only whitelisted packages being able to reach this instance. The separation layer is not able to be directly attacked via a network interface due to utilization of the previously mentioned IOMMU technology.
Subway (CR5.2/ NDR5.2)	The zone boundary protection requirements are network-component-specific. The assessment of this requirement has been carried out in the following steps: • verification of the client's indication of interest for assessment in "62443-4-2 Applicability QMA.xlsx", • verification of the information provided by the client in the columns "Conformity Statement" and "Conformity Evidence" in "Documentation iec62443_4_2.xlsx" • analysis of the CR 5.2 requirement in the IEC 62443-4-2 standard, • analysis of the NDR 5.2 requirement and its justification in the standard, • assessment of the column "Conformity Statement", in which the client briefly described how he meets CR 5.2 (NDR 5.2) requirements. It includes the use of a MILS separation kernel (PikeOS) for the implementation of independent and mutually isolated channels with the implementation of surveillance application monitoring, enabling / disabling network traffic on physical and virtual Eth communication interfaces based on an intervention from a diagnostic system, • verification of the information given in the "Conformity Evidence" column in PikeOS 4.2 documentation,
Smart grid (CR7.2)	Due to MILS separation kernel, every partition has assigned the resources (memory and CPU) needed.
Railway (CR7.2)	The separation layer incorporates various techniques to rate-limit the resources of the virtual instances TAS-Platform (A) and TAS-Platform (B) which are managed by the used virtualization technique to limit CPU and memory consumption according to the needed resources, and also applies CPU instruction limiting to both virtual instances to further minimize the attack surface.
Subway (CR7.2)	The assessment of this requirement has been carried out in the following steps: • verification of the client's indication of interest for assessment in document "62443-4-2 Applicability QMA.xlsx", • verification of the information provided by the client in the columns "Conformity Statement" and "Conformity Evidence" in the document "Documentation iec62443_4_2.xlsx", • analysis of the requirement CR 7.2 in IEC 62443-4-2 standard and its justification in this standard, • assessment of the content of the "Conformity Statement" column, in which the client briefly described how he meets the CR 7.2 requirement. It includes the use of the PikeOS operating system enabling the allocation of system resources depending on the virtual platform configuration, • verification of the information given in the "Conformity Evidence" column in the PikeOS documentation,

V. RELATED WORK

Compositional assurance can be expressed in models. For instance, it has been shown that, at the level of behaviour of event traces, security properties do not necessarily compose, if component interactions are not well controlled [17]. This can be mitigated by choosing appropriate architectures and similar building blocks that allow tight control over information flows. Rushby [18] and DeLong [19] have formalized this for separation kernels, inspiring our own notation in Section II. If we step back to take a very broad look, composition of systems of course not only has been studied in computer science, but also in system science as a whole, and also the insight that a transition function should be at a high level to be reasonably understandable has been expressed in that community too [20].

The CC allow compositional certification through "Composed Assurance Packages" [10], though this approach is so far rarely used [21] [22]. The smart card community has worked out detailed guidance for the compositional certification of smart cards and their operating [23] [24], including even estimations of cost savings [25]. We have seen that the input for evaluation is not only the separation kernel but also the guidance on how to use it securely and safely. This has been generally observed for many safety [26] [27] and security evaluations [23] [24]. If components from different vendors or across the hardware/software boundary are involved, appropriate information exchange between parties still can be difficult

when it is not specified what information is exchanged or only high-level information is exchanged [28] [29].

Compositional architectures and assurance arguments for MILS as studied here in certMILS as well as in other projects such as D-MILS [30] emulate the smart card approach by providing an environment for relatively robust building blocks via the separation kernel, also facilitating information exchange between different parties by setting relatively clear domain separation. For our own use, but also as a means to interact with the community at large, certMILS has published guidelines and templates for MILS certification for component developers, product integrators and evaluators, such as a CC protection profile (PP) draft [31], drafts for additional PP modules [32] and guidelines for using the PP [33]. We expect these to ease future certifications of MILS systems in particular, as well as compositional systems in general.

Sufficiency of CC certification for OS (Section IV.C) had previously been indicated also in IsaSecure's guideline for the application of IEC 62443-4-1, SDLA-312 version 3.0 [34], and more recent versions of SDLA 312 [35] go along with the guidance of IEC 62443-4-1 unit SM-9 for externally supplied components in general, which applies to our pilots as discussed in Section IV.C. Similarly, acceptance of other certifications is suggested in the railway sector's VDE 0831-104 [36].

