The IACS Cybersecurity Certification Framework (ICCF)

Lessons from the 2017 study of the state of the art

P. THERON,

A. LAZARI,

April 2018

Joint Research Centre

EUR 29237 EN

IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art

This publication is a technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

How to cite this report:
Theron, P. and Lazari, A., The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art., EUR 29237 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-85968-7, doi:10.2760/856808, JRC111611

All images © European Union 2018.

Contents

Abstract

The principal goal of this report is to present the experiments of the industrial automation and control systems (IACS) component Cybersecurity Certification Framework (ICCF) performed in 2017 by the national exercise teams (NETs) of several Member States, namely France, Poland and Spain. Based on real-life cases of use and simulations of ICCF activities, this report documents the current practices of these countries and NET members' views in relation to IACS products' cybersecurity certification. These studies have led to a series of findings that will be useful for the future of the ICCF in the context of the European Cybersecurity Certification Framework. In conclusion, a plan of action is proposed for the 2018-2019 period.

1 Executive summary

The ERNCIP IACS Cybersecurity Certification Thematic Group has worked towards fostering IACS cybersecurity certification in Europe. To that end, the thematic group has elaborated the IACS component Cybersecurity Certification Framework (ICCF). The ICCF has inspired the European Cybersecurity Certification Framework (ECCF).

The ICCF:

- proposes **four IACS cybersecurity certification schemes** (ICCS):
    - ICCS-C1 (self-declaration of compliance);
    - ICCS-C2 (independent compliance assessment);
    - ICCS-B (product cyber resilience certification);
    - ICCS-A (full cyber resilience certification);
- … that involve up to three **evaluation activities**:
    - compliance assessment (in all four ICCS);
    - cyber resilience testing (ICCS-B and A);
    - development process evaluation (ICCS-A).
- … that require the guidelines and resources of **three pillars**:
    - IACS Common Cybersecurity Assessment Requirements (ICCAR);
    - IACS Components Cybersecurity Protection Profiles (ICCPRO);
    - The IACS Cybersecurity Certification Process (ICCP).
- … and involves a **fourth pillar** for fostering and disseminating the ICCF:
    - the IACS Cybersecurity Certification EU Register (ICCEUR).

First, the present report documents existing practices in several EU Member States in relation to the ICCF's evaluation activities and pillars.

Next, the findings from those studies are presented. They are expected to help to improve the ICCF and foster its use in the context of the ECCF.

Finally, the report draws, from the previous elements, a plan of action that could be implemented in the 2018-2019 period in order to turn the ICCF into a fully usable scheme in the context of the ECCF.

Feedback and inquiries should be communicated to:

Joint Research Centre

ERNCIP Office

jrc-erncip-office@ec.europa.eu

---

2 Introduction

2.1   The history and work of the ERNCIP IACS Thematic Group

In 2013, partner directorates-general of the European Commission and the Joint Research Centre (JRC) mandated the ERNCIP IACS Thematic Group to undertake a preliminary feasibility study of an IACS cybersecurity certification framework.

The ERNCIP IACS thematic group has gone through three successive phases.

- 2014 aimed at taking stock of the context, needs and requirements and outlining the principles of a European IACS cybersecurity certification framework.
- 2015 was an intermediate time of reflection, communication with stakeholders and planning.
- 2016 saw the second phase of our thematic group, with a goal to deliver practical recommendations to the industrial systems community at large. This second phase delivered the IACS components Cybersecurity Certification Framework (ICCF).
- 2017 marked the third phase of the ERNCIP IACS Thematic Group. During this phase, several Member States took part in an experiment aimed at documenting the current practices in relation to IACS cybersecurity certification.

In 2017, each participating Member State created a national exercise team (NET) that involved:

- its national cybersecurity agency;
- an IACS vendor;
- a certification authority;
- a cybersecurity evaluation laboratory (often called information technology security evaluation facility (ITSEF);
- possibly industry representatives, academics or experts.

Six NETs were expected to take part in the ICCF phase 3 work plan.
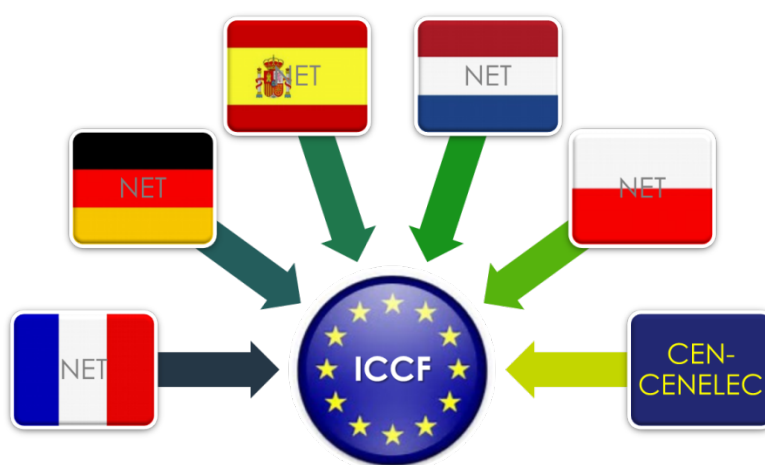
Figure 1: Planned ICCF phase 3 NETs

- Germany, Spain, France, the Netherlands and Poland, and the CEN-Cenelec Cyber Security Coordination Group (CSCG).

However, only France, Poland and Spain could complete the exercise assigned to their NETs.

Each NET was due to explore the ICCF activities through the following choice of exercises:

- E1 — elaboration of a protection profile (PP) and a security profile and reporting on the easiness/difficulty of this activity;
- E2 — simulation of a product compliance assessment, and reporting on the easiness/difficulty of this activity;
- E3 — simulation of testing a product's cyber resilience, and reporting on the easiness/difficulty of this activity;
- E4 — simulation of the evaluation of a product's development process, and reporting on the easiness/difficulty of this activity;
- E5 — abandoned, not defined;
- E6 — study of ICCF governance bodies and processes.

NET	CSCG	France	Germany	Netherlands	Poland	Spain
INITIALLY PLANNED EXERCISES	E6	E1 + E2 + E3 (based on French CSPN[1] scheme)	E1 + E3	E3	E1 + E3	E1 + E2 + E3 (based on French CSPN scheme)
USE CASE **Vendor product**	ICCF governance bodies and processes	Stormshield SNi40 industrial firewall	Industrial firewall (not specified)	Compumatica Secure Networks BV MagiCtwin Diode for industrial environments	Mikronika RTU (v1 and v2) Polon — Alfa CIE (control indication equipment) for fire detection and alarm	Siemens SIMATIC RTU3030C remote terminal unit (RTU)

NB: Only French, Polish and Spanish NETs' results are taken into account in this report.

2.2 Methodology of the exercises

Each NET had to perform the following tasks:

- Select a use case (NB: the Polish NET relied on three use cases), i.e. an IACS component that would serve as the material basis of the exercise.
- Establish its composition under the direction of the country's national cybersecurity agency (where it existed); each NET had to also include representatives of a national certification

---

[1] CSPN is the acronym of "Certification de Sécurité de Premier Niveau".

authority, an evaluation laboratory or ITSEF and the vendor of the chosen IACS product, and possibly further members such as experts, academics or user industries.

- Set up a protocol for simulating the tasks during table-top exercise sessions. In effect, it was impossible to actually perform the activities prescribed in the ICCF in the time and resource frame of the exercises.
- Schedule and run the simulation sessions.
- Document the process, its inputs, process and results.

Work started early 2017, and NETs had to be finished by the end of November 2017.

Finally, the NETs gathered for a plenary meeting of the ERNCIP IACS Thematic Group in January 2018 to draw collective lessons from their exercises.

2.3   Contents of the report

The present report documents the exercises performed by the French, Polish and Spanish NETs, their findings and a proposal for a plan of action for the next phase of development of the ICCF in the context of the European Cybersecurity Certification Framework pursued by DG Communications Networks, Content and Technology.

2.4   The ICCF and support to the European Commission's roadmap towards European cybersecurity certification

In a proposal for a regulation (^{2}) of 13 September 2017 the European Commission published the potential directions for the governance and implementation of a European cybersecurity certification framework for products and services. The proposal highlights all of the requirements for the future establishment of certification schemes within the context of the framework. The ERNCIP Thematic Group on IACS, through its work on the feasibility study for the IACS Cybersecurity Certification Framework (ICCF), has contributed to the formulation of some articles of the published version of the regulation, since a part of the study regarding the assurance levels of the European cybersecurity certification schemes was incorporated into the final text of the proposal (Article 46).

Furthermore, since the proposal has been published, it is worthwhile to perform a quick compliance analysis to verify to what extent the ICCF's feasibility study is already in line with the 'certification package', therefore making the ICCF a potential candidate certification scheme according to the Article 44 of the proposal.

The analysis took into account the following articles of the published text of the regulation, because of their relevance for the compliance analysis:

- Article 45：Security objectives of European cybersecurity certification schemes;
- Article 46: Assurance levels of European cybersecurity certification schemes;
- Article 47: Elements of European cybersecurity certification schemes.

(^{2})   Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') COM(2017) 477 final, Brussels, 13.9.2017 — 2017/0225 (COD).

The text of Article 45 sets out the following security objectives for future cybersecurity certification schemes:

'(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;

(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration;

(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

(d) record which data, functions or services have been communicated, at what times and by whom;

(e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom;

(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

(g) ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities and are provided mechanisms for secure software updates.'

The aforementioned cybersecurity objectives are at the core of the ICCF's formulation since the aim of the feasibility study on the cybersecurity certification of IACS components is to assure that certified devices will have specific features and mechanisms in place so as to cover those objectives.

The text of Article 46 sets out the following assurance levels for future cybersecurity certification schemes:

'(a) assurance level basic shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents;

(b) assurance level substantial shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity incidents;

(c) assurance level high shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with

the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity incidents.'

Article 46 of the proposal is the one where most of the work performed by the ERNCIP Thematic Group has been incorporated with adjustments, since the regulation has to cover many more products than the one deployed in industrial environments. Such a condition implies that the formulation of the ICCF's assurance levels matches the ones of the proposal as shown by the following figure and table.

ICCS-A
- Accredited Third-party Full Certification
- Certification required for most critical environments

ICCS-B
- Accredited Third-party Product Certification
- Certification required for critical infrastructures

ICCS-C2
- Compliance Assessment by accredited third-party
- Enhanced C&C for common, non critical products

ICCS-C1
- Vendor's Self-declaration of Compliance
- Easy access C&C for common, non critical products

Figure 2: The ICCF's assurance levels (originally named 'schemes')

These schemes would lead to the delivery of self-declarations of compliance, labels and certificates as illustrated below.

ICCF / ICCS-C1 Self Declaration of compliance — The vendor hereby declares that they positively assessed this product against the IACS Common Cybersecurity Assessment Requirements selected in a Security Profile that can be consulted online on the IACS C&C EU Register.	European Commission proposal's basic assurance level

ICCF Industrial Automation & Control System Cybersecurity Compliance & Certification Framework **ICCS-C2 3rd-Party Compliance Assessment Label**	European Commission proposal's basic assurance level
ICCF Industrial Automation & Control System Cybersecurity Compliance & Certification Framework **ICCS-B Product Cyber Resilience Certificate**	European Commission proposal's substantial/high assurance level
ICCF Industrial Automation & Control System Cybersecurity Compliance & Certification Framework **ICCS-A Full Cyber Resilience Certificate**	European Commission proposal's high assurance level

Table 1: Assurance levels in the ICCF vs those in the proposal

Article 47, regarding the 'elements of European cybersecurity certification schemes', contains a list of features that a scheme should have in order to be formally established as per the proposal. The following table contains an assessment of the maturity of the ICCF vs the requirements set out in the proposal.

