D8.4

Report on validated security certification methodology with subway 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:	1st January, 2017
Duration:	48 months
Programme:	H2020-DS-LEIT-2016

Deliverable type:	Report
Deliverable reference number:	DS-01-731456 / D8.4 / 1.1
Work package contributing to the deliverable:	WP 8
Due date:	M54 – June 2021
Actual submission date:	5th July, 2021

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

Abstract:	The report contains how the methodology was applied, improvement suggestions, suggestion for integration into existing and emerging certification schemes, illustrating how subway 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, subway, 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)

Petr Novobilsky (QMA)

Jiri Sterba (EZU)

Jan Henys (EZU)

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

This deliverable describes how the methodology was applied, includes improvement suggestions, as well as suggestions for integration into existing and emerging certification schemes. It also illustrates how subway existing safety and regulatory requirements are enhanced by security certification with focus on identifying and solving obstacles or conflicts between those requirements and security certification.

As certMILS has approached its final month of implementation and certification according to IEC 62443 standards, this document aims to be an overview of the outcomes of the applied security certification and evaluation methods, as well as of the fulfilled requirements of the introduced Subway Pilot from Q-media. It incorporates state-of-the-art contributions of the project partners EZU and Q-media and the internal requirements mapping of the Zone protection Gateway R02-100 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 of requirements 9

4.2 IEC 62443-4-2...9

4.2.1 Examples of requirements 12

Chapter 5 Scope and meaning of the certification...13

Chapter 6 Lessons learned 14

Chapter 7 Summary and Conclusion 16

Chapter 8 List of Abbreviations...17

Chapter 9 Bibliography 18

Annex...19

List of Figures

Figure 1: ENISA Certification Scheme 3

Figure 2: Extract from the Test Report for IEC 62443-4-1 certification 8

Figure 3: Extract from the Test Report for IEC 62443-4-2 certification 11

Figure 4: IEC 62443-4-1 certificate 19

Figure 5: IEC 62443-4-2 certificate 20

Chapter 1 Introduction

Over the last few years there have been more and more new technologies introduced and adopted by the rail industry (railway, subway). For example, increased use of wireless communication on trains, at stations and even at the operational control centre (OCC) - wireless systems such as the European Railway Traffic Management System (ERTMS) and communications-based train control (CBTC) signalling. New technologies expose the trains to new kind of cyber-attacks. Up until recently, the networks were completely isolated from the external factors, so the operators are mostly not very well prepared for detecting and resolving the new threats. What differentiates the subway from the railway world is probably the fact that once the attacker stops a train, he can create a big ripple effect that causes huge disruption across the whole network, as opposed to railway services where there are usually only two tracks and alternative routes available. With timings between one train and the next so short, creating huge disruption in metro undergrounds is much easier and has a more severe impact [1].

Within this context the certMILS consortium was running the subway pilot. Understanding the importance and impact is crucial and having Q-media as one of the partners of Dopravní podnik hlavního města Prahy (further referred to as DPP) was very beneficial. DPP is operating all metro lines in Prague. With four tasks (Pilot specification, Pilot security design compliant to ISO/IEC 15408, IEC 62443 and EN50129/159, Pilot implementation, Pilot security evaluation) and three deliverables (Compositional design of the subway pilot, Subway demonstrator implementation, Pilot security artefacts - Subway) 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

Q-media, as the pilot’s owner, after market analysis and discussions with its partners realized that IEC 62443 standards provide a conscious way to certificate Industrial Systems and their components integrated in the subway sector. The reasoning for that decision is that the requirements of those standards focus on fulfilling the following aspects:

- Data integrity that flows to and from the evaluated devices. Many of Industrial Control Systems or their components 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 kernel (PikeOS), which is a realization of the MILS platform within the pilot architecture, and by the features of the IECEE certification schemes used for the certification within this pilot.

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 learned from the evaluation and certification activities. Further work should be based on lessons learnt defined in 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 schemes already during the course of the project. After several discussions about evaluation and certification activities we eventually identified that IECEE certification scheme built around IEC 62443 standards is perfect fit for our project´s pilots and subway pilot especially.

The strong connection between those activities can be further enhanced by having EZU as 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 the 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 CBTLs.

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):

