D6.4

Report on validated security certification methodology with smart grid 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 / D6.4 / 1.0
Work package contributing to the deliverable:	WP 6
Due date:	M48 – December 2020
Actual submission date:	23rd December, 2020

Responsible organisation:	DEKRA TC (E&E)
Editor:	Álvaro Ortega
Dissemination level:	PU
Revision:	1.0

Abstract:	Evaluation – Certification Gap Analysis of the Smart Grid pilot according to the IEC 62443-4-1 and 62443-4-2 standards.
Keywords:	IEC 62443, RTU, PikeOS, high assurance, Smart Grid, MILS, IACS

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

Editor

Álvaro Ortega (E&E)

Alejandro Fernández (E&E)

Contributors (ordered according to beneficiary numbers)

Benito Caracuel (SCHN)

Ana Lourdes Sanz (SCHN)

Disclaimer

Executive Summary

This report contains how the compositional methodology was applied, including improvement proposals, suggestion for integration into existing and emerging certification schemes, illustrating how smart grid (IACS) existing safety and regulatory requirements are enhanced by the security certification with focus on identifying and solving obstacles/conflicts between those requirements and security evaluation.

As certMILS approaches its final months of implementation and certification according to IEC 62443, this document aims to be an overview of how the methodology was applied and which outcomes of the applied security certification and evaluation methods were reached during the evaluation phase. All the evaluation process integrated state-of-the-art contributions of the project partners: EZU, DEKRA and UROS and the internal requirements mapping of the RTU SCHN team to the chosen standards IEC 62443-4-1 and IEC 62443-4-2.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

This deliverable describes how the compositional certification methodology developed within the certMILS project was applied to the Smart Grid Pilot provided by Schneider Electric.

certMILS has the objective to develop and apply compositional certification methodology on three industrial pilots, using a common MILS architecture. From a logical perspective, this means that for finding a good compositional architecture, evaluation and certification, our search approach was not just a purely top-down search for the optimal fulfilment of external requirements, but also has a strong bottom-up starting point by using a technical component, the MILS separation kernel, of which we well understand the technical architecture as well as the assurance argument. Pilot demonstrators and security evaluators use the MILS platform to do compositional evaluation and certification according to certMILS methodology and industrial standards.

1.1 Connection to the methodology defined in D1.3

The compositional evaluation/certification methodology defined in D1.3 [9] covers the MILS architecture and provides several approaches for the evaluation/certification depending on how the control system is integrated and built.

DEKRA Testing and Certification performed an initial familiarization with the pilots provided by Schneider:

- High-assurance pilot: the solution in which PikeOS (separation kernel) is integrated
- Medium-assurance pilot: the solution in which PikeOS is not part of the architecture

The commonalities between them is that, from the component perspective, IEC 62443-4-2 can be applied as defined in chapters **4.2 IEC 62443 composition certification** and **5.2 IEC 62443 Specifics** of D1.3 [9] for verifying the fulfilment of the functional requirements.

Regarding the integration and composition using PikeOS in the High-assurance pilot, the evaluation/certification effort performed in WP5 by SYSGO and ATSEC using Common Criteria as presented in section **4.1 CC composition certification** of D1.3 [9] was applied.

Schneider Electric, as pilot owner, realized that IEC 62443 [2] standards provides a conscious way to certificate Industrial Systems integrated in Smart Grid 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 device. Many of Industrial Control Systems are integrated within critical systems that could led to a disruption of services if the data is inconsistent.
- Well-defined actions that the system users can accomplish.
- Protection against common attacks to IACS systems.
- All system and user actions must be reflected in the system logs. Then, such logs shall be protected against modifications.

IEC 62443 standards also provide flexibility and complexity thanks to division of different aspects to different parts (standards).