Elements of cybersecurity certification schemes	ICCF features in line with the proposal and maturity assessment
(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered	Yes. See report of phase 2 ([3]). More work to be performed in 2018/2019 to finalise the class of products included in the scheme as described in Chapters 5, 6 and 7 of this report.
(b) detailed specification of the cybersecurity requirements against which the specific ICT	Yes. See report of phase 2. Evaluation standards have been reviewed and identified for the

---

[3] Available at: https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC102550_introduction-to-iccf_erncip-iacs-tg-onlineversion.pdf

products and services are evaluated, for example by reference to Union or international standards or technical specifications	purpose of the scheme. More work to be performed in 2018/2019 as described in Chapters 5, 6 and 7 of this report.
(c) where applicable, one or more assurance levels	Yes. Four levels of assurance proposed.
(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved	Yes. More work to be performed in 2018/2019 as described in Chapters 5, 6 and 7 of this report.
(e) information to be supplied to the conformity assessment bodies by an applicant which is necessary for certification	Yes. More work to be performed in 2018/2019 as described in Chapters 5, 6 and 7 of this report.
(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used	Yes. Self-declaration of compliance, label and certificates are proposed and their usage is explained. More work to be performed in 2018/2019 as described in Chapters 5, 6 and 7 of this report.
(g) where surveillance is part of the scheme, the rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements	Yes. Two factors should allow monitoring of the compliance with the scheme. The first factor relies on two requirements to be enforced in the evaluation phase: (1) the skills of the personnel handling the evaluation at the conformity assessment body; and (2) the common evaluation methodologies to be followed by all of the accredited conformity assessment bodies throughout the Union. Both of these factors should be further discussed in phase 4 of the ICCF together with a post-certification monitoring procedure such as a peer-review of technical evaluation reports.
(h) conditions for granting, maintaining, continuing, extending and reducing the scope of certification	More work to be performed in 2018/2019, as described in Chapters 5, 6 and 7 of this report, more specifically on maintenance of already issued certificates (e.g. in case of a software update to a certified device).
(i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements	Not addressed. To be explored in phase 4 of the ICCF.
(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with	Not addressed. To be explored in phase 4 of the ICCF in conjunction with procedures and requirements as per the Network and Information Security directive (EU) 2016/1148.
(k) rules concerning the retention of records by conformity assessment bodies	Yes. In the phase 2 report, the online portal should help keeping track of the certified devices, their technical specification at the moment of the evaluation and the certificates issued.
(l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services	Yes. See Chapter 4 of this report. More comparative work to be potentially performed in the next phase (2018-2019) of the ICCF.
(m) the content of the issued certificate	Not yet addressed. More work to be potentially

	performed in phase 4 of the ICCF on this matter.

Table 2: Analysis of the ICCF against the proposal's criteria

2.5 Contributions

In alphabetical order, the members of the NETs were as follows.

French NET

- Thomas GALLIANO and Romain MUGUET, ANSSI - Agence nationale de la sécurité des systèmes d'information, national cybersecurity agency and certification body
- Thierry MIDY, Stormshield (vendor)
- Robert WAKIM, Stormshield (vendor)
- Olivier MARY, Oppida (ITSEC, evaluation laboratory)
- Vincent DIEMUNSCH, RTE France (stakeholder)

Polish NET

- Janusz Górski, Gdansk University of Technology (NET-PL leader)
- Piotr Chojnicki, Telbud, system integrator
- Paweł Florek, Kacper Karpiński, CNBOP-PIB, certification body
- Michał Karolak, EY EMEIA Advisory Centre, security compliance testing
- Izabela Lewandowska-Wiśniewska, PZU LAB, insurance company
- Krzysztof Politowski, Ministerstwo Cyfryzacji, Department of Digitalisation, government
- Mariusz Sowiński, Polon-Alfa, vendor
- Tomasz Szała, Mikronika, vendor
- Andrzej Wardziński, Gdańsk University of Technology/Argevide, academia and tools support

(*) which also plans to become a conformity assessment body.

Spanish NET

- Centro Criptológico Nacional (CCN), national cybersecurity agency and certification body
- Miguel Garcia-Menendez, CCI, industrial organisation
- José Ruiz Gualda, Applus+, evaluation laboratory
- José Alejandro Rivas, Applus+, evaluation laboratory
- Sergio Gonzalez de Castro, Applus+, evaluation laboratory
- Hector Puyosa, UPCT, industry user
- Ignacio Alvarez Vargas, Siemens, vendor
- José Luis Donoro Ayuso, Siemens, vendor

JRC — European Commission

- Alessandro Lazari, JRC, Ispra
- Georgios Giannopoulos, JRC, Ispra
- Igor Nai Fovino, JRC, Ispra
- Gianmarco Baldini, JRC, Ispra

3 List of abbreviations

The following acronyms and terms are used in this report.

ANSSI = Agence Nationale de Sécurité des Systèmes d'Information (France)	
CA = critical asset	
CRT = communication robustness testing	
ECCF = European Cybersecurity certification Framework	
IACS = industrial automation and control systems	
ICCAR = IACS common cybersecurity assessment requirements	
ICCEUR = IACS Cybersecurity Certification EU Register	
ICCF = IACS component Cybersecurity Certification Framework	
ICCP = IACS Cybersecurity Certification Process	
ICCS = IACS Cybersecurity Certification Scheme	
ICCS-A = IACS Cybersecurity Certification Scheme A (full cyber resilience certification)	
ICCS-B = IACS Cybersecurity Certification Scheme B (product cyber resilience certification)	
ICCS-C2 = IACS Cybersecurity Certification Scheme C1 (independent compliance assessment)	
ICCS-C1 = IACS Cybersecurity Certification Scheme C2 (vendor's self-declaration of compliance)	
ICPRO = IACS Components Cybersecurity Protection Profiles	
ICS = industrial control system	
IGB = ICCF Governance Board	
JRC = European Commission Joint Research Centre (located in Ispra, Italy)	
NET = national exercise team	
PLC = programmable logic controller	
PP = protection profile	
RTU = remote terminal units	
SCADA = supervisory control and data acquisition	
SDSA = software development security assessment	
SP = security profile	
TER = Technology Evaluation Report	
ToE = target of evaluation	
VPN = virtual private network	

4 NETs' undertakings and analysis

4.1 French NET

4.1.1 Tests performed by the NET

The French NET simulated the highlighted ICCF activities.

E1	Elaboration of a protection profile and a security profile and reporting on the easiness/difficulty of this activity.
E2	Simulation of a product compliance assessment, and reporting on the easiness/difficulty of this activity.
E3	Simulation of testing a product's cyber resilience and reporting on the easiness/difficulty of this activity.
E4	Simulation of the evaluation of a product's development process and reporting on the easiness/difficulty of this activity.

4.1.2 Documents delivered by the French NET

The French NET worked on drafting a protection profile, a security profile (called 'security target' in the NET's document as the NET referred to the Common Criteria — ISO 15408 — standard) and a test plan for a given product.

The NET also reflected on and documented the method required to draft these documents, and specifically to address the difficulties professionals could encounter in the course of these activities. The NET's report documents the steps of the corresponding tasks and provides examples.

The French NET's report includes the following documents, all presented in the annex:

- **French NET report**: this document presents the overall process of the exercise: composition of the NET, methodology, methodology of the elaboration of the protection profile, methodology of the elaboration of the security profile, evaluation of the product and conclusions;
- **test plan report**: this document details the compliance assessment methodology (called conformity in the document) and contains a cyber resilience tests report (called resistance in the document);
- **protection profile of an industrial firewall**: this document presents how to describe the product and its usage, the associated critical assets, the threat model, the security objectives and how these elements may relate to one another;
- **Stormshield Network Security, Industrial Firewall SNi40 — CSPN Security Target**: this document gives details of how, for a specific product, its description and associated critical assets and threat model are described. NB: it instantiates the protection profile mentioned above.

4.1.3 Analysis of French practices

Reading these documents helps one to understand current French practices. The following analysis can be made.

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
Reference to a standard/scheme	The French CSPN scheme, derived from Common Criteria. The CSPN methodology was created by ANSSI in 2008, and consists in 'black box' or 'grey box' testing under constrained time. The CSPN is an alternative to Common Criteria evaluation, for which the cost and the duration can be an obstacle, and when the degree of confidence aimed at is lower.	Freedom of choice of a standard is the rule in the ICCF. The choice of a particular standard induces differences in vocabulary, such as security target (Common Criteria) vs security profile (ICCF). • *These differences should be specifically mentioned in the documentation of evaluations.*
Overall process	Protection profile => security profile => evaluation plan => compliance assessment + cyber resilience tests. Process documented by Figure 3. The relation between evaluation and certification is detailed in Figure 7.	Corresponds to ICCS-B.
Protection profile	In the CSPN, it includes: • product description; • critical assets ([4]); • threat model; • security objectives; • mappings.	The CSPN's threat model does not quite match the ICCF PP model ([5]). Threats, expressed in terms of attack methods, are not related to the protection assumptions present in the product description, hence making it hard to formally express residual threats [6]. Protection assumptions should, as per the ICCF, help to explain how gross threats are mitigated by the assumed protections within or around the product. In the CSPN document, apart from the (data) model provided in Section 5.3, Methodology, this contribution of assumed protections is not explained. • *The CSPN could be more explicit.* Critical assets (CA) in the CSPN are

---

[4]   A critical asset is the conjunction of a part and a security characteristic assigned to that part.
NB 1: A critical asset is an assertion of the security of a product's part.
NB 2: Within a product or family of products, there are as many critical assets as there are combinations of parts and security characteristics.
Each critical asset faces threats that may undermine the security characteristics of a critical asset.
NB: Threats are identified through a risk analysis.
For each critical asset, the author of the protection profile (PP) formulates zero to several Protection Assumptions resulting from typical / generic Operating Conditions and that indicate how a threat against a critical asset is assumed to be reduced under those operating conditions.
(Definitions provided in the ICCF phase 2 report).
[5]   See ICCF phase 2 report for details of the data model of PPs.
[6]   See ICCF phase 2 report's section on PPs.