VI. Results and lessons learned

A. Overall results

We developed and used a compositional architecture (Section III). We did compositional certifications using two different certification approaches, the CC and IEC 62443 (Section IV), based on a certified MILS platform, and the means of platform-to-system assurance propagation provided by the MILS architecture. What is new and the contribution of this work is the pervasive look at assurance covering both the MILS separation kernel and the composed systems. We have also for first time pin-pointed which IEC 62443 work units were suitable to make the connection. Working from a research project gave resources to contribute closely to the IECEE CB standardization process and to try it out (Section IV.C), resulting in the world's first IECEE CB IEC 62443-4-1 certification. IEC 62443-4-1 SUM-5 requires a faster security patching process than the longer-term CC evaluation process; the MILS architecture allows to patch partitions on top of the separation kernel safely and securely.

B. Use of generic certMILS research artefacts for certification

An assumption we wanted to assert with the pilots, is whether the MILS is useful for the security architecture used in compositional certification. In addition to the similarity of the pilots, concrete artefacts were reused as described by [2].

C. Limitations of the certMILS approach

In certMILS we assumed the underlying hardware to be correct. As Spectre/Meltdown have shown, this is an optimistic assumption. However, currently for COTS hardware, there is no hardware certification assurance easily available. Indeed, recent developments in open hardware such as the open RISC-V ISA could be promising for better information exchange across the hardware-software boundary. We also did not explicitly address the issue of recertification, for which several approaches exist, e.g. re-use of artefacts and maintenance certifications [37]. Some aspects – such as secure boot – could have technically been covered also by the separation kernel (at the expense of a larger code base to certify), whereas others such as identity management are usually on the application side.

D. Real-world certification and research project aspects: additions and short-cuts

Previous experience with research projects involving certification showed that aiming at a real certification within a project increases the motivation for both applicants and evaluators to spend more effort, but full certification is not always feasible (e.g. other constraints such as product line development). For each IEC 62443-4-1 and IEC 62443-4-2 we did a gap analysis (smart grid) and two certifications (railway and subway).

For the smart grid pilot, Schneider Electric split out a medium-assurance pilot for doing most of the IEC 62443 gap analysis and a high-assurance pilot for the use of a separation kernel and IEC 62443 work units related to use of a separation kernel. Project partner DEKRA gained a lot of expertise during the evaluation, as some internal training processes were needed for the evaluators and is now in a good position to perform IEC 62443 evaluations for other parties. In addition, Schneider Electric gained experience in this kind of processes by identifying gaps in respect to the standard and by learning about the evaluation process that is very useful for future evaluations.

For the subway pilot, project partner Q-Media had to balance between ideal business needs for going towards a more generic product and the need to freeze certification requirements. In the end, a specific setup was used for evaluation.

For the railway pilot, application of kernel driver robustness testing was trialled [38]. The technical approach was originally developed for the separation kernel, but also ported for use in the Linux-based separation technology in use by the platform pilot. The trial revealed the real-world complications of introducing code-injection-based testing technologies, such as adapting/rebuilding an existing toolchain to accommodate for plug-ins as well as substantial performance issues related to fuzz-testing hardware drivers compared to common software-only fuzz-testing.

For the separation kernel itself, there was delay caused by a previous certification that had to be finished before the higher-level certification activities of the certMILS project itself could start. But the assurance level (EAL3) of the previous certification [39] [40] was sufficient to supply the compositional arguments in certMILS for the pilots.

VII. Acknowledgment

This work is part of the certMILS project under grant agreement No. 731456, funded by the European Union's Horizon 2020 research and innovation programme. We gratefully acknowledge advice and help from our advisory board: Christian Schlehuber, DB Netz, Victor Bermúdez Llamusi, Red Eléctrica de España, Cristina Simache, Vitesco Technologies, Thomas Steffens, TÜV Rheinland, Jiří Čejka, Dopravní Podnik hl. m. Prahy (DPP) and Jaroslav Šmíd, NÚKIB.

VIII. REFERENCES

[1] S. Tverdyshev, H. Blasum, B. Langenstein, J. Maebe, B. De Sutter, B. Leconte, B. Triquet, K. Müller, M. Paulitsch, A. Söding-Freiherr von Blomberg and A. Tillequin, "MILS Architecture," 2013. [Online]. Available: https://doi.org/10.5281/zenodo.45164.