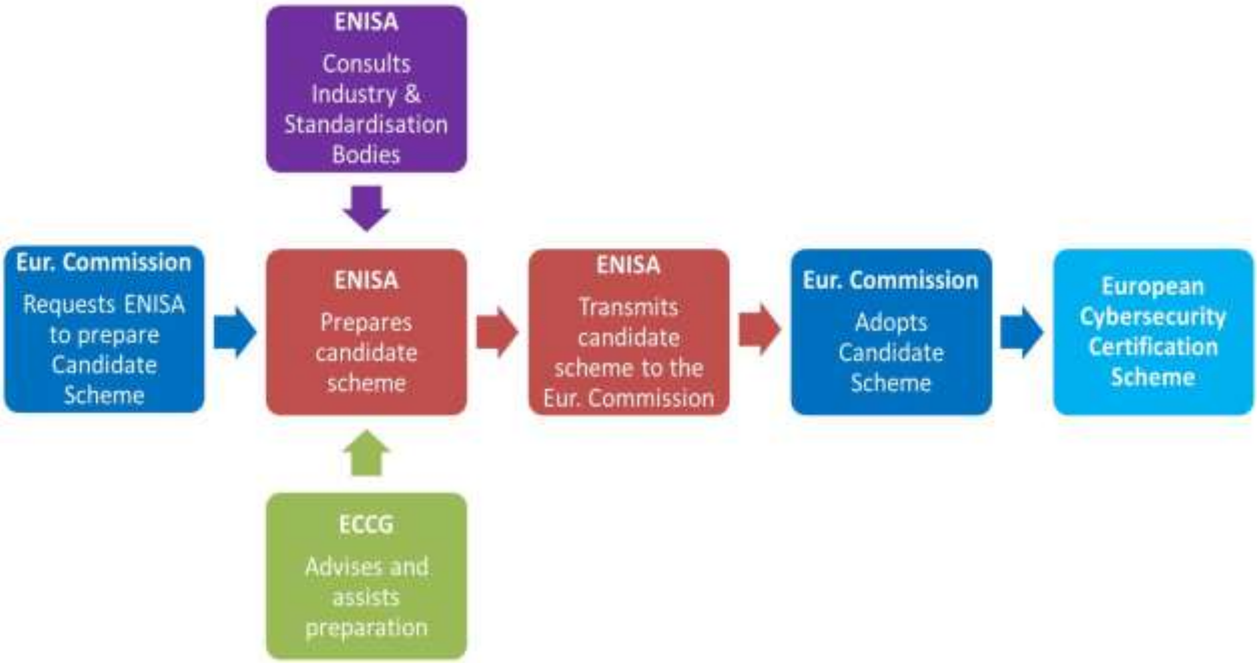

ENISA
Consults Industry & Standardisation Bodies
Eur. Commission
Requests ENISA to prepare Candidate Scheme
ENISA
Prepares candidate scheme
ENISA
Transmits candidate scheme to the Eur. Commission
Eur. Commission
Adopts Candidate Scheme
European Cybersecurity Certification Scheme
ECCG
Advises and assists preparation

Figure 1: ENISA Certification Scheme[1]

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

At the time of writing this report, we can summarize the current status as follows:

- First scheme published under the guidelines of the CSA (Cybersecurity Act) – EUCC - Common Criteria based European candidate cybersecurity certification. It proposes the creation of a common European framework for the certification of "cybersecure" ICT products and services. It can be considered a horizontal scheme, as it can be usable in several sectorial competences. EUCC is based on Common Criteria (ISO/IEC 15408 and ISO/IEC 18045) and is aimed at replacing the current national certification schemes also based on Common Criteria.
- Several other schemes are in phase of development (e.g. for 5G, IoT).

The certMILS consortium is already active in this new approach to European cybersecurity certification through:

- Partner ATSEC participating in ad-hoc Working Group 01 - Transposition of the SOGIS-MRA certification framework and
- Active approach to public consultation of the first certification scheme (EUCC) 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

Railway operation incl. railway facilities of the subway are subject to the Czech Railway Authority (Railways Act). The development, deployment and operation of these devices are subject to railway regulations and standards. Due to the fact that these are critical infrastructure systems, they are subject to additional regulations that ensure their security.

Each railway undertaking has a set of internal rules for applying these generally binding rules. It applies these requirements to a specific environment or to specific facilities in a way that is acceptable to it. The economic aspect plays a role here.

One of the areas currently being emphasized is the cybersecurity of the critical infrastructure.

Within the Czech Republic, the guarantor of cybersecurity is NÚKIB, which uses ZKB (Act No. 181/2014 Coll., On Cyber Security and on Amendments to Related Acts (Cyber Security Act). It is also responsible for Directive (EU) 2016/1148 of the European Parliament and of the Council - NIS.

Decree 82/2018 Coll. incorporates the NIS Directive into the national legal system and provides, inter alia, for the areas concerned:

- content and scope of security measures
- types, categories and assessment of the significance of cybersecurity incidents
- requirements and method of reporting a cybersecurity incident

The subway is one of the affected areas where NIS is applied. For this purpose, the operator created a set of internal regulations based on EN 27000, which ensure the cybersecurity of its information system.

The field of railway technology, as mentioned above, is subject to railway standards. The default regulation is [8], which accepts the 62443 standards for assessing IT security.

Devices operating at the border of these two cybernetic systems must be designed to separate them to meet their functional and non-functional requirements.

Chapter 4 Summary of the outcomes from certification/evaluation process

QMA paid close attention to correctly reference all needed requirements from the internal QMA 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 QMA 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 and/or contacts.

The standardization and certification according to IEC 62443-4-1 and IEC 62443-4-2 was considered as very practicable and reasonable for QMA and particularly for the Zone protection Gateway R02-100 development cycle.