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
		defined in terms of both environmental CAs and the product's CAs: • *The rationale of this choice is to be analysed in order to decide if it should be included in the ICCF.* In the CSPN, mappings (assets vs threats and threats vs security objectives) are expressed in the shape of two tables in the annex. The meaning of these tables and the consequences to draw from them are not explicit. • *The CSPN could make these elements more explicit.* The CSPN's security objectives seem to be equivalent to the ICCF PP's 'rationale' of the relation between critical assets, residual threats and the security functions that should be fitted into the product or its environment to reduce residual threats. Besides, CSPN PPs do not include recommended security functions as prescribed in ICCF. • *It is necessary to study this point and determine if the CSPN should clarify these two points.* In the CSPN, the definition of a PP should be validated by the national cybersecurity agency, which is also, in France, the certification authority. • *ICCF processes should specify clear rules about who should elaborate, review and approve PPs.*
Security profile (SP)	In the CSPN, it includes: • product identification; • product description; • critical assets; • threat model; • security functions; • mapping.	In the CSPN, product identification means designating precisely the product, its version and category. However, the 'Stormshield Network Security, Industrial Firewall SNi40 — CSPN Security Target' (SP) document is not structured as indicated in the 'French NET Report' document and these data are indicated on the cover sheet of the SP document. The version is also detailed in Section 1, Product description of the 'Stormshield

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
		Network Security, Industrial Firewall SNi40 — CSPN Security Target' document.
		• *All evaluation documents should comply with common, standardised structuring rules.*
		• *The ICCF should specify these document structure rules.*
		In the ICCF, and except for the product's 'parts', the description of the product was not an aspect that was specified finely.
		• *The ICCF should specify what a product's description should include.*
		Besides, in the ICCF, 'parts' are to help specifying critical assets, whereas in the CSPN the link between parts and critical assets is fairly vague:
		• *The ICCF should specify more finely how evaluation schemes should implement its data model to make documents more formally comparable.*
		• *In general, the 'ergonomics' of ICCF documents is an issue to study as the readability of documents is a prerequisite for a shared understanding and mutual recognition.*
		The object of the evaluation, the 'evaluated platform' in the CSPN SP document, includes a Windows 7 console beside the Stormshield product itself; it also includes the specification of the product's detailed configuration.
		• *The ICCF should require that the target of evaluation (ToE) be defined in a standard way. This includes specifying the elements composing and interacting with the ToE.*
		• *The ICCF should also indicate the level of precision/detail of the specification of the ToE's perimeter and configuration.*
		• *These data are of utmost importance as they specify the*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
		scope of the evaluation and of the certificate. The relation between security functions, ToE's critical assets and residual threats is not explicit in the CSPN SP document. And security mechanisms implementing the security functions are not specified here. Note added by the French NET during the review of this report: *However, this information is not always detailed in the ST for confidential matter. It is shared with the ITSEF though, through technical documentation the developer has. This is especially true for the cryptographic specifications, for example. They are detailed in another document that is not publicly released.* • *The recommendations made for PPs above apply to SPs. The ICCF must specify what data must be present in evaluation documents and the format of those data.* • *Whether security mechanisms should be specified in the SP or not needs to be studied. If current practices do not recommend it, the goal of mutual recognition of certificates may induce it.*
Cybersecurity requirements	Cybersecurity requirements are not clearly expressed in the documentation. There is also no reference to a standard's set of such requirements. Note added by the French NET during the review of this report: *The CSPN does not have this. It would be impossible to have a document listing the standards a product should implement, given the wide variety of products we have. And furthermore, it is up to*	The ICCF specifies that PPs and SPs should make a clear reference to a set of cybersecurity requirements extracted from the chosen standard. These requirements are not explicitly documented, even in the 'conformity' section of the 'test plan report' document. • *CSPN PPs and SPs should list explicitly those requirements to make the evaluation more formal and its process less variable. References to the standard's requirement*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	the developer to select the technology he or she wants to use, and up to the evaluator to test if it is robust or not. The only requirements we have concern cryptography and the RGS (Règlement Général de Sécurité) listing the algorithms that are not to be used. We also have a document that concerns the TLS (Transport Layer Security) cipher suites that are not to be used either. But it is not mandatory to respect this specific document.	*numbers should be explicit for the sake of traceability.*
Evaluation goals, plan and process	The CSPN 'test plan report' document uses standard data containers to document the assessments to perform. Those cartridges include: product reference, assessment objectives ([7]), prerequisites, tools to use for the assessment, method (called 'proceedings' in the French document) of the assessment and expected result.	The ICCF has not yet specified these aspects. • *In order to foster mutual recognition, the ICCF should indicate the ad hoc method and format of the data used to specify assessments.* The CSPN raises some questions about the definition of the objective(s) of an assessment item (one only or several), the contents of prerequisites (operators, test platforms, other related elements), the method (should a protocol, or standardised protocol, be referred to?), tools (is it enough to mention a category of tools or should each tool be specified finely?) and expected results (how to express them, should a tolerance be indicated?, should the conditions in which results are expected be specified?, etc.). • *Further studies are needed to answer these questions.* Note added by the French NET during the review of this report: *One has to keep in mind that after reading the technical evaluation report, the certification body (ANSSI) challenges the ITSEF during*

([7]) Whether multiple objectives should be pursued in a single assessment is debatable. It might be better that one assessment pursues one objective only. However, the workload for specifying assessments so finely might exceed reasonable limits of cost and time while one of the goals of the CSPN is to run evaluations in a limited frame of time and cost.

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
		a face-to-face meeting with the evaluators. ANSSI experts are also invited to attend this meeting.
Compliance assessment	The CSPN documents do not depict the process of compliance assessments.	The ICCF has issued in the phase 2 report very generic recommendations about the process of all evaluation activities. • *Further studies are needed here as well to refine the definition of the ICCF in order to foster mutual recognition and dialogue between the actors of the evaluation and certification process.* • *A standard can solve this issue.*
Cyber resilience tests	Idem	*Idem*
Development process evaluation	Not studied by the French NET.	NA
Evaluation report	Not provided by the NET.	NA

4.1.4 Overall process of the CSPN methodology.
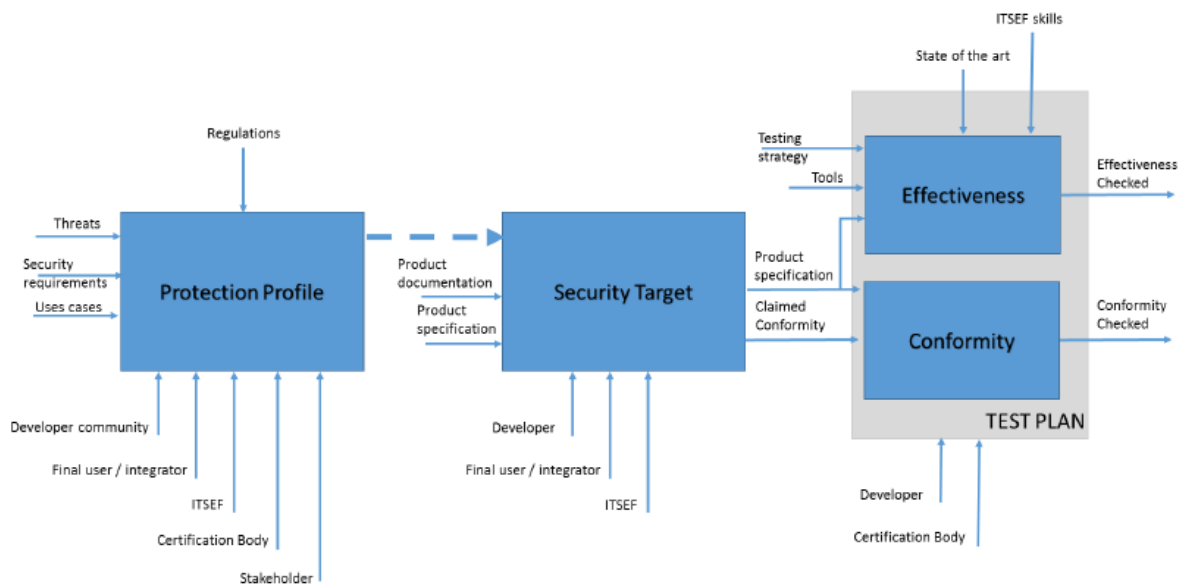
Figure 3: Overall process of the CSPN method for ICCS-B

4.1.5 Model of a protection profile
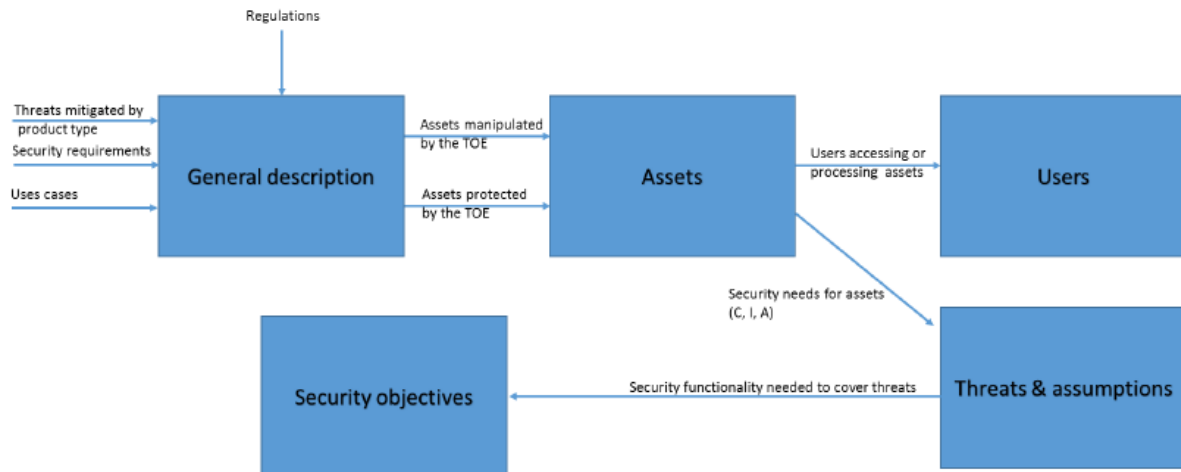
Figure 4: Model of a protection profile

4.1.6 Table of contents of a CSPN protection profile
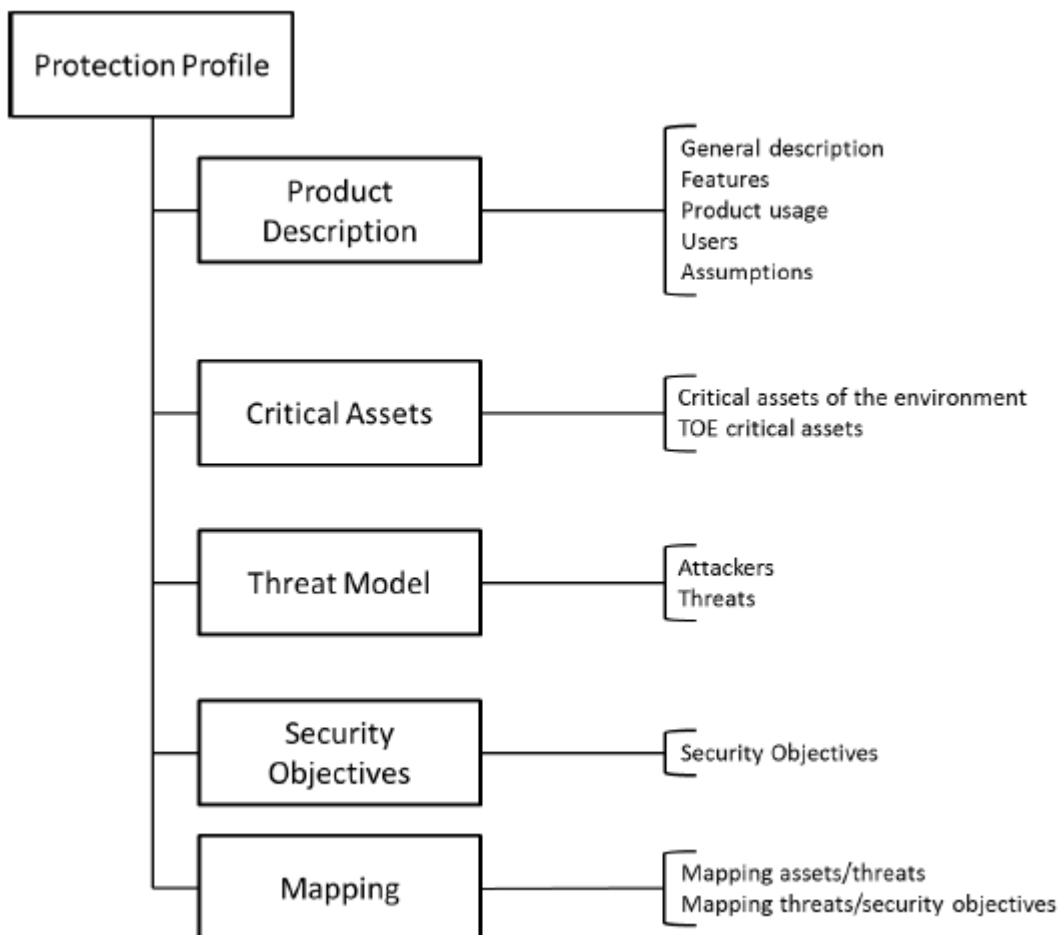
Figure 5: Table of contents of a CSPN protection profile