DEKRA and Schneider agreed in applying the methodology defined in D1.3 [9] as follows:

1. Schneider decided integrating PikeOS into the high-assurance pilot. The partitions defined are:
    a. partition 1, which includes the core functionality of the RTU (more critical), and,

   b. partition 2, which includes secondary functionalities of the RTU (less critical, such as the webserver for monitoring and supervision of the RTU).
2. The Composition Certification using CC as per section 4.1 of D1.3 [9] comes from the evaluation of the Separation Kernel (PikeOS) made by ATSEC. In a world where resources were unlimited, the separation kernel would also have undergone a broader IEC 62443 certification. However, as SKs are general-purpose products, and not limited to industrial control systems from a market perspective, for a SK vendor it is more meaningful to certify against CC. The CC process requirements are sufficient for a SK to be used as a component. In addition, the SK helps to fulfil certain IEC 62443-4-2 functional requirements, reusing assurance provided by the SK.
3. For the overall evaluation process encompassing the RTU and the SK, the approach defined in section 4.2 of D1.3 [9] has been used for IEC 62443-4-1 (Maturity Level 2) and IEC 62443-4-2 (Security Level 3). In the domain of industrial automation and control systems (IACS), the standard IEC 62443 considers the security of entire plants and takes strongly into account the constant changes that need to be made to a plant, by putting great emphasis on the processes during the life cycle of an IACS.
4. For the Medium-Assurance pilot (with no SK), the approach is slightly different as the Composition Certification using CC as defined in 4.1 of D1.3 [9] is not applicable. However, the evaluation in order to verify whether IEC-62443-4-1 and IEC62443-4-2 selected requirements for Maturity Level 2 and Security Level 3 respectively are fulfilled is the same.

1.2 Suggestions for improvement of methodology defined in D1.3

During the evaluation and after several discussions within the certMILS consortium, 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 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 [1] 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 Smart Grid 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 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.

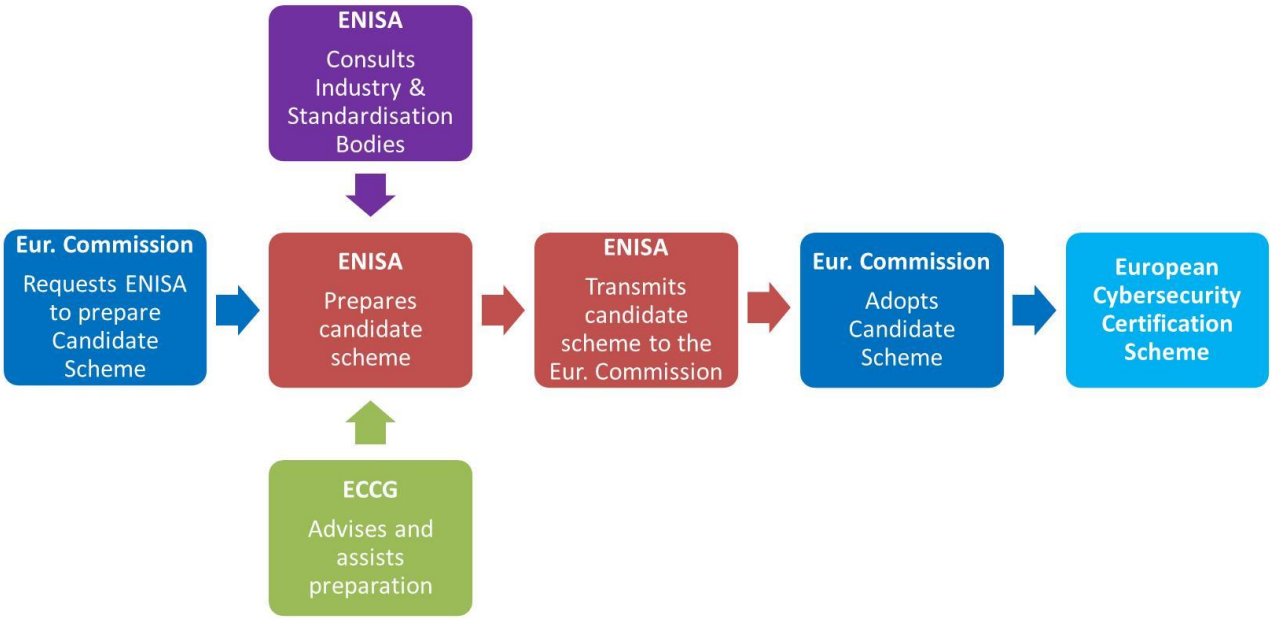


Figure 1: ENISA Certification Scheme

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

The European Smart Grid Task Force defines Smart Grids as electricity networks that can cost efficiently integrate the behaviour and actions of all users connected to it — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety. A Smart Grid employs innovative products and services together with intelligent monitoring, control, communication, and self-healing technologies [3].