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 the Zone protection Gateway R02-100, which is implementing also a very important part – PikeOS separation kernel. IEC 62443-4-2 offered new challenges in the terms of the product (component) capabilities for QMA and helped to address these innovations accordingly.

All claimed requirements were assessed during the certification. A list of these requirements is included in the D8.3 deliverable [4], section 2.1 with requirements from IEC 62443-4-1 and section 3.1 with requirements from IEC 62443-4-2. For requirements that were evaluated as "Pass" EZU issued CB Certificates, one for IEC 62443-4-1 and one for IEC 62443-4-2. Both certificates are valid worldwide and are issued in conjunction with each other, as required by the certification scheme. Examples of the assessed requirements can be found below in sections 4.1 and 4.2.

4.1 IEC 62443-4-1

The criteria used for the assessed requirements selection were chosen to be as close as possible to the full scope of the used standard to assure that product lifetime security has been fulfilled. All assessed requirements were declared maturity level 3, with corresponding conformity evidence being delivered by QMA and assessed by EZU. 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 D8.3 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 certification body with information necessary for the next step – scoping of submittal, which has been deemed to be IEC 62443-4-1 ML 3.

As a first step, QMA submitted an application in context of the certMILS project to EZU in May 2020. It provided the information of requirements and maturity levels chosen for individual requirements (ML3), 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 that each selected IEC 62443-4-1 security requirement was evaluated against the supporting evidence supplied by the applicant to determine compliance by the certification body.

QMA submitted the first batch of conformity evidence in May 2020. Additional evidence material was provided during the course of the assessment.

(3) The results of the assessment are gathered in the TRF and its annex, forming a final TR (Test Report). In this form it was also presented to the applicant. The possible results for each requirement are the following[2]:

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

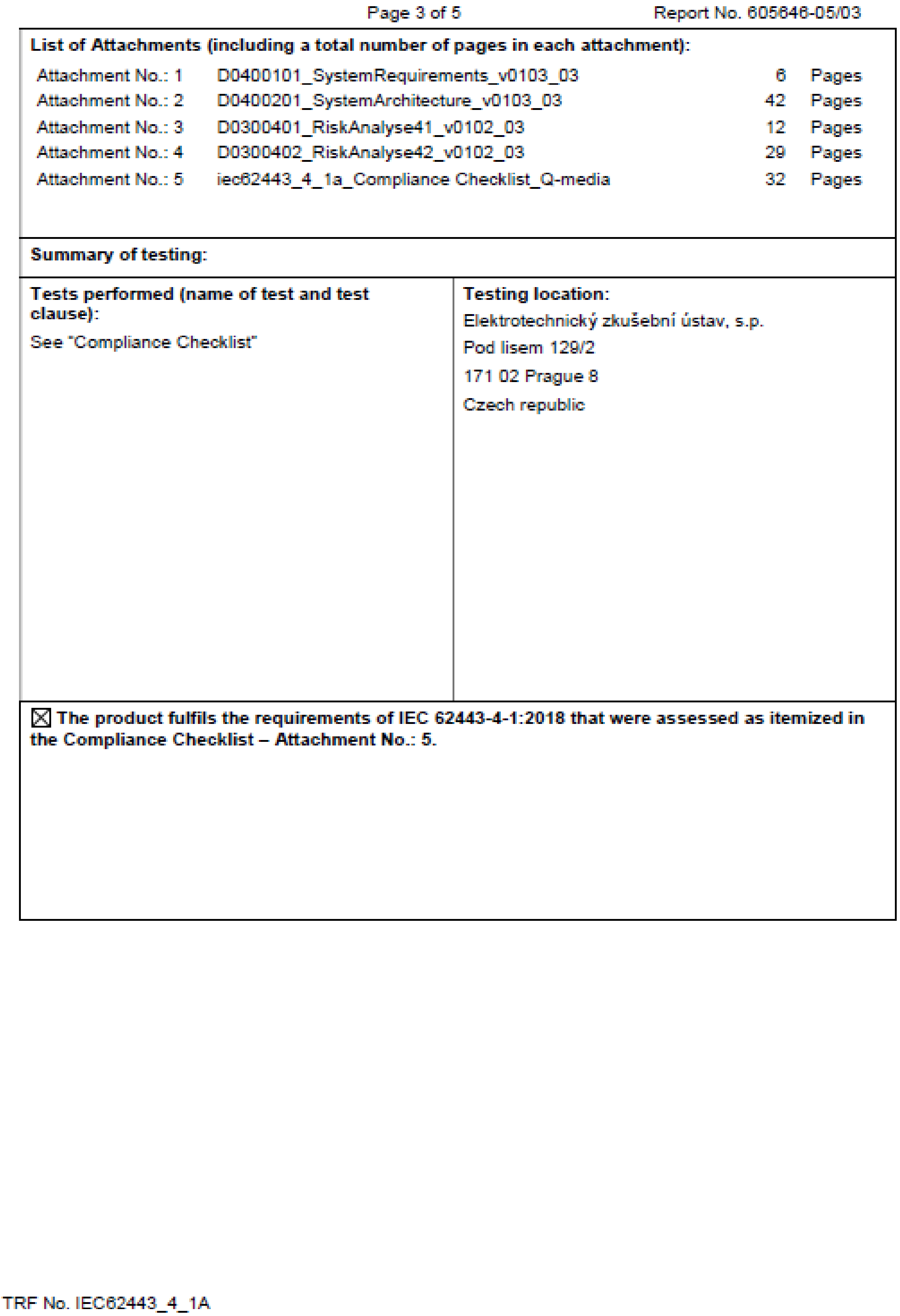
For requirements that were met a certificate was issued. Requirements for these certificates are again defined by IECEE – all certification bodies are obliged to follow these instructions. They are defined in IECEE OD-2037 [3] (Edition 3.4, 2020-10-16) IECEE Test Certificates.

