



D7.4

Report on validated security certification methodology with railway pilot

Project number:	731456
Project acronym:	certMILS
Project title:	Compositional security certification for medium to high-assurance COTS-based systems in environments with emerging threats
Start date of the project:	1 st January, 2017
Duration:	48 months
Programme:	H2020-DS-LEIT-2016

Deliverable type:	Report
Deliverable reference number:	DS-01-731456 / D7.4 / 1.1
Work package contributing to the deliverable:	WP 7
Due date:	M48 – December 2020
Actual submission date:	23 rd December, 2020

Responsible organisation:	EZU
Editor:	Michal Hager
Dissemination level:	PU
Revision:	1.1

Abstract:	The report summarises how the methodology was applied, essential improvement suggestions, suggestion for integration into existing and emerging certification schemes, illustrating by examples how railway existing safety and regulatory requirements are enhanced by the security certification with focus on identifying and solving obstacles/conflicts between those requirements and security certification.
Keywords:	Methodology, certification, certification schemes, railway, requirements



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

Editor

Michal Hager (EZU)

Contributors (ordered according to beneficiary numbers)

Sandro Rauscher (THA)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The report contains how the methodology was applied, includes improvement suggestions, suggestion for integration into existing and emerging certification schemes. It also illustrates how railway existing safety and regulatory requirements are enhanced by the security certification with focus on identifying and solving obstacles or conflicts between those requirements and security certification.

As certMILS approached its final months of implementation and certification according to IEC 62443, this document aims to be an overview of the outcomes of the applied security certification and evaluation methods as well as fulfilled requirements of the introduced Railway Pilot from Thales. It incorporates state-of-the-art contributions of the project partners EZU, DEKRA and UROS and the internal requirements mapping of the TAS-Platform development team to the chosen standards IEC 62443-4-1 and IEC 62443-4-2.

Contents

Chapter 1	Introduction	1
1.1	Connection to the methodology defined in D1.3.....	1
1.2	Suggestions for improvement of methodology defined in D1.3	2
Chapter 2	Integration into existing and emerging certification schemes	3
Chapter 3	Regulatory requirements aspects.....	5
Chapter 4	Summary of the outcomes from certification/evaluation process	6
4.1	IEC 62443-4-1	6
4.1.1	Examples for requirements	7
4.2	IEC 62443-4-2.....	8
4.2.1	Examples for requirements	9
Chapter 5	Scope and meaning of obtained certification	10
Chapter 6	Lessons learned	11
Chapter 7	Summary and Conclusion	13
Chapter 8	List of Abbreviations.....	14
Chapter 9	Bibliography	15
Annex.....		16

List of Figures

Figure 1: ENISA Certification Scheme	3
Figure 2: IEC 62443-4-1 certificate	16
Figure 3: IEC 62443-4-2 certificate	17

Chapter 1 Introduction

As per study provided by ENISA [1] railway sector representing 472 billion passenger-kilometres, 216,000 km of active railways and 430 billion tonne-kilometres for freight transport, plays an important and fast-growing role. Railway infrastructure and systems are key assets, crucial to developing and protecting the EU. The railway sector is undergoing a major transformation of its operations, systems and infrastructure due to the digitisation of systems and infrastructure, the automation of railway processes, the issues of mass transit and the increasing numbers of interconnections with external and multimodal systems. This sector is also evolving as it opens up to competition. This leads to the reallocation of responsibilities and the separation of railway systems and infrastructure. In this context, it is becoming even more crucial for the railway sector to tackle relevant and dangerous cyber threats.

Within this context the certMILS consortium was running the railway pilot. Understanding the importance and impact is crucial and having Thales as one of the major stakeholders in the European railway sector was very beneficial. With four tasks (Pilot specification, Pilot security design compliant to IEC 62443, Pilot implementation, Pilot security evaluation) and three deliverables (Compositional design of the railway pilot, Railway demonstrator implementation, Railway pilot security evaluation) already finished, we faced the final challenge – certification. And that is the theme of this deliverable – the aspects of the cyber security certification of the pilot and lessons learnt that should be carried over to the next assessments and communicated within the market and relevant stakeholders, including the standardization bodies.