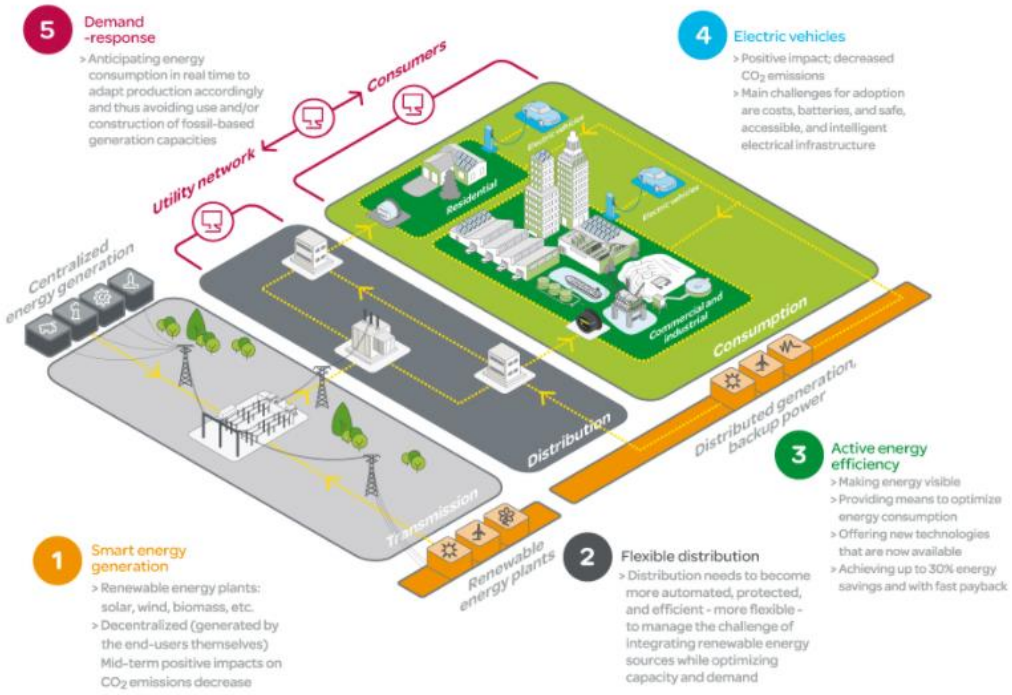


Figure 2: Smart Grid components and infrastructure

As it was mentioned in D6.1 [8], the electricity networks are considered as critical infrastructures by the European Programme for Critical Infrastructure Protection (EPCIP) [4]. In addition, the IACS are evolving to more open and accessible systems with increasing use of commercial-off-the-shelf (COTS) and information technology (IT) solutions. However, this evolution produces that the IACS are more vulnerable to suffer from cyber-attacks. The standard IEC-62443 “Industrial Automation and Control Systems Security”, developed by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) addresses the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS) [7].

Chapter 4 Summary of the outcomes from certification/evaluation process

The standardization and certification according to IEC 62443-4-1 and IEC 62443-4-2 has been considered as very practicable and reasonable for Schneider Electric and particularly for the RTU development cycle.

Further the IEC 62443 terminology, concepts and models embody up-to-date IT security and secure product development lifecycle requirements that conveniently comply with the state-of-the-art development of RTU.

4.1 IEC 62443-4-1

DEKRA Testing and Certification (formerly E&E) has been working on the evaluation of the development procedures used for the RTU devices of the Smart Grid pilot. In this case, the procedure was the Offer Creation process (OCP). The documentation generated by the enforcement of this procedure, database and tools used, training for human resources, roles defined, and other relevant information was checked in the IEC 62443-4-1 evaluation process.

The security product development lifecycle requirements are listed in Table 1. Requirements for evaluation were determined according to standard IEC 62443-4-1 [2]. The Maturity level chosen for the RTU was 2.