4.1.7 Table of contents of a CSPN security profile (named security target)
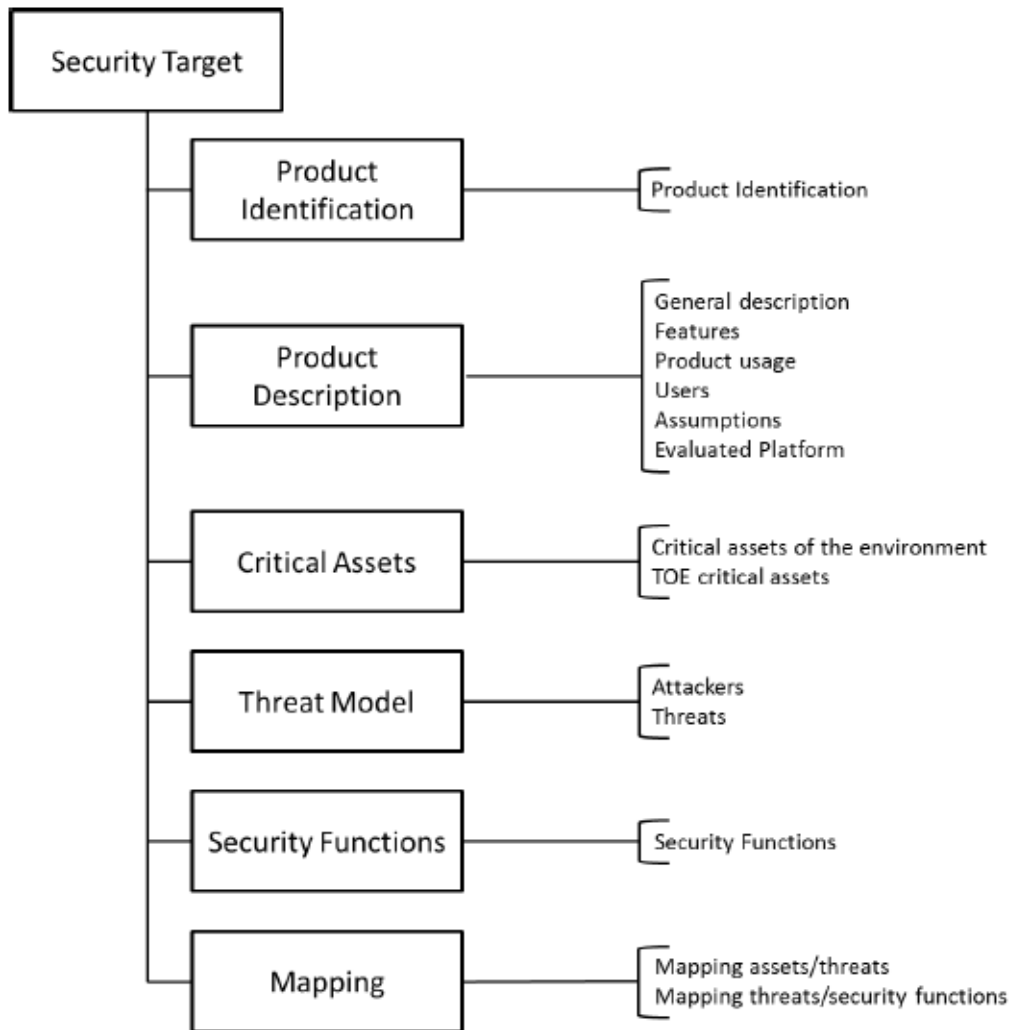
Figure 6: Table of contents of a CSPN security profile

4.1.8 Relation between the evaluation process and the certification process
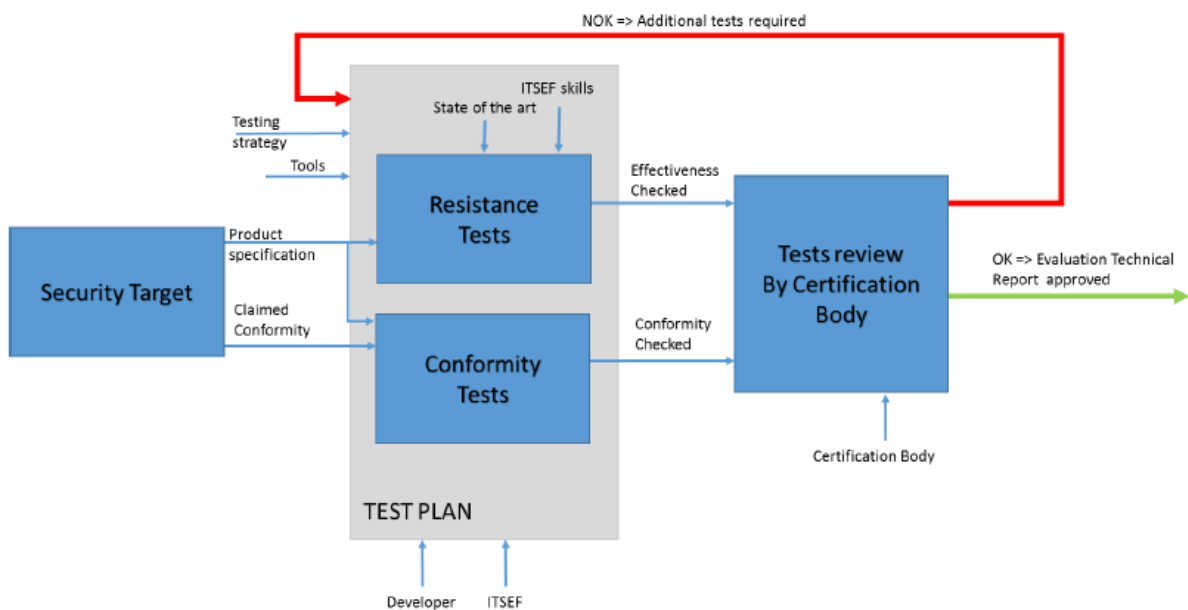
Figure 7: Relation between evaluation and certification processes

4.2 Polish NET

4.2.1 Tests performed by the NET

The Polish NET simulated the ICCF activities highlighted in green (E1) and brainstormed on those highlighted in grey (E2 to E4).

E1	Elaboration of a protection profile and a security profile and reporting on the easiness/difficulty of this activity.
E2	Simulation of a product compliance assessment and reporting on the easiness/difficulty of this activity.
E3	Simulation of testing a product's cyber resilience and reporting on the easiness/difficulty of this activity.
E4	Simulation of the evaluation of a product's development process and reporting on the easiness/difficulty of this activity.

4.2.2 Documents delivered by the Polish NET

The Polish NET drafted three protection profiles related to two classes of IACS components — the remote telecontrol unit (RTU) ([8]) and control and indication equipment (CIE) — for test E1.

Through a questionnaire sent to Polish NET's participants, a brainstorming exercise was conducted for the evaluation activities that were to be simulated in tests E2, E3 and E4.

The NET's report documents firstly the way in which protection profiles are written today and secondly the opinions of NET-PL's members about the activities corresponding to tests E1, E2, E3 and E4.

The report includes the following documents, all presented in the annex:
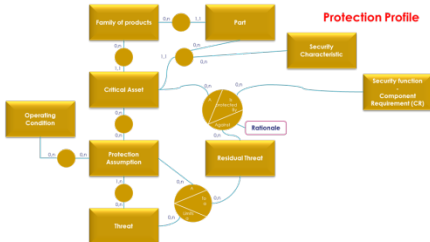
- Report on the results of experiments carried out by the Polish National Exercise Team (NET-PL) during phase 3 of ICCF;
- Appendix 1 of the final report by NET-PL 'Protection profile of a remote terminal unit (RTU), Version 1.0, Mikronika (NET-PL)';
- Appendix 2 of the final report by NET-PL 'Protection profile of fire detection and fire alarm systems (FDAS) — Control and indication equipment (CIE) in distributed architecture, Version 1.0, Polon-Alfa (NET-PL)';
- Appendix 3 of the final report by NET-PL 'Protection profile of a remote terminal unit (RTU), Version 2.1, NET-PL: Mikronika, GUT'.

The first document presents NET-PL's methodology and the conclusions of its work. The other three documents present the contents of protection profiles.

> NB: It is important to state that NET-PL followed the guidelines of ANSSI of France's CSPN methodology to elaborate protection profiles.

([8]) The RTU's protection profile had two versions: Version 1.0 and Version 2.1. If the report states that the version 2.1 PP followed the recommendations of IEC 62443-4-2, the difference between the two documents is minimal.

The following table summarises the analysis of the NET's documents.

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
Reference to a standard/scheme	NET-PL referred to France's CSPN and IEC624430 (concerning the PP contents — see Section 4.2.3).	Freedom of choice of a standard is the rule in the ICCF.
Overall process	Not documented. Note added by the Polish NET during the review of this report: *NET-PL considerations were with reference to the model presently adopted for fire-protection devices and systems certification (see Section 4.2.4). Corresponds to ICCS-B.*	
Protection profile	It has to be noted that NET-PL highlights the fact that creating a PP from scratch may be a significant effort. For instance, the CIE's PP, elaborated from zero, represents a 1- to 2-person-month effort. Note added by the Polish NET during the review of this report: *The effort reported for the RTU's PP was 2 person-days (for version 1.0) and 2 person-weeks (for version 2.1). It seems that the differences result from the differences in the scope covered by the effort estimates (learning about security, learning about the component class, defining the PP).* NET-PL highlights the need for a cybersecurity protection profile standard; specifying the contents of PPs would be useful. NET-PL recommends that rules be defined in relation to PPs' elaboration, storage, distribution and updates. Note added by the Polish NET during the review of this report: *NET-PL stresses the need for a comprehensive business model underlying the development, maintenance and usage of protection/security profiles that*	Although they make an explicit reference to the same CSPN method, the three PPs do not display the same table of contents. • *The ICCF must specify the table of contents of PPs and, beyond PPs, of all documents involved in the evaluation and certification process.* Besides, the correspondence between the ToE's parts and critical assets on one hand and the security functions on the other hand is not clear enough in the CSPN methodology, at least as applied by NET-PL. Readers may not be clear about how to exploit such PP documents. By reference to the ICCF phase 2 report's Section 4.2.6.2.3.1, Conceptual model of a protection profile, some recommendations can be drawn for the future. • *The contents of PPs should reflect the conceptual structure advocated in this data model. In practice, this translates into the modification/clarification of*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	would be acceptable for all stakeholders.	*CSPN documentation. The mapping tables presented in PPs' annexes should document the 'joint' relations (circles) of the ICCF PP conceptual model. This would help PP authors by guiding them more accurately, and would make all PPs similar in structure for readers.* • *The ICCF's PP and SP data models should be reviewed in order to increase their adequacy for stakeholders' needs. In particular, the current link between security functions and security requirements is not explicated in these data models.*
Security profile	Not addressed by NET-PL	• *A standard should support the implementation of the ICCF.* • *Future work on the ICCF should include an analysis of target workload and delay for elaborating PPs in order to better frame a recommendation of methodology and participants.*
Cybersecurity requirements	In all three annexes, tables list the IEC 62443-4-2 cybersecurity requirements. However: • In the Annex 1 document (RTU PP v1.0), IEC 62443 requirements are simply listed in its Section 7, with a vague link to, and mentioned in the text of security functions. • In the Annex 2 document (RTU PP v2.1), requirements are listed in Sections 6 and 7. In Section 6, the table establishes a broad link between 'threats', 'protected critical assets', 'security functions' and 'foundational requirements'. In Section 7, the table links security functions to IEC 62443-4-2 cybersecurity requirements and indicates that the rationale between these two elements must be provided, giving some	• *Similar recommendations as for PPs above apply here.*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	examples of such a rationale. • In the Annex 3 document (CIE PP v1.0), cybersecurity requirements are presented in Section 7 while security functions are presented in Section 6. Section 6's table links threats to security functions but without a reference to critical assets. Section 7's table links security functions to IEC 62443-4-2 cybersecurity requirements, but without the rationale of these links.	
Evaluation goals, plan and process	Not addressed by NET-PL <u>Note added by the Polish NET during the review of this report:</u> *By analogy to the presently implemented evaluation process for fire-protection systems and components, NET-PL speculated on the structure of the cybersecurity evaluation goals, activities and results.* *As an additional exercise, NET-PL considered that the concept of conformance template derived from the evidence-based argumentation theory could be used to support evaluation criteria, if supported by adequate tools. Such a conformance template has been created for the RTU's PP, version 2.1 and was represented in the NOR-STA tool.*	• *Security profiles (SPs) or complementary documents must specify the evaluation's goals, plan and process(es).* <u>Note added by the Polish NET during the review of this report:</u> • *A clear and comprehensive business model (covering the perspectives of all stakeholders) should support evaluation*
Compliance assessment	Not simulated by NET-PL, but some views about the process and certification criteria are expressed, stemming from the inquiry conducted among Polish NET members.	• *A standard should support the implementation of the ICCF.*
Cyber resilience tests	Idem. NET-PL highlights the need to make rules about the management of changes in products vs the issue of the validity/significance of tests' results. NET-PL's recommendations include	• *A standard should support the implementation of the ICCF. This may include testing requirements, process and tools.*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	testing process and tooling standardisation in favour of mutual recognition of certificates.	
Development process evaluation	Similar outcomes of Polish NET's work. This NET highlights the possibility to resort on existing standards to perform development process assessments.	• *Future work on a standard supporting the ICCF should include possible references to ad hoc other standards.*
Evaluation report	Not addressed by NET-PL.	• *A standard should support the implementation of the ICCF.*