(4) The certificate was then issued to QMA in June 2021 without any further complications.

The Test Report (TR) itself carries basic information about QMA and EZU and information about the scope and target of the assessment. Conformity with selected individual requirements of IEC 62443-4-1 is confirmed in its Attachment No.: 5 (“Compliance Checklist”). There are 5 Attachments to this TR overall, as shown in the extract of the TR (page 3) below (see Figure 2):

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

[3] Available for public on: https://www.iecee.org/documents/refdocs/



Page 3 of 5 Report No. 605646-05/03

List of Attachments (including a total number of pages in each attachment):

Attachment No.: 1	D0400101_SystemRequirements_v0103_03	6	Pages
Attachment No.: 2	D0400201_SystemArchitecture_v0103_03	42	Pages
Attachment No.: 3	D0300401_RiskAnalyse41_v0102_03	12	Pages
Attachment No.: 4	D0300402_RiskAnalyse42_v0102_03	29	Pages
Attachment No.: 5	iec62443_4_1a_Compliance Checklist_Q-media	32	Pages

Summary of testing:

Tests performed (name of test and test clause):	**Testing location:**
See "Compliance Checklist"	Elektrotechnický zkušební ústav, s.p. Pod lisem 129/2 171 02 Prague 8 Czech republic

☒ **The product fulfils the requirements of IEC 62443-4-1:2018 that were assessed as itemized in the Compliance Checklist – Attachment No.: 5.**

TRF No. IEC62443_4_1A

Figure 2: Extract from the Test Report for IEC 62443-4-1 certification

4.1.1 Examples of requirements

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

- Security management (SM-1) - the development process was supplemented by a part ensuring the development of security-relevant equipment. The development of SL-3 level equipment was verified.
- Security requirements (SR) - based on [7] and performed Security analysis, more than 250 System requirements were identified within the process.
- Penetration testing (SVV-4) - in accordance with the requirements of the standard, penetration tests were performed on R02-100 by an independent agency (SVV-5). The resulting Test report was part of the documentary part of the certification process.
- Security guidelines (SG) - for the use of R02-100 in subway, the User Guide was developed. This guide considers both the operator's requirements and the possibilities of this embedded component, connecting the Trusted and Untrusted zones.

Zone protection Gateway R02-100 does not comply with the following requirements:

- SM-10
  - Reasoning: No components have been developed externally for Gateway
- Practice SUM (Security update qualification)
  - Reasoning: Security update of products is a part of the Patch management process, implemented according to [5], part SP.11. The purpose is to harmonize activities related to security updates of products with the standard [6].

4.2 IEC 62443-4-2

The criteria used for the assessed requirements selection were chosen by the applicant during a scoping phase of the certification process. All assessed requirements were declared as “Passed”, with corresponding conformity evidence being delivered by QMA and assessed by EZU. The process of certification was based upon IEC 62443-4-2 standard.

(Note: Some of the text here has already been described in detail in section 3.2 of D8.3 deliverable [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 May 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 submitted later in May 2020.

It especially provided 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.

The assessment was interrupted by the COVID-19 pandemic and problems connected with the demonstrator (DPD), but QMA was well prepared for delivering evidence thanks to the hard work of all staff involved.

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

(3) The results of the assessment are gathered in the TRF and its annex, forming a final TR (Test Report). In this form it was also presented to the applicant. The possible results for each requirement are[4]:

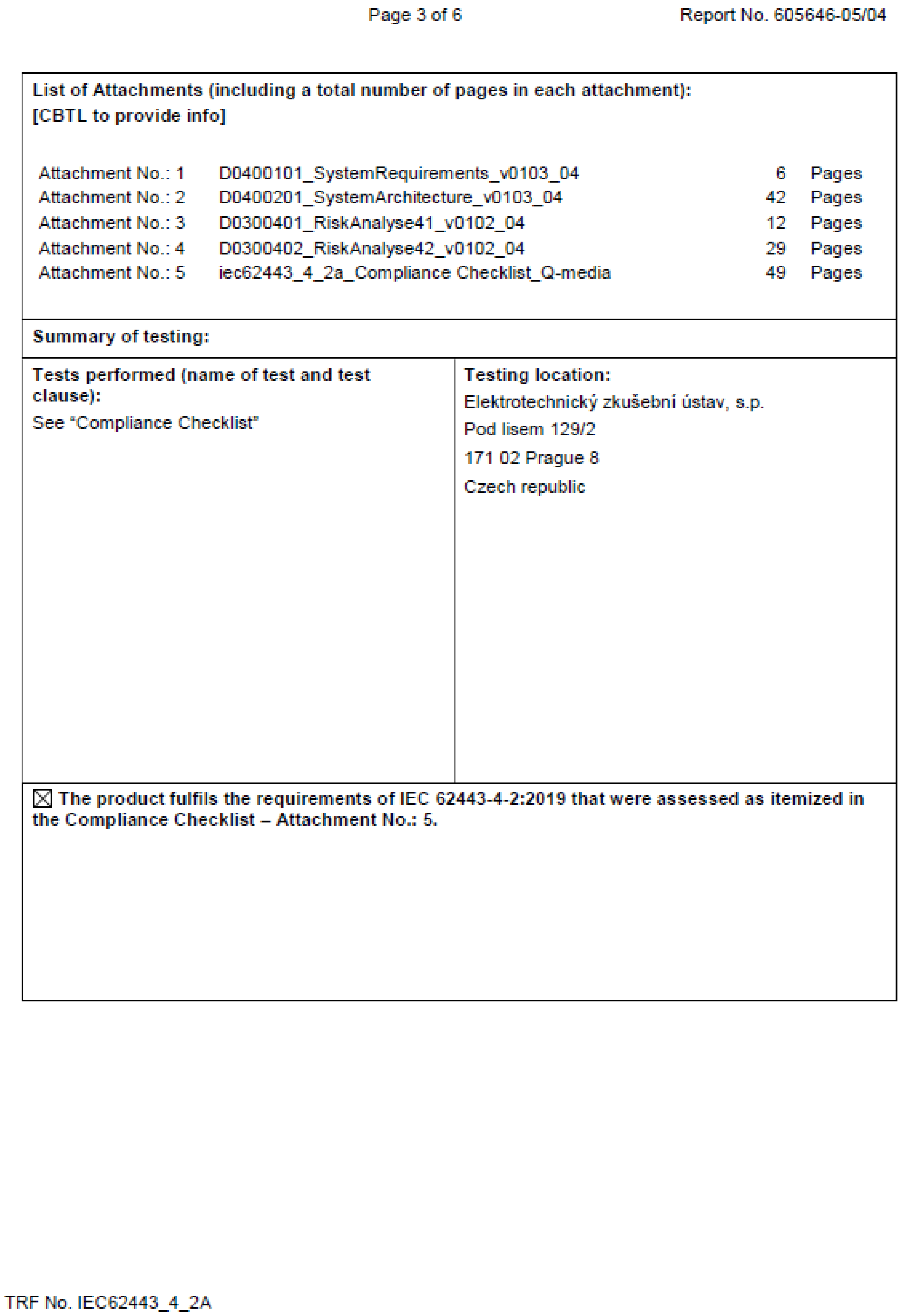
- pass
- fail
- N/E (not evaluated)

(4) For requirements that were met a certificate was issued. Requirements for these certificates are again defined by IECEE – all certification bodies are obliged to follow these instructions. They are defined in IECEE OD-2037 [5] (edition 3.4, 2020-10-16) IECEE Test Certificates. The certificate was issued in June 2021 without any further complications.

The Test Report (TR) itself carries basic information about QMA and EZU and information about the scope and target of the assessment. Conformity with selected individual requirements of IEC 62443-4-2 is confirmed in its Attachment No.: 5 ("Compliance Checklist"). There are five Attachments to this TR overall, as shown in the extract of the TR (page 3) below (see Figure 3):

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

[5] Available for public on: https://www.iecee.org/documents/refdocs/



Page 3 of 6

Report No. 605646-05/04

List of Attachments (including a total number of pages in each attachment):
[CBTL to provide info]

Attachment No.: 1	D0400101_SystemRequirements_v0103_04	6	Pages
Attachment No.: 2	D0400201_SystemArchitecture_v0103_04	42	Pages
Attachment No.: 3	D0300401_RiskAnalyse41_v0102_04	12	Pages
Attachment No.: 4	D0300402_RiskAnalyse42_v0102_04	29	Pages
Attachment No.: 5	iec62443_4_2a_Compliance Checklist_Q-media	49	Pages

Summary of testing:

Tests performed (name of test and test clause):	**Testing location:**
See "Compliance Checklist"	Elektrotechnický zkušební ústav, s.p. Pod lisem 129/2 171 02 Prague 8 Czech republic

☒ **The product fulfils the requirements of IEC 62443-4-2:2019 that were assessed as itemized in the Compliance Checklist – Attachment No.: 5.**