1.1 Connection to the methodology defined in D1.3

Thales, as pilot owner, quickly realized that IEC 62443 standards provide a conscious way to certificate Industrial Systems integrated in railway sector. Reason behind that decision is that the requirements are focused on fulfilling the following aspects:

- Data integrity that flows to and from the evaluated devices. Many of Industrial Control Systems are integrated within critical systems that could lead to a disruption of services if the data is inconsistent.
- Well-defined actions that the system users can accomplish.
- Protection against common attacks that IACS systems are usually victims.
- All system and users actions must be reflected in the system logs. Then, such logs shall be protected against modifications.

The IEC 62443 standards also provide flexibility and complexity thanks to division of different aspects to different parts (standards). Further advantage identified in the chosen IECEE certification scheme built on these standards is that the certification scheme is less formal and no involvement of national certification (surveillance) body is required.

With that being said, the strongest connection between the pilot certification and the methodology defined in D1.3 is within the following chapters of D1.3 [2]:

- Chapter 4.2 IEC 62443 composition certification and
- Chapter 5.2 IEC 62443 Specifics

The compositional aspect is supported by using the separation layer, which is a realization of the MILS platform within the pilot architecture, and by the nature of the IECEE certification schemes themselves.

1.2 Suggestions for improvement of methodology defined in D1.3

We identified two major aspects that shall be integrated into the methodology. They are defined as follows:

- 1) Incorporate the lessons learnt from the evaluation and certification activities. Further work should be based on lessons learnt defined in the Chapter 5 below.
- 2) Take into account new national and European legislation on cyber security. Even during the course of the project new regulatory requirements emerged. There is no doubt that even more regulatory requirements will be defined in the upcoming months and years. Biggest impact might have the new Cyber Security Act [3] and certification schemes defined under its influence.

Chapter 2 Integration into existing and emerging certification schemes

We started a strong integration into the existing and emerging certification already during the course of the project. During the first discussions about evaluation and certification activities we identified that IECEE certification scheme built around IEC 62443 standards is perfect fit for our project's pilots and railway pilot especially.

Strong connection between those activities can be further enhanced by having a member in the IECEE CMC Work Group 31. WG 31 is the primary work group, which goal is to further develop certification schemes around IEC 62443 standards and also has a big influence and contact channel established with IEC TC 65. IEC TC 65 prepares international standards for systems and elements used for industrial process measurement, control and automation and coordinates standardization activities, which affect integration of components and functions into such systems including safety and security aspects.

Another important involvement is having a member in IECEE ETF 16, which is Expert Task Force created for supporting of IECEE CMC WG 31. The primary responsibility of the ETF is to ensure the consistent interpretation and application of IEC 62443 requirements by all NCBs and CBTs.

In future we expect emerging certification schemes under the new Cyber Security Act. Those schemes are to be developed by ENISA based on the initial requirement from European Commission. See Figure 1 below:

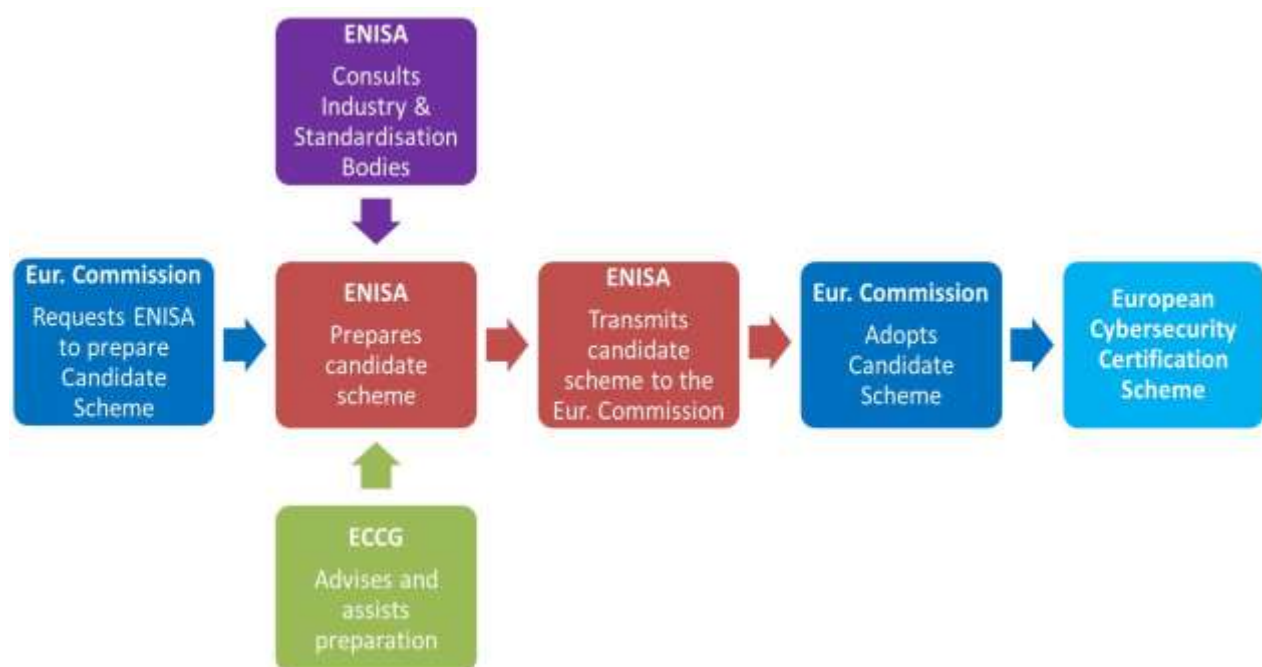


Figure 1: ENISA Certification Scheme

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2017:500:FIN>

certMILS consortium is already active in this new approach to European cyber security certification:

- ATSEC participation in ad-hoc Working Group 01 - Transposition of the SOGIS-MRA certification framework
- Active approach to public consultation of the first certification scheme developed:
 - Commenting on
 - High-assurance shall not necessarily be based on hardware
 - PP should not be prerequisite to high-assurance certifications

Chapter 3 Regulatory requirements aspects

Modern railway operation has become more interconnected through the introduction of operational control centers. Up until now, connections between railway systems have been deployed within closed networks according to the railway standard CENELEC EN 50159.

Certifications according to IEC 62443-4-1 and IEC 62443-4-2 in context of certMILS are one of the major steps to enable the integration of safety and security on TAS-Platform to be ready for future highly interconnected and geographically distributed railway systems.

Furthermore, IEC 62443 eases the process to comply with the NIS Directive used by THA, especially for THA acting as an operator and product/maintenance service supplier of critical infrastructure with special regards to confidentiality and privacy.

The NIS Directive in Austria describes measures and assertions for high standards of information security and issued the following requirements:

- Defining a strategy for cybersecurity
- Establishment of a single point of contact
- Establishment of a national competent authority
- Establishment of a computer security incident response team

Another part of the NIS Directive in Austria is that the operator of critical infrastructure has to prove the fulfilment of all requirements every two years, which is a very important aspect in the automation of industrial IT system security as these products have a lifecycle from 5-20 years and have to be available 24/7.

Chapter 4 Summary of the outcomes from certification/evaluation process

THA paid close attention to correctly reference all needed requirements from the internal THA document archive, as the Cybersecurity standards from the IEC62443 family were in focus of the evaluation. The meticulous steps required to fulfil the certifications and their processes allow THA to ease internal traceability of needed requirements and to not leave-out or wrongly/insufficiently implement any necessary requirements to fulfil requirements of possible future certifications.

The standardization and certification according to IEC 62443-4-1 and IEC 62443-4-2 was considered as very practicable and reasonable for THA and particularly for the TAS-Platform development cycle, as the first drafts of the standard covered nearly all use cases for the incorporated railway domain. The final versions of the standards did not negate what was in the drafts.