4.2.3   Protection profiles elaborated by NET-PL

While working on PPs, and concerning their structure, NET-PL referred to two sources:

- the model recommended in the ICCF phase 2 report Section 4.2.6.2.3.1 (conceptual model of a PP);
- selected examples of PPs published on ANSSI's web portal (the structure recommended by the CSPN was followed).

With regards to the contents of the PPs that were elaborated, the main problem encountered by NET-PL related to the selection of the relevant security functions to be included.

Without having adequate guidance in this domain, the writer of the PP was left uncertain concerning the completeness and coverage of his decisions.

To cope with this problem NET-PL decided to refer to the IEC 62443 standard and to use its concept of foundational requirement (FR) and the related checklist ([9]).

This resulted in the two different versions of PP of the RTU (Version 1.0 and Version 2.1) elaborated by NET-PL.

The resulting PP structure is presented in the following figure.

([9])   As suggested in the ICCF phase 2 report.
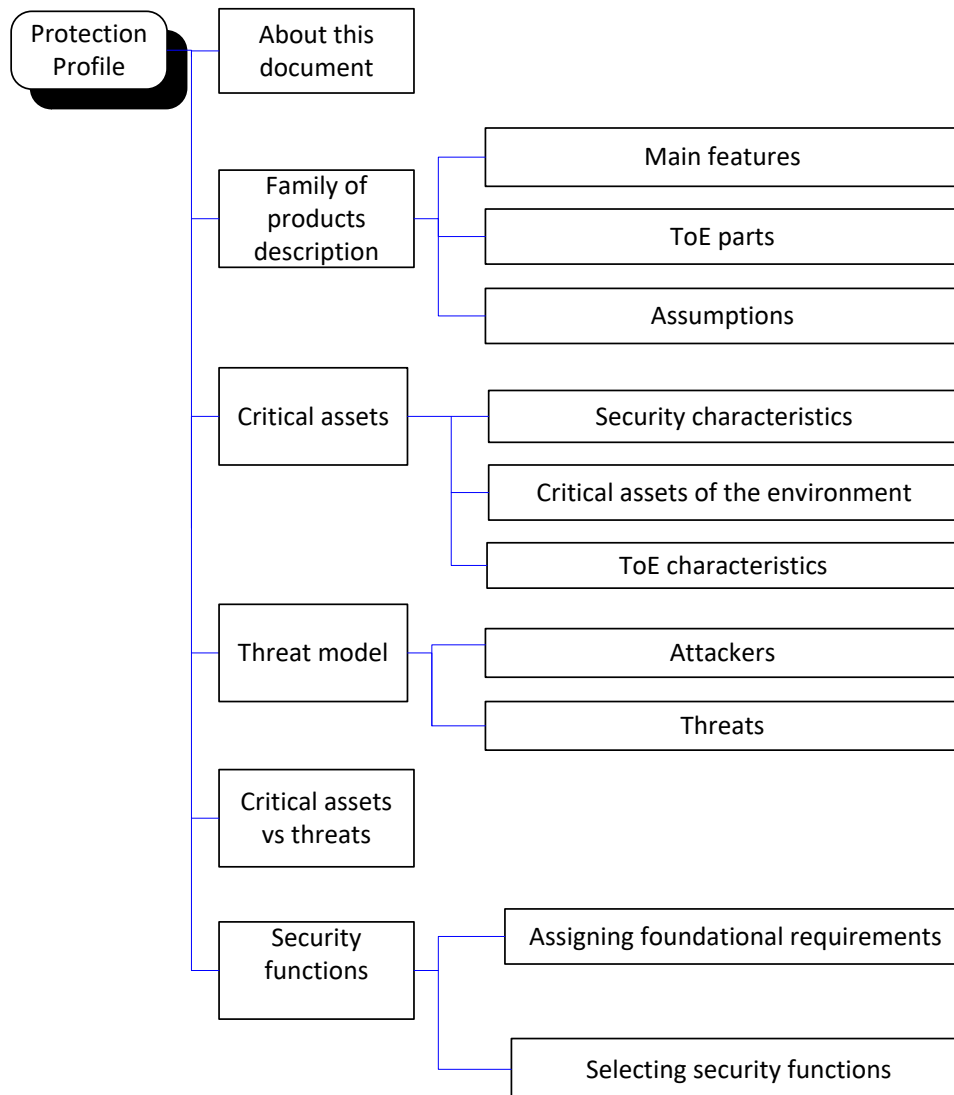
Figure 8: Structure of a protection profile

4.2.4   Certification process model

NET-PL used as a reference the certification process model presently implemented by Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej — Państwowy Instytut Badawczy (CNBOP-PIB) for certification of fire protection devices and systems shown below:
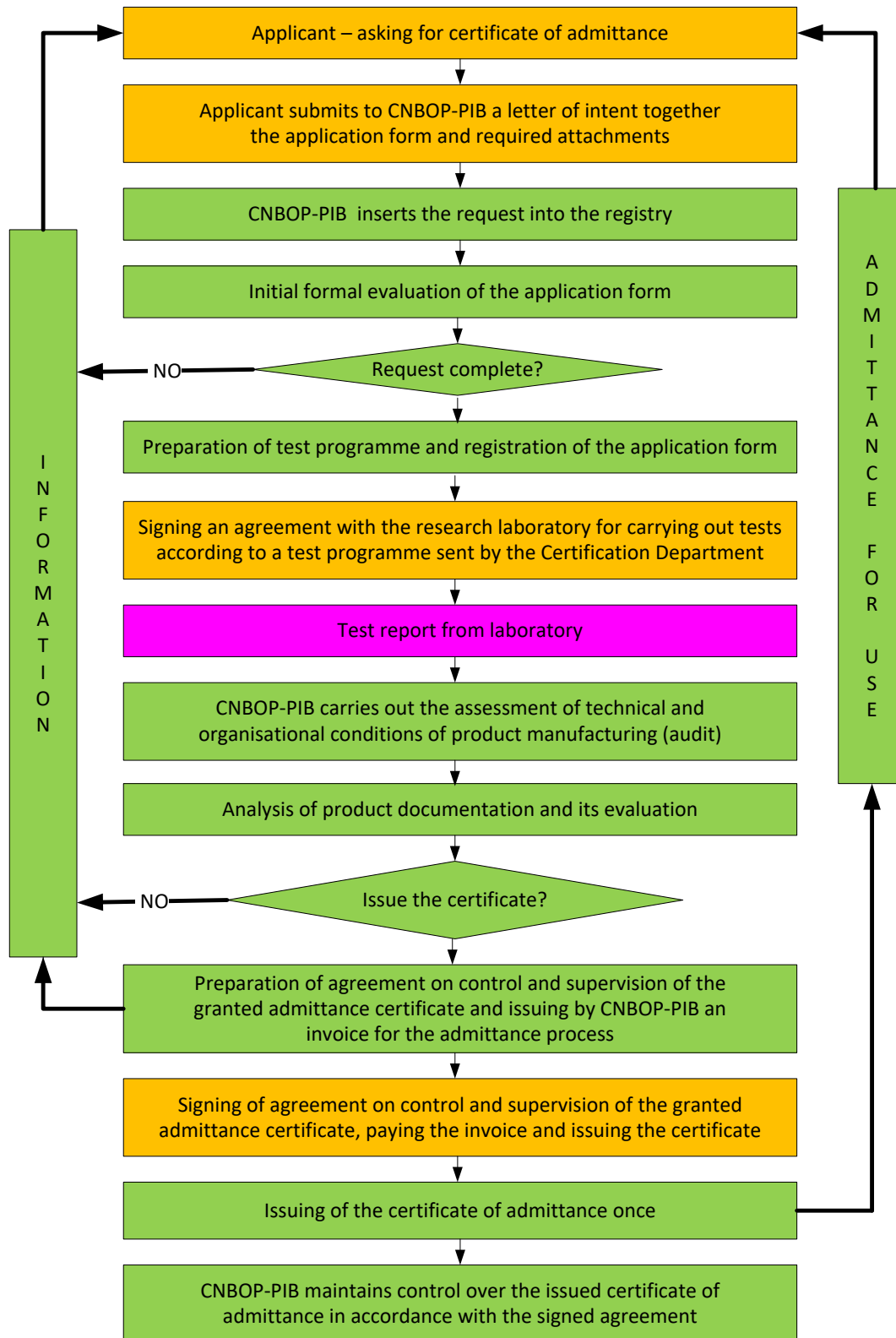
LEGEND

■ Actions by CNBOP-PIB ■ Actions by a client ■ Actions by a specialized lab

Figure 9: Model of the certification process referred to by Polish NET

4.2.5 Further details provided by Polish NET

NET-PL used a web-based documentation tool, NOR-STA, for two purposes:

- to support cooperation and communication within NET-PL;
- to derive from a PP the compliance argumentation template supporting the compliance assessment.

This is documented in the 'Report on the results of experiments carried out by the Polish National Exercise Team (NET-PL) during phase 3 of ICCF' (see Polish NET annex).

4.3 Spanish NET

4.3.1 Tests performed by the NET

The Spanish NET simulated the following highlighted ICCF activities.

E1	Elaboration of a protection profile and a security profile and reporting on the easiness/difficulty of this activity.
E2	Simulation of a product compliance assessment and reporting on the easiness/difficulty of this activity.
E3	Simulation of testing a product's cyber resilience and reporting on the easiness/difficulty of this activity.
E4	Simulation of the evaluation of a product's development process and reporting on the easiness/difficulty of this activity.

4.3.2 Documents delivered by the Spanish NET

The Spanish NET drafted a security profile (test E1) for an RTU (test E1) and simulated the activities concerned by tests E2 and E3.

The NET's report documents the selected IACS product (Siemens' SIMATIC RTU 3030C) and the results of the E1, E2 and E3 tests.

Its report consists in one document: Spanish NET report on E1 to E3 ICCF tests.