Practice	ID	Requirement
Security management (SM): This practice regards to ensure that the security activities are well planned, documented and executed through out product's life-cycle. The interested part shall demonstrate that it is able to support appropriate security measures overall development phases.	SM-1	Development process
	SM-2	Identification of responsibilities
	SM-3	Identification of applicability
	SM-4	Security expertise
	SM-5	Process scooping
	SM-6	File integrity
	SM-7	Development environment security
	SM-8	Controls for private keys
	SM-9	Security requirements for externally provided components
	SM-10	Custom developed components from third-party suppliers
	SM-11	Assessing and addressing security-related issues
	SM-12	Process verification
	SM-13	Continuous improvement
Specification of security requirements	SR-1	Product security context

(SR): Regarding to this practice, the interested part shall probe that each of the software, hardware or firmware is delivered along with a document where all security requirements capabilities are well defined.	SR-2	Threat model
	SR-3	Product security requirements
	SR-4	Product security RQs content
	SR-5	Security requirements review
Secure by design (SD): This set of requirements regards to demonstrate that the device, which is being evaluated, is secure in all stages of the design. That means, the manufacturer must probe that they had apply security measures along all development stages.	SD-1	Secure design principles
	SD-2	Defence-in-depth design
	SD-3	Security design review
	SD-4	Security design best practices
Secure implementation (SI): The manufacturer must probe secure implementations, such as static analysis tools usage or vulnerabilities analysis, when he develops products (software, hardware or firmware). As evaluator organism, we must verify this requirement by requesting such analysis results to the interested manufacturer on getting the certificate.	SI-1	Security implementation review
	SI-2	Secure coding standards
Security verification and validation testing (SV): The manufacturer shall document security testing performed once software/hardware/firmware is full developed. Such testing requirements shall demonstrate the security of the product besides it is secure during all life cycle. The manufacturer must show which security testing accomplished as well as which scenarios consider when such tests are performed. According to the regulation, four types of security testing are addressed: security requirements testing, threat mitigation testing, general vulnerabilities testing and penetration testing.	SVV-1	Security requirements testing
	SVV-2	Threat mitigation testing
	SVV-3	Vulnerability testing
	SVV-4	Penetration testing
	SVV-5	Independence of testers
Security defect management (DM): The manufacturer shall provide evidences of the generated documents about security tests performed, inter alia, which provides to the consumers.	DM-1	Receiving notifications of security-related issues
	DM-2	Reviewing security-related issues
	DM-3	Assessing security-related issues
	DM-4	Addressing security-related issues
	DM-5	Disclosing security-related issues
	DM-6	Periodic review of security defect management practice
Security update management (PM): The manufacturer shall provide evidences about its updates provisioning, as well as how such updates are tested before consumers delivery. In addition, manufacturer shall show the used mechanism to delivery such updates.	PM-1	Security update qualification
	PM-2	Security update documentation
	PM-3	Dependent component or operating system security update documentation
	PM-4	Security update delivery

	PM-5	Timely delivery of security patches
Security guidelines (SG): The manufacturer must provide evidences about provided documents that describes how to integrate, configure and maintain the defense in depth strategy of the product.	SG-1	Product defense in depth
	SG-2	Defense in depth measures expected in the environment
	SG-3	Security hardening guidelines
	SG-4	Secure disposal guidelines
	SG-5	Secure operation guidelines
	SG-6	Account management guidelines
	SG-7	Documentation review

Table 1: IEC 62443-4-1 requirements selected for the evaluation.

During the evaluation, some gaps were found between the OCP procedure and the requirements of IEC 62443-4-1. It makes the procedure being not sufficient to fulfil the requirements established in the standard for maturity level 2, and therefore, no certification process was carried out after the evaluation. Instead, DEKRA Testing and Certification created a report including a complete analysis in which all the gaps are identified and explained. The report was submitted to Schneider Electric for their internal comprehension and use in order to improve their internal development processes for being able to adapt them to IEC-62443-4-1 standard.

The information contained in the evaluation (gap analysis) report is confidential and therefore it is not put in this deliverable.

The front page and index is included in the report (Figure 3 and Figure 4):