Further the IEC 62443 terminology, concepts and models embody up-to-date IT security and secure product development lifecycle requirements which conveniently comply with the state-of-the-art development of TAS-Platform. IEC 62443-4-2 offered new challenges in the form of Security for Industrial Automation and Control Systems for THA and have helped to address these innovations accordingly.

Examples of the assessed requirements can be found below. Some evaluated requirements have been very similar to other evaluated requirements and therefore they have been intentionally omitted in this document.

4.1 IEC 62443-4-1

The criteria used for the assessed requirements selection were chosen to be as close as possible to the used standard to assure that product lifetime security was fulfilled. All assessed requirements were declared maturity level 2 and possess according conformity evidence. The process of certification based upon IEC 62443-4-1 standard is the following:

(Note: Some of the text here has already been provided in section 2.2 of D7.3 deliverable [4], and has been intentionally repeated to make it available to readers of this public deliverable.)

(1) The first step for the applicant was to submit an application to be assessed for conformance. After contractual matters were solved, the applicant received the Test Report Form (TRF) and its annex, plus Questionnaire. The questionnaire provides the certification body with information necessary for the next step – scoping of submittal, which was deemed to be IEC 62443-4-1 ML 2.

As a first step, THA submitted an application in context of the certMILS project to EZU in April 2019, after some minor difficulties regarding deadlines of an internal security assessment report, which had to be finished beforehand. It especially provided the information of requirements (all except for two could be fulfilled) and maturity levels chosen (ML2), identification of certification scenarios and specifications of processes that are going to be assessed.

(2) In the next phase the applicant completed the applicable portions of a Test Report Form (TRF) and provided evidence in support of the capabilities that are intended to demonstrate compliance to the selected requirements. After that, each selected IEC 62443 security requirement was evaluated against the supporting evidence supplied by the applicant to determine compliance by the certification body.

THA submitted the needed conformity evidence in April 2019. Preparation for submitting this evidence had already started in April 2019 because of Reinhard Hametner from THA, who had also been closely working on IEC 62443 standardization at this point and therefore the needed work had already been optimized to the TAS Platform development team workflow, such as mapping of requirements needed for the certification, gap and vulnerability analyses and preliminary preparation for the penetration test.

(3) The results of the assessment were gathered in the TRF and its annex. In this form it was also presented to the applicant. The possible results for each requirement are the following¹:

- pass
- fail
- N/E (not evaluated)

For requirements that were met it also issued a certificate. Requirements for these certificates are again defined by IECEE – all certification bodies are obliged to follow these instructions. They are defined in IECEE OD-2037² (Edition 3.4, 2020-10-16) IECEE Test Certificates.

(4) The certificate was then issued to THA in June 2019 without any further complications.

(5) The certification process was then started again for upgrading the ML2 (Defined) to ML3 (Practiced) which is required for the Product application capabilities certification scenario. During this certification it was verified that the processes defined were actually used for the target of certification – TAS platform. The first batch of evidence for this step were provided in February 2020. Additional evidence material was provided during the course of the assessment. Final certification decision was granted in December 2020.

4.1.1 Examples for requirements

The following requirements have had their conformity validated and serve as examples for the reader:

- Vulnerability testing
 - The dedicated TAS-Platform security team provides customers with timely in-depth analyses of current applicable CVEs once per month.
- Penetration testing
 - A two-week-long Penetration Test in Vienna was deducted by DEKRA and the TAS-Platform development team in context of certMILS.
- Independence of testers
 - The dedicated TAS-Platform testing team is situated in Romania and is therefore independent of the TAS-Platform development team which is situated in Austria.
- Secure operation guidelines
 - The TAS-Platform development team provides customers with a dedicated and always up-to-date “Security Handbook”, as well as second level support from developers themselves.

TAS-Platform does comply with all needed requirements except for five. Two examples:

¹ N/A (not applicable) is not needed when N/E is presented within this certification scheme.