[2] A. Hohenegger, G. Krummeck, J. Baños and A. Ortega, "Security certification experience for industrial cyberphysical systems using Common Criteria and IEC 62443 certifications in certMILS," 4th ICPS 2021. https://ieeexplore.ieee.org/document/9468241/ .

[3] J. Prochazka, P. Novobilsky and D. Prochazkova, "Cyber Security of Urban Guided Transport Management according to MILS Principles," p. 7, 2019.

[4] H. Okhravi and F. T. Sheldon, "Data diodes in support of trustworthy cyber infrastructure," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10*, Oak Ridge, Tennessee, 2010.

[5] S. Tverdyshev, B. Caracuel, A. Álvarez, A. Ortega, J. E. Rico, R. Hametner, H. Blasum, T. Kertis and T. Schulz, "Security Architecture Template," May 2018. [Online]. https://zenodo.org/record/2586566

[6] T. Schulz, A. Hohenegger, A. Ortega and H. Blasum, "Community Feedback on the Separation Kernel Protection Profile Draft," January 2019. [Online]. Available: https://zenodo.org/record/2541464.

[7] H. A. Simon, The sciences of the artificial, 3rd ed., Cambridge, Mass.: MIT Press, 1996.

[8] International Electrotechnical Commission (IEC), "IEC 62443-4-1: Security for industrial automation and control systems - Part 4-1: Secure product development life-cycle requirements," 2018. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[9] International Electrotechnical Commission (IEC), "IEC 62443-4-2: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components," 2019. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[10] Common Criteria Sponsoring Organizations, "Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 5," April 2017. [Online]. Available: http://www.commoncriteriaportal.org/cc/.

[11] A. Hohenegger, "Die Common Criteria und IEC-62443," in *Deutscher IT-Sicherheitskongress*, SecuMedia Verlag, 2019, pp. 85-96.

[12] CENELEC, prTS 50701: Railway applications – Cybersecurity, CLC/FprTS 50701, 67491, vote for ts/tr, CLC/TC 9X, 2021-04-02, N, EN., 2021.

[13] IEC Systemof Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System), "Rules of Procedure –CB Scheme of the IECEE for Mutual Recognition of Test Certificates for Electrotechnical Equipment and Components (CB Scheme) and its related services:Statement of Test Results - Energy Efficiency Testing Service (E3)Global Motor Energy Efficiency (GMEE) Program Industrial Cyber Security Program," p. 21, 2019.

[14] ISA Security Compliance Institute (ISCI), "ISASecure - IEC 62443 Conformance Certification - Official Site," 2020. [Online]. Available: https://www.isasecure.org/en-US/.

[15] exida.com LLC, "exida - IEC 62443 Cybersecurity Certification," 2020. [Online]. Available: https://www.exida.com/Certification/IEC62443-Cyber-Cert.

[16] J. Prochazka, P. Novobilsky, D. Prochazkova and T. Kertis, "Certification Cycles of Train Cyber Gateway," in *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15). No. 3728. ISBN 978-981-14-8593-0.*, 2020.

[17] J. McLean, "A general theory of composition for trace sets closed under selective interleaving functions," in *IEEE symposium on research on security and privacy*, 1994.

[18] J. Rushby, "Compositional Certification," 2009. [Online]. Available: http://www.csl.sri.com/users/rushby/slides/dhs07.pdf.

[19] R. DeLong, "Compositional Certification Lecture Notes," 2009. [Online]. Available: http://rgdoi.net/10.13140/RG.2.1.2557.5922.

[20] L. J. Kohout and B. R. Gaines, "Protection as a general systems problem," *International Journal of General Systems,* vol. 3, no. 1, pp. 3-23, January 1976.

[21] A. Hohenegger, H. Blasum, S. Tverdyshev, L. Garcia, A. Álvarez de Sotomayor, B. Caracuel, T. Kertis, G. Krummeck, H. Kurth, S. Persson, R. Hametner, M. Paultisch, P. Tummeltshammer and M. Hager, "Regulative Baseline: Compositional Security Evaluation," July 2017.

[22] R. Schwarz, K. Müller, A. S.-F. Blomberg, B. Leconte, G. Gobbo, M. Paulitsch and A. Tillequin, Trustworthy MILS: CC composite evaluation approach, 2015.