Figure 3: Front page of IEC 62443-4-1 report

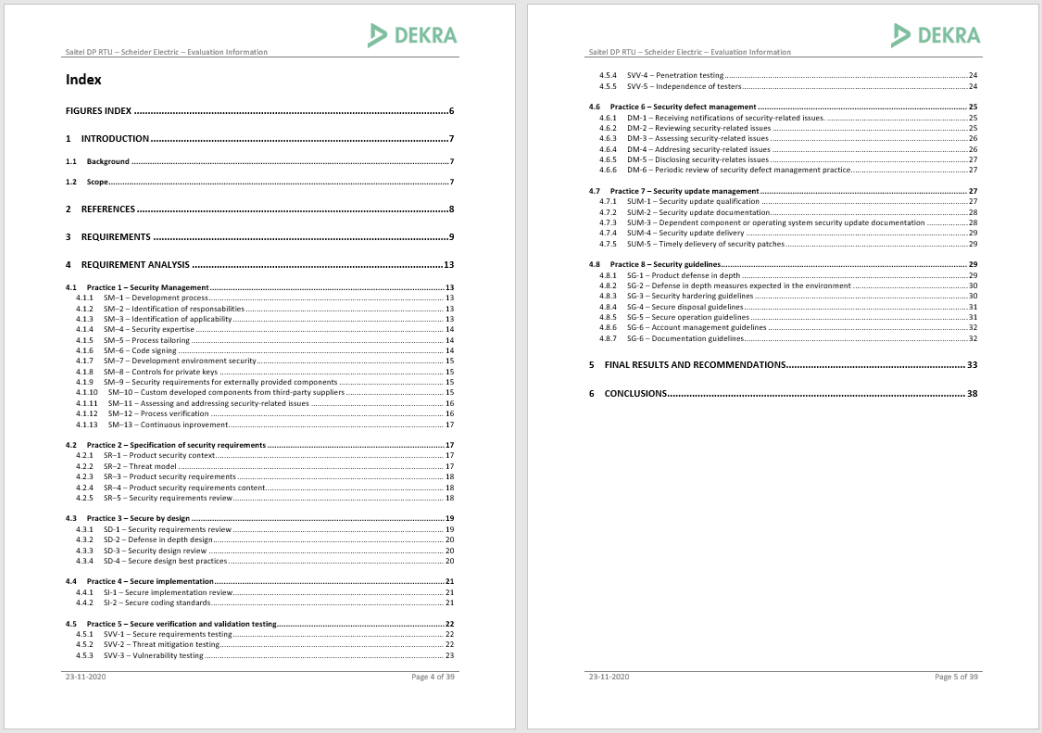


Figure 4: Contents of IEC 62443-4-1 report

4.2 IEC 62443-4-2

DEKRA Testing and Certification (formerly E&E) has been working on the evaluation of the security requirements for IACS components. The RTU is one of these IACS components. It is an embedded device with a Linux operating system and several communication interfaces. The target for the high assurance pilot is the Security Level 3. The IEC 62443-4-2 [7] requirements considered for the evaluation are shown in the following table. The evaluation includes the medium-assurance and the high-assurance pilots.

Foundational Requirements	ID	Requirement
Identification and authentication control (FR1): The evaluator must test the provided roles and users. The aim of this 'practice' is to verify that users who belong to roles have enough privileges to accomplish those tasks for which they have been created, and no further. In addition, the evaluator must test how the evaluated devices identify and authenticate the users who log on the device. The evaluator must prove that the identification and authorization are done properly.	CR1.1	Human user identification and authentication
	CR1.2	Software process and device identification and authentication
	CR1.3	Account management
	CR1.4	Identifier management
	CR1.5	Authenticator management
	CR1.7	Strength of password-based authentication
	CR1.8	Public key infrastructure certificates
	CR1.9	Strength of public key authentication
	CR1.10	Authenticator feedback
	CR1.11	Unsuccessful login attempts
	CR1.12	System use notification
	CR1.14	Strength of symmetric key-based authentication
Use control (FR2): The evaluator must prove that no user is able to accomplish those tasks, which he shouldn't. The goal	CR2.1	Authorization enforcement
	CR2.5	Session lock
	CR2.6	Remote session termination