This report has the following contents:

- o Exercises 1, 2 and 3 goals, assumptions, principles, methodology and results: this document presents the overall process of the exercise (composition of the NET, methodology of the elaboration of the security profile, methodology of the compliance and cyber resilience evaluation of the product and conclusions for each exercise);
- o Security profile for the SIMATIC RTU3030C — V2.0.20 (Annex A): this document presents the ToE and its usage, the associated critical assets, the corresponding threat model, the security objectives and how these elements may relate to one another
- o ICCF cyber resilience evaluation technical report for the SIMATIC RTU3030C — V2.0.20 (Annex B): this report includes an example of the contents that a cyber resilience evaluation technical report could deliver.

NB: The Spanish NET also followed the guidelines of ANSSI of France's CSPN methodology to elaborate the security profile and to serve as a basis for test E3.

The following table summarises the analysis of the Spanish NET's document (core part and annexes).

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
Reference to a standard/scheme	French CSPN. Note added by the Spanish NET during the review of this report: *In the future, the Spanish NET strongly suggests defining the standard to be followed within the ICCF. This standard could be a new European standard for lightweight/basic security evaluations based on Member States' existing methodologies (e.g. the French CSPN).*	Freedom of choice of a standard is the rule in the ICCF.
Overall process	Not addressed specifically by the Spanish NET. Note added by the Spanish NET during the review of this report: *An evaluation and certification process (PO-005 Product Certification) is already in place in Spain for Common Criteria (https://oc.ccn.cni.es/pdf/po-005_certificacion_en.pdf). This procedure is already applicable for other evaluations methodologies.* Process documented in Figure 10.	• *The ICCF's recommendations published in the phase 2 report must be further detailed.* • *Creating a standard in support of the ICCF would help with specifying the broad processes that should be followed in view of the mutual recognition of certificates despite possible differences in the choice of the standard of reference (see prior point in the table). It should take account of existing evaluation and certification processes in use across EU Member States and fill the gaps that might be found in them.*
Protection profile	Not addressed by the Spanish NET. Note added by the Spanish NET during the review of this report: *Protection profiles should be defined collectively by all concerned industry stakeholders.*	
Security profile	The RTU's SP includes: • the product's commercial name and unique	• *Comments are similar to those made for the French*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF

	references;
	• an overview containing
	   o the product' expected usage
	   o typical users of the product
	   o the product's usage environment;
	• the security problem
	   o assumptions
	   o assets
	   o threats
	   o environment security measures;
	• the product's security functions/ mechanisms.
	It is also named a security target.
	The report states that 'Writing a security profile is a task to be done by the developer.'
	The effort required to establish an SP is deemed 'acceptable'.
		and Polish NETs.

Cybersecurity requirements	These are not clearly detailed in the ICCF security profile. Annex B, Section 4 mentions cybersecurity requirements as part of a form of test specification.
	
	Note added by the Spanish NET during the review of this report:
	Cybersecurity requirements are included in the security profile (section on security functions) for the ToE. Moreover, Section 7.2, Methodology of test E3 provides a draft methodology of the cybersecurity requirements to be met by a ToE.
	
	Response to the above note:
	Following the note above, we looked for the requirements and found the elements (selection only here) presented here:
	• ICCF cyber resilience evaluation technical report for the SIMATIC RTU3030C — V2.0.20 (Annex B), Section 5.3, Security functions
	   o 'The following security objectives are considered:
	      ▪ **Malformed input management**: The ToE has been developed in order to correctly handle malformed input, in particular malformed network traffic.
	      ▪ **Secure storage of secrets**:
		• *Idem*
		• *The Spanish NET's post-review note is very interesting as it points to one of the crucial issues revealed by this year's tests of the ICCF, i.e. the lack of standardisation of the format to be used to document cybersecurity objectives, cybersecurity requirements, cybersecurity functions and all other aspects of security profiles and of the evaluation and certification process.*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	User secrets are securely stored in the ToE. In particular, the compromise of a file is not sufficient for retrieving them.'	
Evaluation goals, plan and process	The specification of these aspects is approached through the various chapters of the report. Annex B, Section 4 mentions some cyber resilience test specifications. Note added by the Spanish NET during the review of this report: *For each exercise (E1 to E3), the goals have been defined. The methodology to be used for each exercise has been specified.*	• *Idem.*
Compliance assessment	The steps of the compliance assessments identified by the Spanish NET are (as in Section 6.2 of the report): 1. verification of the consistency of security functions with the security problem definition; 2. verification of the vendor's documentation and supporting evidence of how security functions and requirements are addressed by the ToE. In conclusion, the NET indicates that: • a standardised, precise evaluation method is needed to ensure the repeatability of assessments; • there is a risk that vendors might not know reference standards and/or CSPN method with consequent difficulties in specifying the cybersecurity requirements appropriate to the product, thus implying increased work for the evaluation laboratory; • compliance assessments are seen as insufficient and functional tests of the product are seen as a necessary complement.	• *The ICCF's recommendations published in the phase 2 report must be further detailed.* • *Creating a standard supporting the implementation of the ICCF is likely to be the best way to work on these aspects.* Suggestion added by the Spanish NET during the review of this report: • *Including functional testing in the compliance assessment should be considered in an update of the ICCF.*
Cyber resilience tests	The CSPN method was adapted (Section 7.2 of the report). The recommended approach is a 'tiered method' starting with tests at the physical level, up to the logical level, up to the environmental level and up to additional system interactions (ASI).	• *The ICCF's recommendations published in the phase 2 report must be further detailed.* • *Creating a standard supporting the implementation of the ICCF is likely to be the*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	Tests should include for each tier: - resistance of security mechanisms; - vulnerability analysis; - penetration tests; - evaluation test report. Conclusions drawn by the Spanish NET are as follows: - The choice of a security reference level (SL-C in IEC 62443-4-2) should be specified as a basis for framing the tests. - The main conclusion obtained through the NET simulation testing exercise is that the evaluation period must have an upper boundary on the testing effort. The proposed time boundary for cyber resilience tests should be set between 20 and 40 days. *The approach to be followed is slightly different to the CSPN [CRITERIA]. Two main phases have been defined: vulnerability analysis and penetration testing. Guidance on how to conduct this methodology has been provided.* (Post-review comment provided by the Spanish NET) - Some form of collaboration between the vendor and the laboratory must be envisaged. This is the case for code analyses that are deemed a sensitive issue for vendors and that could/ should be carried out at the vendor's premises. This may cause difficult logistic and technical problems with regards to the tools required for such purpose. *Another approach could be to have*	*best way to work on these aspects.*

ASPECTS OF THE ICCF	NATIONAL PRACTICES	DISTANCE TO THE ICCF
	source code review as a module/augmentation to the certificate. (Post-review comment provided by the Spanish NET) • After assessments have been finished, the vendor should have a specified time period to resolve the issues, except for 'residual vulnerabilities'.	
Development process evaluation	Not addressed by the NET's exercise.	
Evaluation report	Annex B includes some examples of the contents of a technical evaluation report for the cyber resilience test.	• *A template for the technical evaluation report should be defined as part of the ICCF.*

4.3.3 Further details supplied by the Spanish NET

The following further details have been provided regarding the product certification procedure.
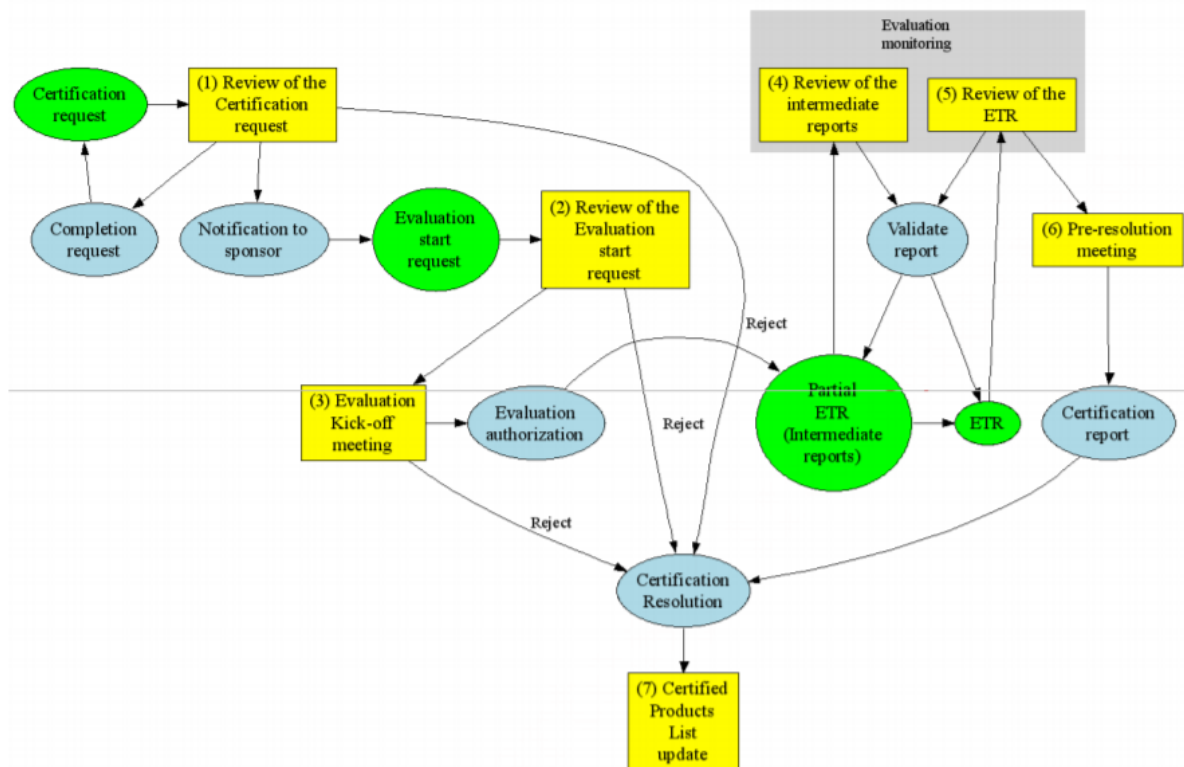
Figure 10: Spanish product certification procedure of reference

5 Synthesis of NETs' outcomes: list of recommendations for phase 4

The analysis of the three reports of the Spanish, French and Polish NETs has highlighted a series of improvements and needs to be addressed in ICCF phase 4.

Domains of improvement	Recommendations	Suggested improvements

Standardisation	Creating a standard supporting the implementation of the ICCF and, beyond, of the European Cybersecurity Certification Framework (ECCF)	Definition of the methodology for ICCS-C1, ICCS-C2, ICCS-B and ICCS-A, including the following elements:
		• Overall evaluation and certification process
		  o Processes
		  o Steps
		  o Tasks
		  o Methods and tools
		  o Participants
		• Documents used for evaluation and certification
		  o Definition of their ergonomic aspect
		  o Structuring rules
		  o Explanation of correspondence with ICCF requirements
		• Protection profile and security profile
		  o Table of contents
		  o Level of detail and format of the description of the ToE, its perimeter and configuration
		  o Inclusion or not of the specification of evaluations goals, plan and process
		  o Format of PP and SP data
		• Compliance assessment
		  o Scope, series and nature of assessments
		• Cyber resilience tests
		  o Tiered approach and associated criteria
		  o Series and nature of tests
		  o Cooperation with vendors and conditions for code assessments
		• Product's development process assessment
		  o Including references to existing standards
		• Evaluation reports
		  o Table of contents

		- Vocabulary correspondences between ICCF and selected standard of reference; - Verification and validation processes. - Guidelines - The set of guidelines providing advice on how to implement the ICCF standards in practice
Economy of the evaluation and certification process	ICCF recommendations	Target (or expected?) workload and delay not to exceed for evaluations and certification
The ICCF's enhancement	Conceptual models (PP, SP)	- PP and SP data models should be reviewed: - Definition of critical assets (CAs) as product operation environment's CAs and product's CAs - Link between residual threats, critical assets, security functions and cybersecurity requirements - Link between security functions and security requirements - Definition and inclusion into the conceptual model of: - the objective(s) of an assessment item (one only or several), - the contents of prerequisites (operators, test platforms, other related elements?), - the method (should a protocol, or standardised protocol be referred to?), - tools (is it enough to mention a category of tools or should each tool be specified finely?), - expected results (how to express them?, should a tolerance be indicated?, should the conditions in which results are expected to be specified?, etc.); - Choice as to whether security mechanisms should be specified in SPs or not, and therefore included in the conceptual model or not - Clarification, improvement and alignment (between ICCF and national schemes) of conceptual/data models

		(of processes, criteria, PP/SP, etc.), in order to assure that similar information be used and produced whatever the standard used as a reference in evaluation / certification activities
Verification and validation	Demonstration of the ICCF performance in a real life context	• Reflection on the success criteria for the ICCF and the related key performance indicators (KPIs) • Planning for experiments to evaluate their values

6 Collective findings of the NETs

Besides the findings from the analysis of each NET's contribution, the meeting in Paris on 9 January 2018 allowed NETs to conclude their work by identifying collectively the following issues.