[23] EUROSMART, "Security IC Platform Protection Profile with Augmentation Packages," 2014. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0084b_pdf.pdf;jsessionid=D3676C772782F69FB9C7CC22D420A029.internet472?__blob=publicationFile&v=1.

[24] SOGIS, "Composite product evaluation for Smart Cards and similar devices," 2018. [Online]. Available: https://web.archive.org/web/20201229164054/https://www.sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1.pdf.

[25] GlobalPlatform, "GPC_SPE_31: GlobalPlatform card composition model version 1.1," 2012.

[26] B. Jacobs, "Detailed requirements the OPENCOSS compositional certification approach D5.2," 2012. [Online]. Available: https://web.archive.org/web/20170830064656/http://www.opencoss-project.eu/sites/default/files/D5_2_Detailed_requirements_compositional_certification_OPENCOSS_platform_final.pdf.

[27] P. Gliwa, Embedded Software Timing: Methodology, Analysis and Practical Tips with a Focus on Automotive, Cham: Springer International Publishing, 2021.

[28] P. A. Karger and H. Kurth, "Increased Information Flow Needs for High-Assurance Composite Evaluations," in *Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04)*, Washington, DC, USA, 2004.

[29] H. Kurth, "Why Composite Evaluations Fail (A13a)," in *International Common Criteria Conference (ICCC) 2018*, 2018.

[30] A. Cimatti, V. Sommarive, W. Kampichler, J.-P. Katoen, W. Steiner, S. Strasse, T. Kelly, D. Lane, Y. Yo, H. Ruess, Y. Bakalov, S. Hansen, S. Bensalem, A. de Vignate and A. Legay, "D4.2 Compositional assurance cases and arguments for distributed MILS," p. 26, 2015.

[31] J. E. Rico, H. Kurth, A. Hohenegger, A. Ortega, H. Blasum, S. Tverdyshev and M. Hager, "Base MILS Platform Protection Profile," May 2018. [Online]. Available: https://zenodo.org/record/2586499.

[32] A. Ortega, H. Kurth, A. Hohenegger, B. Caracuel, J. E. Rico, L. Garcia, H. Blasum and S. Tverdyshev, "MILS Platform PP Modules," May 2018. [Online]. Available: https://zenodo.org/record/2586507.

[33] J. Rollo, H. Kurth, A. Hohenegger, A. Álvarez de Sotomayor, B. Caracuel, A. Ortega, S. Tverdyshev, H. Blasum and T. Kertis, "Guidelines to use and apply PP for all involved stakeholders," May 2018. [Online]. Available: https://zenodo.org/record/2586574.

[34] ISA Security Compliance Institute, "SDLA-312 Security Development Lifecycle Assessment Version 3.0," 2014. [Online]. Available: http://www.isasecure.org/en-US/Certification/IEC-62443-SDLA-Certification.

[35] Automation Standards Compliance Institute, "SDLA-312 Security Development Lifecycle Assessment Version 5.7," 2020. [Online]. Available: https://www.isasecure.org/en-US/Documents/Authentication-Required-Specifications/SDLA-3-0-0/SDLA-312-Sec-Dev-Lifecycle-Assess(v5_7).

[36] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, UK 351.3 Bahn-Signalanlagen, "Elektronische Bahn-Signalanlagen - Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443," 2015.

[37] A. D. Sinnhofer, W. Raschke, C. Steger and C. Kreiner, "Evaluation paradigm selection according to Common Criteria for an incremental product development," in *International workshop on MILS: architecture and assurance for secure systems, MILS@HiPEAC 2015, amsterdam, the netherlands, january 20, 2015*, 2015.

[38] T. Schulz, A. Hohenegger, A. Ortega, L. Müller, P. Gorski and H. Blasum, "Security testing framework (certMILS D4.4); post-acceptance archival planned at zenodo.org," 2020. [Online].

[39] BSI, "PikeOS Separation Kernal CC Certification Report," [Online]. Available: https://www.commoncriteriaportal.org/files/epfiles/1041a_pdf.pdf. [Accessed 28 June 2019].

[40] SYSGO AG, "Security Target PikeOS Separation Kernel v4.2.2," 2018. [Online]. Available: https://www.commoncriteriaportal.org/files/epfiles/1041b_pdf.pdf.