of this 'practice' is to protect against unauthorized actions on the component resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions.	CR2.7	Concurrent session control
	CR2.8	Auditable events
	CR2.9	Audit storage capacity
	CR2.10	Response to audit processing failures
	CR2.11	Timestamps
	CR2.12	Non-repudiation
	CR2.13	Use of physical diagnostic and test interfaces
System integrity (FR3): The evaluator must test whether the device checks the integrity of the device communication. The device takes measures to detect whether installed software is legit as well as similar tests to physical assets.	CR3.1	Communication integrity
	CR3.2	Protection from malicious code
	CR3.3	Security functionality verification
	CR3.4	Software and information integrity
	CR3.5	Input validation
	CR3.6	Deterministic output
	CR3.7	Error handling
	CR3.8	Session integrity
	CR3.9	Protection of audit information
	CR3.10	Support for updates
	CR3.11	Physical tamper resistance and detection
	CR3.12	Provisioning product supplier roots of trust
	CR3.13	Provisioning asset owner roots of trust
	CR3.14	Integrity of the boot process
Data confidentiality (FR4): This 'practice' goal is to prove that no information is disclosed when data is transmitted as well as the information stored into the device is not accessible by a user without authorization.	CR4.1	Information confidentiality
	CR4.2	Information persistence
	CR4.3	Use of cryptography
Restricted data flow (FR5): The evaluator must test the device ability to configure which 'route' will follow the information from itself to other destination.	CR5.1	Network segmentation
Timely response to events (FR6): This 'practice' goal is to prove how the evaluated device informs about its generated events, how it protects them against manipulation and whether they are stored in a secure way. The evaluator supposes a set of situations in order to research how the devices behaves.	CR6.1	Audit log accessibility
	CR6.2	Continuous monitoring
Resource availability (FR7): The evaluator must test several DoS attacks against the evaluated device such as resources exhaustion, network DoS as well as known vulnerabilities which outcomes in DoS attacks. The goal of this test is to observe the improvements when a high assurance device is embedded in an infrastructure.	CR7.1	Denial of service protection
	CR7.2	Resource management
	CR7.3	Control system backup
	CR7.4	Control system recovery and reconstitution
	CR7.6	Network and security configuration settings
	CR7.7	Least functionality
	CR7.8	Control system component inventory
Embedded device requirements: specific requirements for embedded devices	EDR2.13	Use of physical diagnostic and test interfaces
	EDR3.2	Protection from malicious code

EDR3.10	Support for updates
EDR3.11	Physical tamper resistance and detection
EDR3.12	Provisioning product supplier roots of trust
EDR3.13	Provisioning asset owner roots of trust
EDR3.14	Integrity of the boot process

Table 2: IEC 62443-4-2 requirements selected for the evaluation.

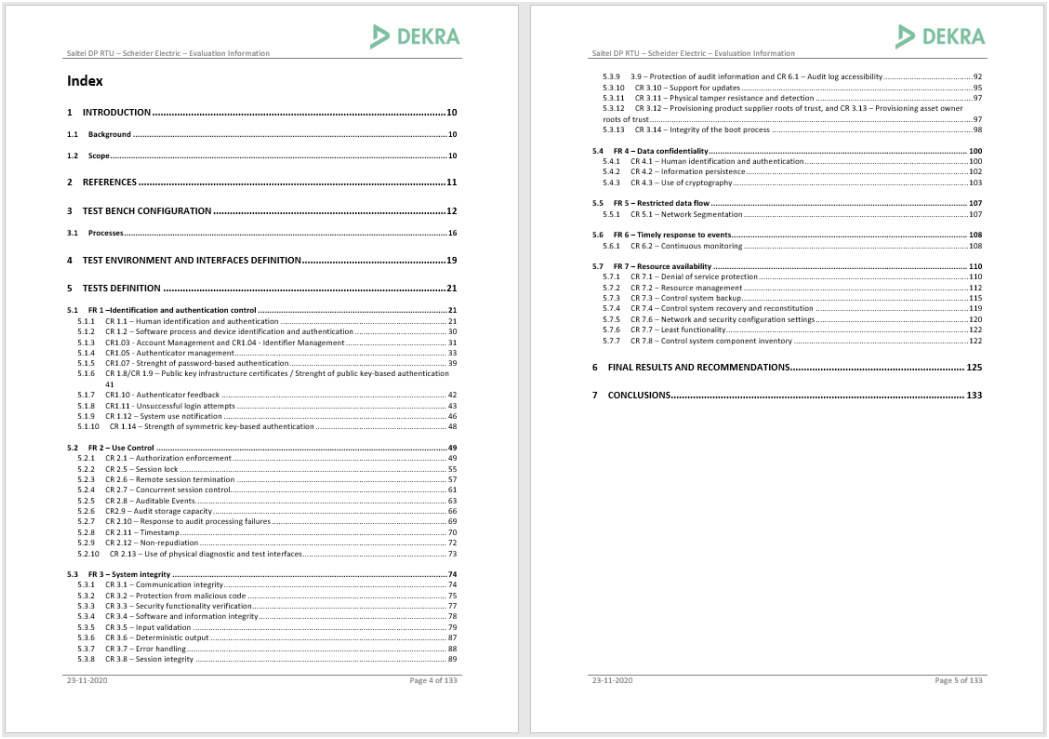
During the evaluation, some gaps were found between the RTU operation and the security requirements of IEC 62443-4-2. It makes the RTU implementation being not sufficient to fulfil the requirements established in the standard for Security Level 3, and therefore, no certification process was carried out after the evaluation. Instead, DEKRA Testing and Certification created a report including a complete analysis in which all the gaps are identified and explained. The report was submitted to Schneider Electric for their internal comprehension and use in order to update the product according to IEC-62443-4-1 standard.