² Available for the public on: <https://www.iecee.org/documents/refdocs/>

- One requirement (SM-10, “Custom developed components from third-party suppliers”) is not applicable because TAS-Platform does not use specifically developed components from a third-party supplier.
- The other not fulfilled requirement (“Secure disposal guidelines”) is forwarded to the customer as TAS-Platform is delivered separately from the hardware and is not delivered with a preconfigured user on the main file system, except an account for an administrative user which is initially not usable. There is no user data on the system and customers must set up all needed user accounts manually themselves after setting up the administrative user before all else by setting a password.

4.2 IEC 62443-4-2

The criteria used for the assessed requirements selection were chosen to be as close as possible to the used standard to assure technical security requirements for IACS components have been fulfilled. The process of certification was based upon the IEC 62443-4-2 standard.

(Note: Some of the text here has already been described in detail in section 3.2 of D7.3 [4], and has been intentionally repeated to make it available to readers of this public deliverable view.)

(1) The first step for the applicant was to submit an application to be assessed for conformance which happened in January 2020. After contractual matters were solved, the applicant received the Test Report Form (TRF) and its annex, plus Questionnaire. The questionnaire provides certification body with information necessary for the next step – scoping of submittal. This was deemed to be IEC 62443-4-2 SL3 and was submitted in February 2020.

It especially provides the information of requirements and maturity levels chosen, identification of certification scenarios and specifications of product and processes connected with its development that are going to be assessed.

(2) In the next phase the applicant completed the applicable portions of a Test Report Form (TRF) and provided evidence in support of the capabilities that are intended to demonstrate compliance to the selected requirements.

After a brief stop to certification activities in the first quarter of 2020 due to the COVID-19 pandemic, certification continued in August 2020.

THA was again well prepared for delivering evidence because of Reinhard Hametner’s groundwork regarding the standard and the very well organized TAS Platform development teams document management, which included entirely new documents including a security architecture, security case, virtualization setup guide and various additions regarding safety and security to already existing documents, e.g. the “TAS Platform Setup Guide”. All of these documents and their respective internal references were labelled for safety and/or security to be easily found by the customer.

Each selected IEC 62443-4-2 security requirement was evaluated against the supporting evidence supplied by the applicant to determine compliance by certification body.

(3) The results of the assessment are gathered in the TRF and its annex. In this form it was also presented to the applicant. The possible results for each requirement are³:

- pass
- fail
- N/E (not evaluated)

(4) For requirements that were met, a certificate was issued. Requirements for these certificates are again defined by IEC 62443-4-2 – all certification bodies are obliged to follow these instructions. They

³ N/A (not applicable) is not needed when N/E is presented within this certification scheme.

are defined in IEC EE OD-2037⁴ (edition 3.4, 2020-10-16) IEC EE Test Certificates. THA again fulfilled nearly all requirements, except non-applicable ones such as requirements regarding wireless connectivity. The certificate was issued in December 2020 without any further complications.

4.2.1 Examples for requirements

The following requirements have the conformity statement “Fully Implemented” and provide the reader with excerpts of the statements.

- Account Management
 - Product is based on Linux OS which contains a concept of local account management. Remote management of accounts and identifiers is supported. Centralized account management can be done with LDAP.
- Authorization Enforcement
 - Product is based on Linux OS and distributed packages provide the capabilities to fulfill this requirement.
Users and groups
Pluggable Authentication Modules (PAM)
File permissions/umask
Set restrictive access rights in proto files
- Unsuccessful Login Attempts
 - Product is based on Linux OS enhanced by PAMs which provide the capability to support this requirement. PAM default configuration is available and additionally described in the Security Handbook. SSH supports this capability as well via the MaxAuthTries variable.
Pluggable Authentication Modules (PAM)
SSH Server

The following requirements have the conformity statement “Partly Implemented” and provide the reader with excerpts of the statements. Partly implemented requirements are forwarded to the customer as SecACs.

- Automated notification of integrity violations
 - MD5 checksums are provided for software packages which are used for integrity checks in safety context (e.g. text segment check of an application). Integrity checks of software loaded during the boot process are only performed on Secure Boot enabled boards where unsigned or falsely signed packages are not loaded.
- Authenticity of software and information
 - Authenticity checks of software and information are only done on Secure Boot enabled boards (D10 and SC33). Currently only the OS is authenticated, user and application software is not protected.
- Information persistence
 - Product is based on Linux OS and distribution which provide the capability to support this requirement. Basic functionality is integrated, e.g. in rm, opkg, dd or fdisk commands. Explicit packages like wipe for secure erase of data on the target system are not deployed as decommissioning is in the responsibility of the customer.