TRF No. IEC62443_4_2A

Figure 3: Extract from the Test Report for IEC 62443-4-2 certification

4.2.1 Examples of requirements

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

- System Integrity (CR 3.4) - a key element guaranteeing the system integrity of the Gateway R01-100 is the Secure Boot process. The process will only allow you to boot an undamaged and digitally signed system image.
- Boundary protection (NDR 5.2 and extensions) - compliance is achieved using the MILS platform PikeOS. It guarantees the separation of individual network segments, and the implementation of specific rules for security features at the segment boundaries.
- Multifactor Authentication (CR 1.01) and Strength of password-based authentication (CR 1.07) are examples of requests that have been covered by additional measures. GW has covered requests only in cooperation with an external LDAP server.

Zone protection Gateway R02-100 does not comply with all requirements from IEC 62443-4-2. Following are examples of requirements that were not subject of the assessment:

(A) Requirements not covered:

- Wireless access management (CR 1.06) and Use control (CR 2.02) - GW does not contain a wireless interface
- Use control for portable and mobile devices (CR 2.03, 2.04) - this is not a mobile device.
- Software application requirements - SW applications were not the subject of the assignment

(B) Requirements are resolved, but not subject to certification:

- Protection of physical diagnostic and test interfaces (EDR2.13) - is covered by the HW property. The manufacturer only activates JTAG for development pieces. The production line has this element inactive.
- Update authenticity and integrity (EDR 3.10) - implemented, not required for a specific application. Certification is expected in the next release after specifying user requirements.

Chapter 5 Scope and meaning of the certification

The scope is limited to the component and to the requirements chosen for the assessment.

For QMA, certificates mean successfully completing essential activities for the development, production and subsequent maintenance of security-relevant components.

The newly applied process, the effectiveness of which was verified on the R02-100 product, will enable a flexible response to cyber threats and related customer requirements throughout the product life cycle.

As a result, the process will have a positive effect on the company's competitiveness.

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. 41 out of 47 process requirements of the 62443-4-1 standard were implemented to develop security-relevant components. In addition, by applying new development procedures and modifying internal guidelines, a process has been created that will make it possible to respond flexibly to the specific security requirements of metro systems.
- Standard 62443-4-2 does not explicitly specify the subject matter of the assessment. In most cases, a component is defined by the requirements of the system of which it is to be a part, or its properties determine the customer's requirements. Developing a generic system to cover all the requirements of the standard is quite expensive.

  Only the requirements of standard 62443-4-2, relevant to the product, were subject to assessment. In the case of gateway R02-100, they have assessed only 44 requirements out of a total of 141. This approach achieved a significant reduction in the costs of implementing measures and product certification.
- Some security requirements are difficult for embedded systems to meet. These are requirements that cannot be covered by the system's functionalities and an expensive system redesign would have to be performed. The criterion may be the financial complexity of the solution, excessive use of system resources, etc. In this case, some aspects of security must be performed by an external component. An example is user management (CR1.1 SL-3), which contains a request for multifactor authentication. In this case, the certification of cooperation with the external component was more effective than the development of a new SW module.
- When preparing certification documents, it is possible to follow up on related certification programs. Because the product or its configuration is usually specific, the certification scheme can be adapted to this fact. However, it is always necessary to know the role of the component in the system as a whole and to assess the interaction with other security standards, such as IEC 15408 or IEC 27000. In addition to eliminating security gaps, this procedure can also simplify the certification process by using available artefacts. In the case of gateway R02-100, hypervisor artefacts obtained from the certification process according to the IEC 15408 standard were used for the certification process.
- Gateway R02-100 was designed so that the application-dependent parts are independent of the communication platform. The principles of composite certification, which simplifies and speeds up the product patch management process, have been verified on this model.

On the side of Certification Bodies:

- Following lessons learned are almost identical to those stated in D7.4 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.
- Communication with the applicants needed:
  - 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 QMA, SRO 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

D8.4 is the final deliverable and closes the overall very effective and comprehensive work done in Work Package 8. The report on validated security certification methodology with railway pilot contains information about how the methodology defined in D1.3 was applied (section 1.1) and suggestions for its further improvement (section 1.2).

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

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

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

Chapter 5 shortly described the scope and meaning of the certification for the applicant.

In Chapter 6 we identified numerous lessons learnt, whose application can further enhance and improve evaluation and certification activities.

Last but not least, in the Annex of this document we enclose the certificates for IEC 62443-4-1 and 62443-4-2 issued by EZU for QMA.

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
OCC	Operational Control Centre
ERTMS	European Railway Traffic Management System
CBTC	Communications-Based Train Control

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 D8.3 "Pilot security artefacts – Subway". certMILS, Horizon 2020, no. 731456.