In addition, during this phase, DEKRA Testing and Certification devised and executed a Penetration Test plan and report which was also provided to Schneider Electric.

The information contained in the evaluation (gap analysis) report and penetration testing report is confidential and therefore it is not put in this deliverable.

The front page and content of the IEC 62443-4-2 gap analysis is the following (Figure 5 and Figure 6):

Figure 5: Front page of IEC 62443-4-2 report



DEKRA

Saitel DP RTU – Scheider Electric – Evaluation Information

Index

23-11-2020 Page 4 of 133

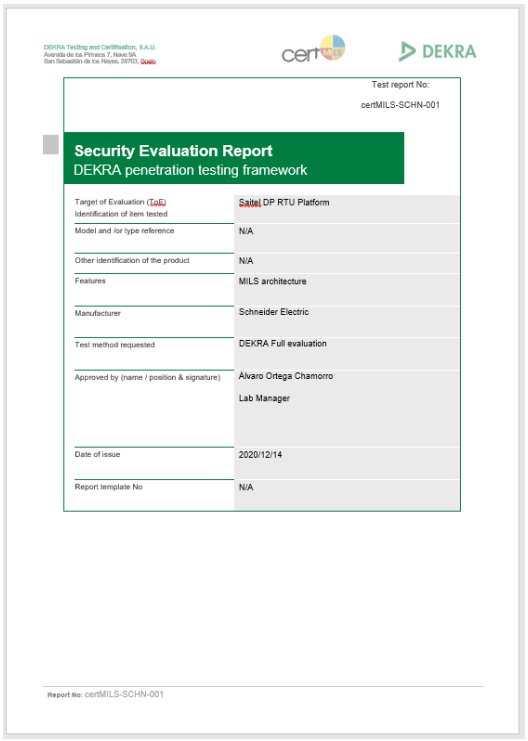
DEKRA

Saitel DP RTU – Scheider Electric – Evaluation Information

23-11-2020 Page 5 of 133

Figure 6: Contents of IEC 62443-4-2 report

The front page of the Penetration test plan and report is the following (Figure 7: the index is not shown due to confidential restrictions):



DEKRA Testing and Certification, S.A.U.
Avenida de los Pirineos 7, Nave 9A
San Sebastián de los Reyes, 28703, Spain

DEKRA

Test report No:
certMILS-SCHN-001

Security Evaluation Report
DEKRA penetration testing framework

Target of Evaluation (ToE) Identification of item tested	Saitel DP RTU Platform
Model and /or type reference	N/A
Other identification of the product	N/A
Features	MILS architecture
Manufacturer	Schneider Electric
Test method requested	DEKRA Full evaluation
Approved by (name / position & signature)	Álvaro Ortega Chamorro Lab Manager
Date of issue	2020/12/14
Report template No	N/A

Report No: certMILS-SCHN-001

Figure 7: Front page of Pentest report

Chapter 5 Lessons learned

Both parties involved in the evaluation (Schneider Electric and DEKRA) gained a very valuable knowledge in the field of IEC 62443 standard, certification structure and specific requirements. The following lessons were learned by each party:

On the side of the applicant for the evaluation/certification (Schneider Electric):

(1) The evaluation process based on the standard IEC 62443-4-1 & IEC 62443-4-2 offered SCHN a complete vision of the cybersecurity status of the RTU, addressing not only the product by also the development process.
(2) Thanks to this evaluation that includes the penetration testing, some vulnerabilities were detected providing a very useful information to SCHN in order to improve the protection of the RTU.
(3) The integration of MILS platform in the RTU device of the Smart Grid pilot contributed to increase the assurance of the pilot thanks to the separation kernel that provides additional protection against cyber-attacks.
(4) It was demonstrated that MILS platform helps us to comply with the IEC 62443- 4-2 requirements.
(5) The evaluation process allowed SCHN to identify the gaps respect to the fulfilment of the standard requirements and this information will be used for future RTU devices in order to enhance the cybersecurity of the IACS.