⁴ Available for the public on: <https://www.iecee.org/documents/refdocs/>

Chapter 5 Scope and meaning of obtained certification

In a world of rising security threats and increasing number of attacks on critical infrastructure, which is targeted by criminal entities such as underground and state-funded hacking groups there is a growing need for higher levels of security.

Downtimes and complete breakdowns of compromised and/or breached critical infrastructures are able to physically hurt people and moreover the economy. Thus, new security measures are nowadays demanded by customers to minimize the attack surface and ultimately, certifications according to IEC 62443-4-1 and IEC 62443-4-2 were chosen as they deemed to be a perfect fit for TAS Platform concerning safety and security.

IEC 62443-4-1 ML 2 (Managed) was chosen to provide the evidence that the formal procedures required could be followed, and therefore IEC 62443-4-2 SL 3 was chosen because the TAS Platform development team was already actively working on prevention of unauthorized disclosure using sophisticated means, such as a monthly vulnerability analysis including testing of public exploits.

The scope is limited to the component, other THA subsidiaries and customers still have to use it correctly for building a MILS based system, as described in various documents, such as the “TAS Platform Setup Guide”, “TAS Platform Security Handbook” and “Virtualization on TAS Platform”, where extensive documentation can be found.

Chapter 6 Lessons learned

On the side of Applicants for certification:

- A lot of work on documentation needed – proofs that support the Conformity statement provided to the Certification Body
- Without the well prepared and organized structure of the TAS Platform development teams document management, certification would have probably taken much longer.
- As this was the first certification according to IEC 62443 for THA, the right scoping and groundwork by Reinhard Hametner eased the process.
- The very good and quick communication in the certMILS project between partners regarding information and issues also tremendously eased the process.
- Not a clear understanding of what the subject of assessment should be for different parts of IEC 62443 (especially in case of IEC 62443-4-2) as there might be different interpretations of what a term “Component” represents.
- Certain features of the certification scheme are unclear to the applicants. The certification scheme presents new features that are not common in the certification field and services. For example the possibility to choose the requirements that will eventually form the certification criteria.
- Publicly available materials (e.g. on IECEE website) do not provide much details of the certification scheme (evaluation processes, specifics etc.)

On the side of Certification Bodies:

The following lessons learned are almost identical to those stated in D8.4 as they are valid for both pilots and for certification services built upon IEC 62443 standards overall. Both pilots have the same certification body – EZU.

- Better communication with the applicants needed
 - o explanation of requirements, maturity levels and other specific aspects of the certification scheme
- Support from the applicants during the evaluation and certification process is fundamental for correctness of the whole process and information provided in the final reports and other outputs.
- Incorporation of the certification scheme details into our own methodology
- Improving internal processes that follow-up the processes defined in the certification scheme is necessary
- Composition aspects – not clearly covered by the certification scheme from IECEE itself. Pushed forward by the work in certMILS – based on discussions with THA and SYSGO.

More lessons learned on the side of certification of IEC 62443-4-2:

- While the evaluation for processes and services is relatively straightforward, evaluation of IEC 62443-4-2 brings more challenges.
- We learnt that this standard can be used in a broad spectrum of environments (not just in industrial automation).
- That means a high variety of products can be subject of evaluation - high requirements on experience and knowledge.
- Usually those type of products have a lot of different (partly unique) concrete versions (e.g. each with different serial number). They might have a common base, but at the end provide (slightly) different features.

Chapter 7 Summary and Conclusion

D7.4 is the final deliverable and puts closure on the overall very effective and comprehensive work done in the Work Package 7. The report on validated security certification methodology with railway pilot contains information about how the methodology defined in D1.3 was applied (Chapter 1.1) and suggestions for its further improvement (Chapter 1.2).