[5] IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

[6] ISA 62443-2-3:2020_D8E7 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment

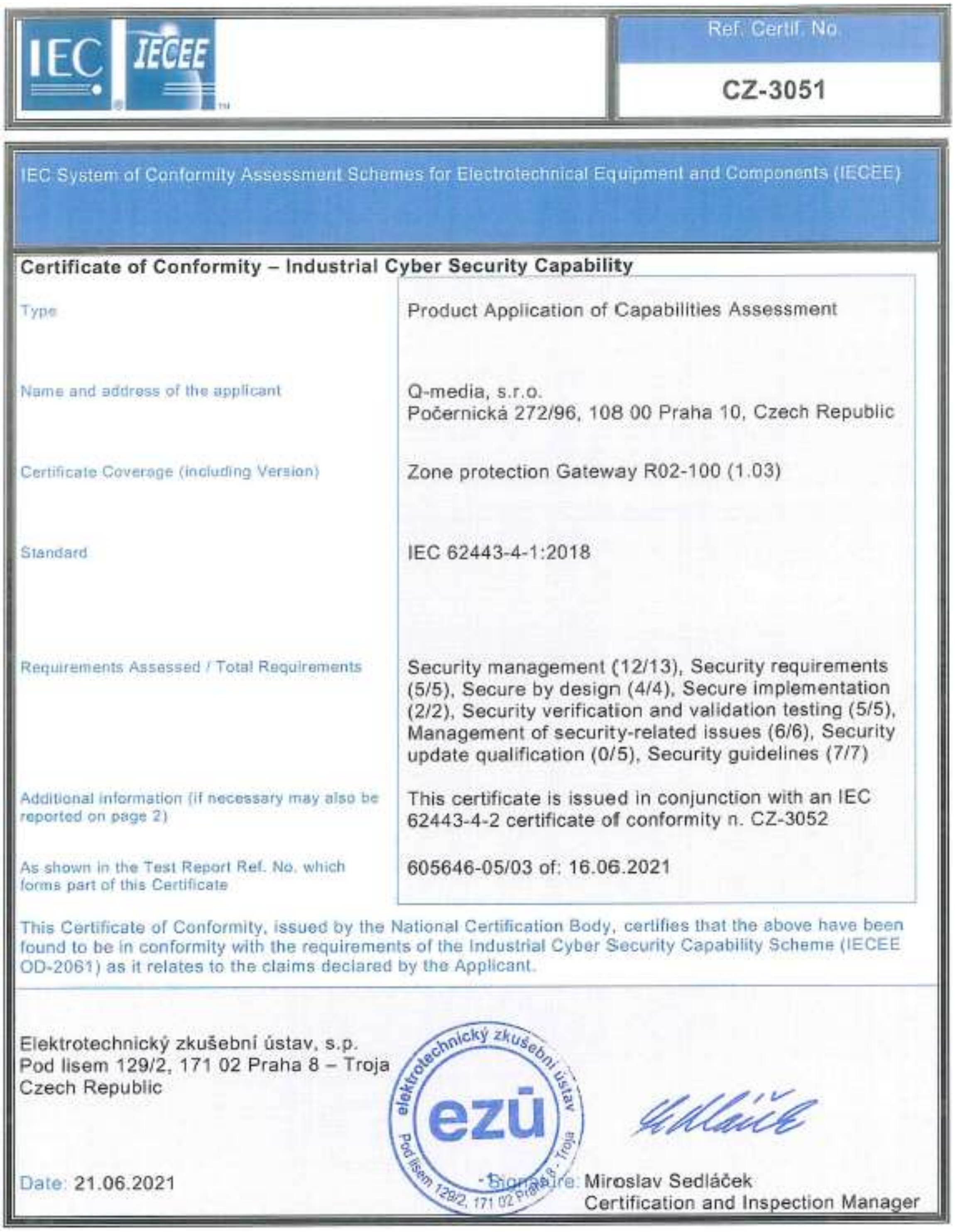
[7] Deliverable D8.1 "Compositional design of the subway pilot". certMILS, Horizon 2020, no. 731456.

[8] EN 50129 ed. 2: 2018 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[9] ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security

[10] ISO/IEC 27000 Information technology — Security techniques — Information security management systems

Annex



IEC IECEE

Ref. Certif. No.

CZ-3051

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	Q-media, s.r.o. Počernická 272/96, 108 00 Praha 10, Czech Republic
Certificate Coverage (including Version)	Zone protection Gateway R02-100 (1.03)
Standard	IEC 62443-4-1:2018
Requirements Assessed / Total Requirements	Security management (12/13), 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 (0/5), Security guidelines (7/7)
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-3052
As shown in the Test Report Ref. No. which forms part of this Certificate	605646-05/03 of: 16.06.2021

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.