On the side of the evaluation laboratory (DEKRA Testing and Certification):

IEC 62443-4-1

(1) IEC 62443-4-1 need a high level of expertise in terms of life-cycle models in order to be able to evaluate how a specific development process fulfils the requirements.
(2) The evaluation team involved in the IEC 62443-4-1 analysis gained a lot of experience in Smart Grid development processes, as they needed to completely interpret and understand the OCP procedure provided by Schneider Electric.
(3) In terms of effort calculation, DEKRA Testing and Certification is now in a good position for being able to determine how a potential IEC 62443-4-1 evaluation/certification is in terms of process and effort calculation. DEKRA Testing and Certification had no previous experience with this standard.
(4) The coordination between applicant/vendor (Scheider Electric) and the laboratory (DEKRA) is a crucial aspect as a lot of clarifications and support to the evaluation team is needed in order to be able to clearly obtain accurate evaluation results.
(5) Even when the certification process has not been completed, an initial communication with an IECEE Accredited Certification Body (DEKRA Certification D.V. - Netherlands) which solved a lot of questions regarding the potential certification process.

IEC 62443-4-2

(1) IEC 62443-4-2 is mostly focused on a functional security verification of component behaviour and architecture.

(2) The familiarisation needed for conducting the evaluation needs a lot of effort in the side of the evaluation team, as they need to be able to perform deep testing over the component provided by the applicant/vendor.
(3) The evaluation team gained a lot of experience and knowledge in the architecture, development and functionality of RTU devices for the two different architectures: medium-assurance and high assurance (using PikeOS).
(4) The coordination between the technical teams of both sides (Schneider Electric and DEKRA) is very important as the component may work unexpectedly after some tests, for which further support is needed.
(5) The evaluation team gained a very valuable experience in interpreting the IEC 62443-4-2 functional requirements and was able to devise proper test plans. DEKRA Testing and Certification had no experience in this standard and now is in a good position for being able to calculate efforts and conduct evaluations in this field.

Chapter 6 Summary and Conclusion

D6.4 is the final deliverable and puts closure on the overall very effective and comprehensive work done in the Work Package 6. The report on validated security certification methodology with Smart Grid 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**).

The evaluation process brings a valuable experience for both parties involved, Schneider Electric and DEKRA, as they gained knowledge on how to, first, interpret the compositional methodology defined in D1.3, and later, apply it to a real process and component.

There are multiple advantages in applying this methodology to Smart Grid infrastructures in particular and to IACSs in general, as it is scalable and effective in terms of time consumption. From the experience gained, we can conclude that the balance between security and evaluation efforts is acceptable.

The integration of the methodology defined in D1.3 and the existing emerging certification schemes is affordable, but nowadays modifications due to Cybersecurity Act and EUCC need to be deeply analysed for rephrasing D1.3 accordingly if needed.

IEC 62443 provides a comprehensive framework in which vendors, laboratories and certification bodies can effectively improve the security of IACS systems using certification, in a way in which all of them obtain benefits.

Chapter 7 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
CB	Certification Body
EoLI	End of Life Instructions
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IECEE	IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components
MILS	Multiple Independent Levels of Security
OCP	Offer Creation process
RTU	Remote Terminal Unit

Chapter 8 Bibliography

[1] 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

[2] IEC 62443. (2018). Security for industrial automation and control systems. International Electrotechnical Commission / International Society of Automation. IEC and ISA.

[3] European Commission, “Definition, expected services, functionalities and benefits of the smart grids” [SEC/2011/463]. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1409145728890&uri=CELEX:52011SC0463

[4] European Commission, "Protection of critical infrastructure". [Online]. Available: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[5] ENISA, “Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors”. [Online]. Available: https://www.enisa.europa.eu/publications/maturity-levels

[6] SANS Technology Institute, “Securing Industrial Control Systems-2017”. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

[7] IEC 62443-4-2 “Security for Industrial Automation and Control Systems – Technical Security Requirements for IACS Components”. [Online]. Available: http://isa99.isa.org/Public/Series/Documents/ISA-62443-4-2-Public.pdf

[8] D6.1 Report: Compositional Design of the Smart Grid Pilot. certMILS, Horizon 2020, no 731456.

[9] D1.3 Report: Compositional security certification methodology. certMILS, Horizon 2020, no 731456.