- Trust in the evaluation process and the cross-recognition of certificates are two main issues that imply:
    - a common methodology and process for evaluation and certification;
    - a common methodology for cyber resilience tests;
    - a reference manual (standard) for the review of the results of the tests;
    - a reference manual (standard) for the peer-review of results of the different ICCF schemes in the EU;
    - a common vocabulary;
    - a process for the maintenance of the scheme and of the certificates already issued;
    - a common process for the maintenance of PPs and SPs.
- A pending question is about the possible impacts of the ECCF on the ICCF (see Table 2);
- Finally, all the participants estimated that the time and budget of an evaluation and of the certification process should be limited in order to make the European cybersecurity certification endeavour realistic (not too costly, not too long).

7 Conclusion: proposed 2018-2019 programme of action

Based upon the elements reported in previous sections, we articulate here the essential elements that could/should organise work in ICCF phase 4.

7.1 Main goals

Goals for ICCF phase 4 works are:

- to produce a usable scheme for IACS;
- to give practical support to the ECCF.

7.2 Further studies are required

To respond to the practical findings from NETs' exercises, the ICCF itself should undergo some improvements listed in Section 5 above.

7.3 Focused projects should be launched

Seven projects should be launched during phase 4:

1. To close identified gaps between practices and ICCF guidelines;
2. To run a pilot project implementing the ICCF requirements ([10]) under an observable protocol;
3. To launch a CEN-Cenelec 'ICCF standard' new work Item;
4. To prepare an experimental laboratory that could be run by the JRC in order to maintain and share the knowledge, requirements, processes and tools associated with the ICCF and its associated standard;
5. To work with ENISA to support the creation of the expertise needed to accomplish the tasks regarding the future European certification framework;
6. To foster the industry's engagement in liaison with industry-representation bodies;
7. To create an exportable ICCF that could promote European high-level standards of security, industrial interests and evaluation and certification know-how.

7.4 NETs and partners to involve in phase 4

At this stage, the JRC should prepare the ICCF phase 4 works by looking for the support of the concerned European Commission directorates-general as well as the support of Member States and industrial and academic partners.

7.5 ICCF phase 4 governance

([10]) It is important to decide, if a real evaluation is to be performed, whether the same product will be the object of all NETs' work or if each NET would work on a product of its own choice. In the first case NETs could all easily exchange information and results could be compared fairly easily. In the second case, and without clear guidelines, it would be less easy to follow a common methodology and to compare results.

The ICCF phase 4 works will become significantly heavier than in previous phases. Multiple projects need to be launched and the governance and coordination of initiatives are key to the success of the overall endeavour.

Without being definitive, the following diagram shows the levels of governance and the variety of stakeholders to involve in ICCF phase 4 works.
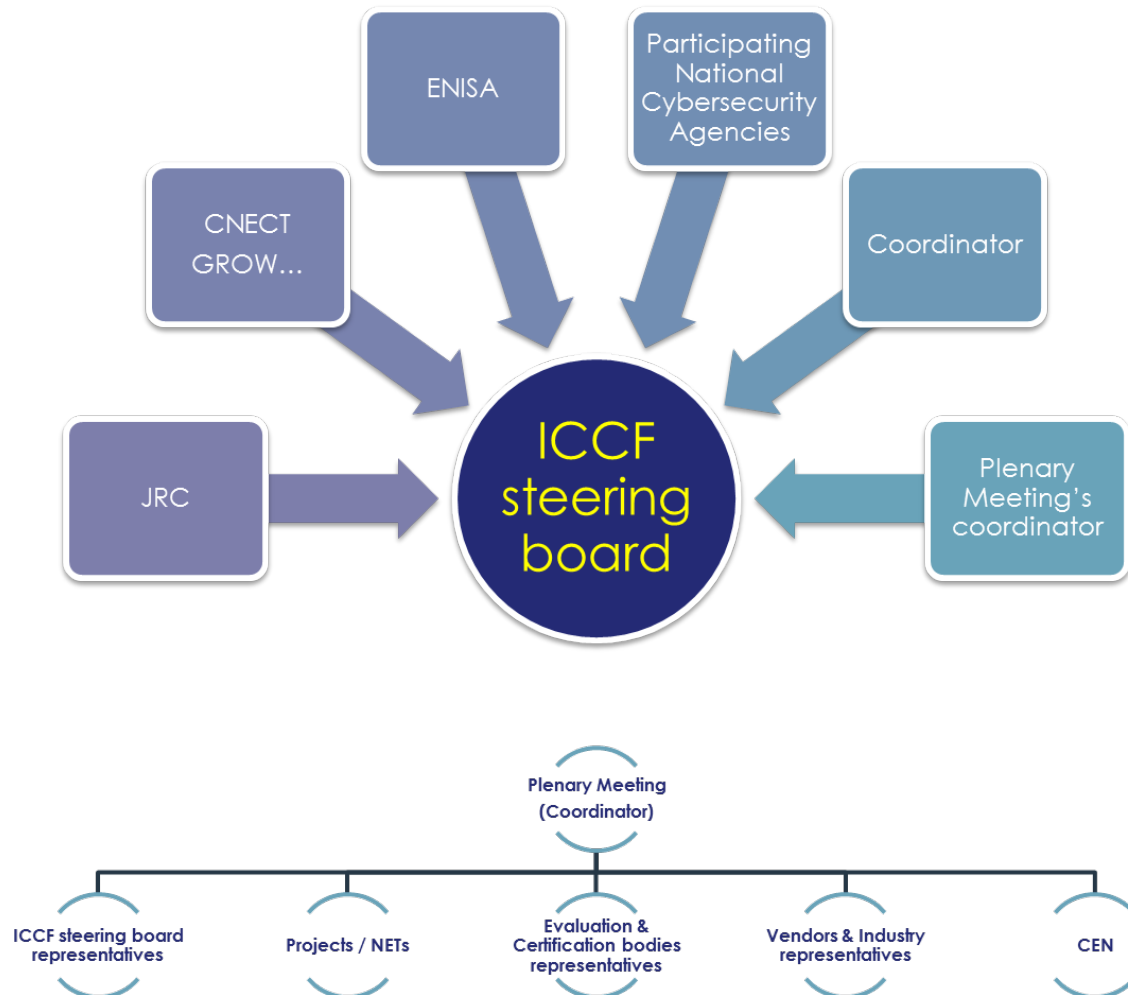
Figure 11: Proposed phase 4 organisation

This two-level governance and project structure will allow the treatment of 'technical' issues and more general issues to be addressed separately, as well as an objective and detached control of projects' orientations, conduct and outcome.

7.6   Setting goals for every stakeholder

Through this organisation, each stakeholder can expect specific gains from the seven projects mentioned in Section 7.3 such as, but not limited to, those mentioned in the green boxes on the right-hand side of the figure below.
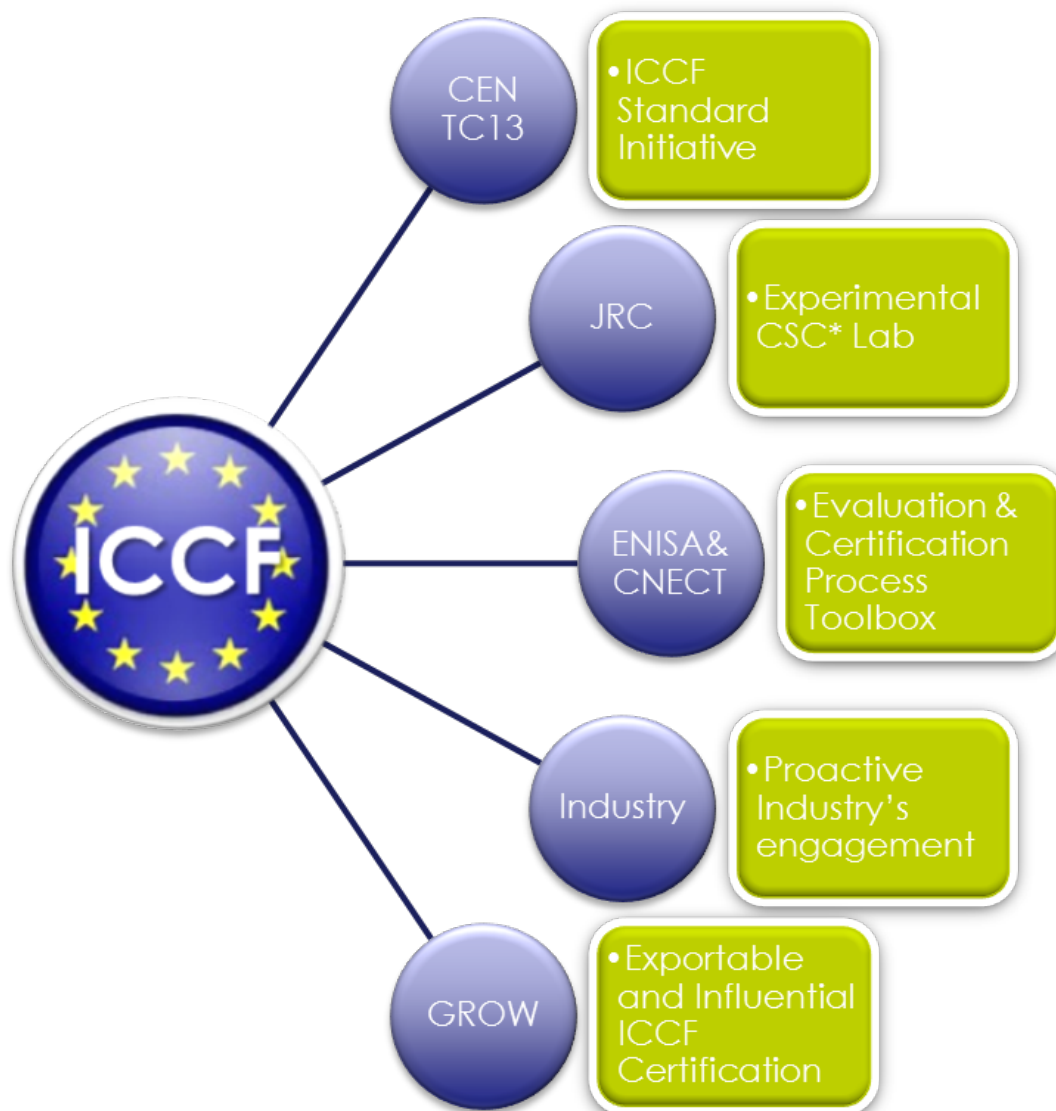
Figure 12: ICCF phase 4's desired outcome