In Chapter 2 we described how integration into existing and emerging certification schemes affected our project and what emerging certification scheme can we already identify.

Chapter 3 illustrates how railway existing safety and regulatory requirements are enhanced by the security certification or where any obstacles or differences were identified.

In Chapter 4 we summarize the outcomes from certification/evaluation process. With that being said, we can only disclose information that can be shared with the public.

In Chapter 5 we identified numerous lessons learnt, whose application can further enhance and improve evaluation and certification activities, and the scope and meaning of the obtained certification for THA.

And last but not least, in the Annex A of this document we enclose the certificates for IEC 62443-4-1 and 62443-4-2 issued by EZÚ for Thales.

Chapter 8 List of Abbreviations

Abbreviation	Translation
ENISA	European Network and Information Security Agency
IECEE	IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components
EU	European Union
IACS	Industrial Automation and Control System
NCB	National Certification Body
CBTL	Certification Body Testing Laboratory

Chapter 9 Bibliography

[1] ENISA. RAILWAY CYBERSECURITY. Security measures in the Railway Transport Sector. November 2020. Available at: <https://www.enisa.europa.eu/publications/railway-cybersecurity>

[2] Deliverable D1.3 “Compositional security certification methodology”. certMILS, Horizon 2020, no 731456. Available at: <https://doi.org/10.5281/zenodo.2586493>

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

[4] Deliverable D7.3 “Railway pilot security evaluation”. certMILS, Horizon 2020, no. 731456.

Annex




		Ref. Certif. No. CZ-3026
IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)		
Certificate of Conformity – Industrial Cyber Security Capability		
Type	Product Application of Capabilities Assessment	
Name and address of the applicant	Thales Austria GmbH Handelskai 92, A-1200 Vienna, Austria	
Certificate Coverage (including Version)	TAS Platform Core SW 2.4.1	
Standard	IEC 62443-4-1:2018	
Requirements Assessed / Total Requirements	Security management (10/13), Security requirements (5/5), Secure by design (4/4), Secure implementation (2/2), Security verification and validation testing (5/5), Management of security-related issues (6/6), Security update qualification (5/5), Security guidelines (5/7)	
Additional information (if necessary may also be reported on page 2)	This certificate is issued in conjunction with an IEC 62443-4-2 certificate of conformity n. CZ-3027	
As shown in the Test Report Ref. No. which forms part of this Certificate	605646-05/01 of: 18.12.2020	
This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.		
Elektrotechnický zkušební ústav, s.p. Pod lisem 129/2, 171 02 Praha 8 – Troja Czech Republic		 Miroslav Sedláček Certification and Inspection Manager
Date: 21.12.2020		

Figure 2: IEC 62443-4-1 certificate




		Ref. Certif. No. CZ-3027
IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)		
Certificate of Conformity – Industrial Cyber Security Capability		
Type	Product Capability Assessment	
Name and address of the applicant	Thales Austria GmbH Handelskai 92, A-1200 Vienna, Austria	
Certificate Coverage (including Version)	TAS Platform Core SW 2.4.1	
Standard	IEC 62443-4-2:2019	
Requirements Assessed / Total Requirements	Common Component Security Constraints (4/4), Identification and authentication control (11/22), Use control (12/21), System integrity (8/19), Data confidentiality (1/5), Restricted data flow (1/4), Timely response to events (3/3), Resource availability (6/11), Software application requirements (0/3), Embedded device requirements (0/13), Host device requirements (0/14), Network device requirements (6/22)	
Additional information (if necessary may also be reported on page 2)	This certificate is issued in conjunction with an IEC 62443-4-1 certificate of conformity n. CZ-3026	
As shown in the Test Report Ref. No. which forms part of this Certificate	605646-05/02 of: 18.12.2020	
This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.		
Elektrotechnický zkušební ústav, s.p. Pod lisem 129/2, 171 02 Praha 8 – Troja Czech Republic		
Date: 21.12.2020	Signature: Miroslav Sedláček Certification and Inspection Manager	

Figure 3: IEC 62443-4-2 certificate