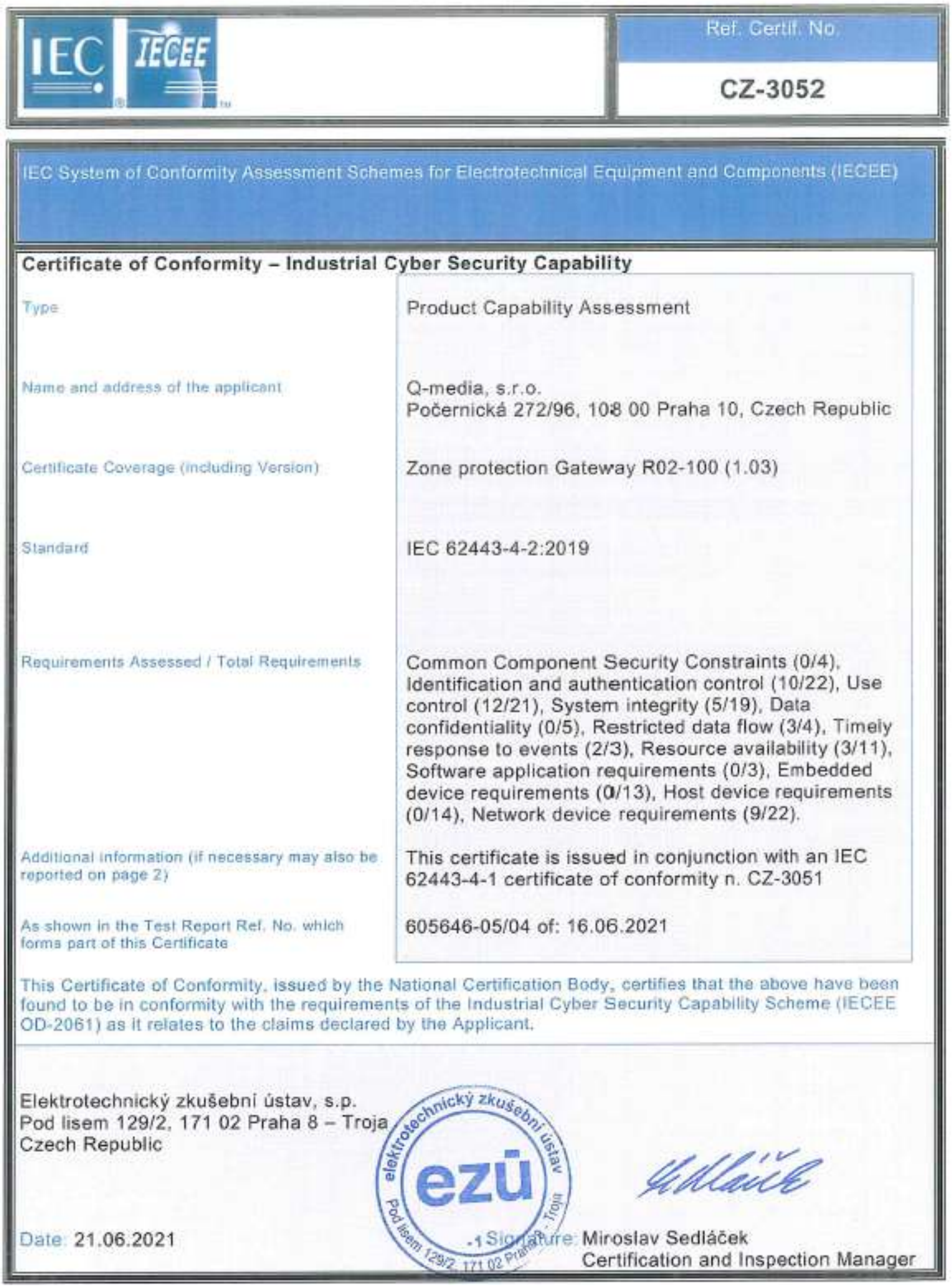
Elektrotechnický zkušební ústav, s.p.
Pod lisem 129/2, 171 02 Praha 8 – Troja
Czech Republic

elektrotechnický zkušební ústav
ezú
Pod lisem 129/2, 171 02 Praha 8 - Troja

Date: 21.06.2021

Signature: Miroslav Sedláček
Certification and Inspection Manager

Figure 4: IEC 62443-4-1 certificate



IEC IECEE

Ref. Certif. No.

CZ-3052

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	Q-media, s.r.o. Počernická 272/96, 108 00 Praha 10, Czech Republic
Certificate Coverage (including Version)	Zone protection Gateway R02-100 (1.03)
Standard	IEC 62443-4-2:2019
Requirements Assessed / Total Requirements	Common Component Security Constraints (0/4), Identification and authentication control (10/22), Use control (12/21), System integrity (5/19), Data confidentiality (0/5), Restricted data flow (3/4), Timely response to events (2/3), Resource availability (3/11), Software application requirements (0/3), Embedded device requirements (0/13), Host device requirements (0/14), Network device requirements (9/22).
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-3051
As shown in the Test Report Ref. No. which forms part of this Certificate	605646-05/04 of: 16.06.2021

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

elektrotechnický zkušební ústav
ezú
Pod lisem 129/2, 171 02 Praha 8 - Troja
-1

Date: 21.06.2021

Signature: Miroslav Sedláček
Certification and Inspection Manager

Figure 5: IEC 62443-4-2 certificate