7.7 Coordination of ICCF phase 4 projects

As an example, the CEN-Cenelec ICCF standard initiative (project 3 in Section 7.3, on the right-hand side of the diagram below) could be synchronised with the ICCF pilot project under an observable protocol (project 2 in Section 7.3, the process of which is on the left-hand side of the diagram below).
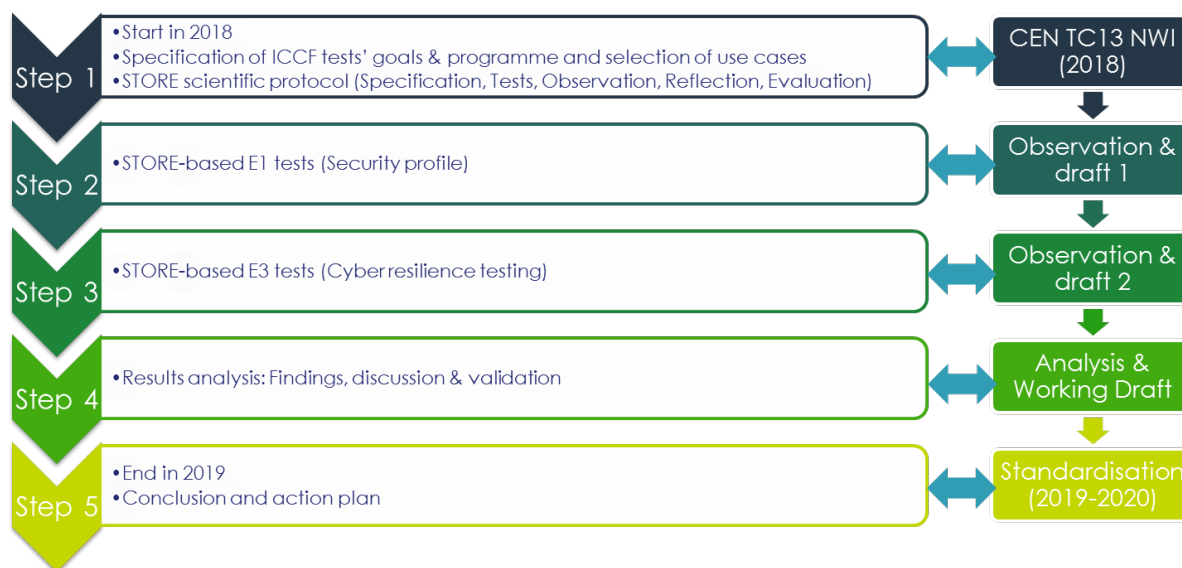
Figure 13: ICCF phase 4 projects' synchronisation

Under this principle, the CEN standardisation team would benefit from the observations of the pilot project to elaborate on them the elements of a future supporting standard.

At the present stage, the protocol of the pilot project needs to be defined and this should be one of the first actions to be taken in the course of phase 4 works.

8 List of tables and illustrations

9 References

(1) MITRE, 'Cyber resiliency engineering framework', 2011.

(2) ASCI EDSA-100 Version 2, 'ISA Security Compliance Institute — Embedded Device Security Assurance — ISASecure certification scheme,' Automation Standards Compliance Institute, 2011.

(3) IEC 62443-4-2, 'Security for industrial automation and control systems — Technical security requirements for IACS components,', Draft 2, Edit 4, 2 July 2015.

(4) DHS, 'NCCIC / ICS-CERT FY 2015 Annual Vulnerability Coordination Report,' 2015. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY %202015_Annual_Vulnerability_Coordination_Report_S508C.pdf (Accessed 11 Sept 2016).

(5) Theron, P., 'ICT resilience as dynamic process and cumulative aptitude', in Theron, P. and Bologna, S. (eds), *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, PA, Hershey, IGI Global, 2013, pp. 1-35.

(6) Tardieu, H., Rochfeld, A. and Colletti, R., *La méthode Merise: Principes et outils*, Paris, Éditions d'organisation, 1983.

(7) H. Tardieu, A. Rochfeld, R. Colletti, G. Panet and G. Vahée, La méthode Merise, Paris: Éditions d'organisation, 1985.

ANNEX I – FRENCH National Exercise Team

The French NET annex includes the following documents:

- French NET report: this document presents the overall process of the exercise, including composition of the NET, methodology, methodology of the elaboration of the protection profile, methodology of the elaboration of the security profile, evaluation of the product and conclusions.
- Test plan report: this document details the compliance assessment methodology (called conformity in the document) and reports on cyber resilience tests (called resistance in the document).
- Protection profile of an industrial firewall: this document prescribes how to describe the product and its usage, the associated critical assets, the threat model, the security objectives and how these elements may relate to one another.
- Stormshield Network Security, Industrial Firewall SNi40 — CSPN Security Target: this document details how, for a specific product, its description, associated critical assets and threat model are described.

French NET Report

1 Executive Summary

The present document is the result of the French NET, which objective was to gather French entities to instantiate the JRC's framework described in [ICCF] document, section 7.2 Proposed plan of action for the ERNCIP IACS TG in 2017. Hereafter is how France would implement both "Compliance assessment" and "Cyber resilience testing" tasks.

The work consisted in gathering a developer, an ITSEF, a stakeholder and a certification body, to draft a Protection Profile, a Security Target and a Test Plan for a given product. But our goal was not only to draft these documents, but also to focus on how to draft these documents, and specifically to address the caveats an author could encounter. Therefore, in the present report, for the three documents, we detail the different steps with examples on how writing the documentation.

Table of Content

2 References

[CSPN]   Certificat de Sécurité de Premier Niveau, ANSSI, http://ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/les-procedures-formulaires-et-methodologies/index.html

[ICCF]   Introduction to the European IACS components Cybersecurity Certification Framework, Joint Research Center

[PP]   Protection profile of an industrial firewall, Version 1.0 short-term, ANSSI

[ST]   Industrial Firewall SNi40 Firewall Software Suite version 3.3.1 CSPN Security Target, Stormshield Network Security

[TPR]   Test Plan Report

3 Acronyms

ANSSI   Agence Nationale de la Sécurité des Systèmes d'Information

CB   Certification Body

CSPN   Certificat de Sécurité de Premier Niveau

ETR   Evaluation Technical Report

ICCF   Introduction to the European IACS components Cybersecurity Certification Framework

ITSEF   Information Technology Security Evaluation Facility

PLC   Programmable Logic Controller

PP   Protection Profile

RTE   Réseau de Transport d'Électricité

SCADA   Supervisory Control and Data Acquisition

ST   Security Target

TOE   Target of Evaluation

VPN   Virtual Private Network

4 Introduction

4.1 French NET

4.1.1 Composition of the French NET

To assess JRC's guidelines defined in the [ICCF] document we have instantiated the various roles as follows:

- − Developer: Stormshield
- − ITSEF: Oppida
- − Stakeholder: RTE France
- − Certification Body: ANSSI

4.1.2 French NET Organization

The French NET gathered during the following internal meetings:

- − Thursday 27th of July
- − Wednesday 13th of September
- − Thursday 5nd of October

4.1.3 Assumptions

As the [ICCF] document does not define a process for the "Compliance assessment", nor the "Cyber resilience testing", the French NET decided to use the French CSPN methodology ([CSPN]), which corresponds to the ICCS-B level defined in [ICCF]. Therefore we are using the CSPN procedure (ANSSI-CSPN-CER-P-01) and instruction (ANSSI-CSPN-CER-I-02) available on the ANSSI website[1]. These documents define acronyms and technical terms, so the reader might need to refer to them in case this document does not fully define them.

4.2 Methodology

The CSPN methodology has been created by ANSSI in 2008, and consists in "black box" or "grey box" testing under constrained time. The CSPN is an alternative to Common Criteria[2] evaluation, for which the cost and the duration can be an obstacle, and when the degree of confidence aimed is lower.

A CSPN evaluation is based on a Security Profile Target, which can also be based on a Protection Profile, to carry on the product evaluation strictly speaking. The figure below summarizes what the following document details: i.e. the relationship between the Protection Profile, the Security Target and the production evaluation (hereafter called test plan for this project).

---

[1] http://ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/les-procedures-formulaires-et-methodologies/index.html
[2] http://www.commincriteriaportal.org
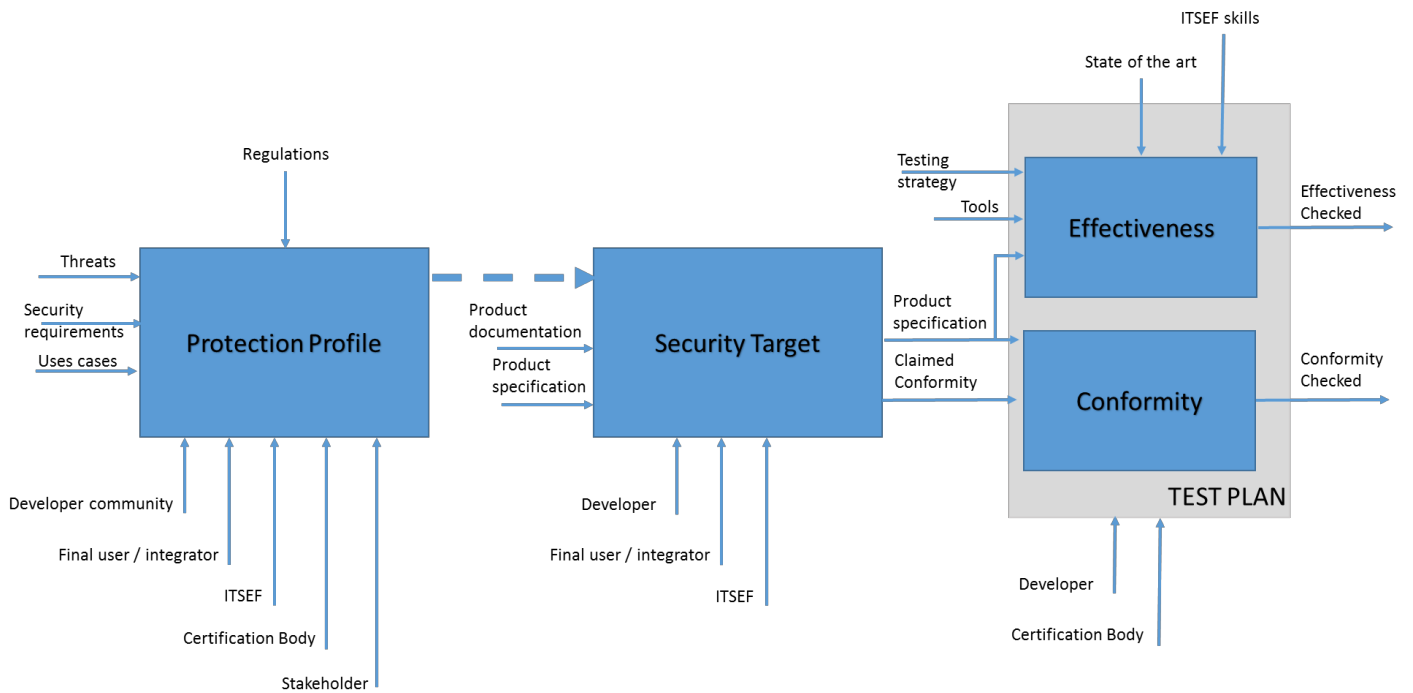
4.2.1 Product Used

The French NET has based its study on the Stormshield SNi40. It's an industrial firewall developed by Stormshield, a fully-owned subsidiary of Airbus Defence and Space.

4.2.2 Inputs

The French NET used the following documents as inputs:

− Firewall Protection Profile (PP) issued by ANSSI. It can also be found on the ANSSI website[3]
− Stormshield SNi40 Security Target[4] (ST), which was a previous security target used for an evaluation.

4.3 Tasks

The French NET decided to perform the three following ERNCIP tasks:

− **E1**: Elaborate a protection profile and a security profile and report on the easiness/difficulty of this
− **E2**: Simulate a product compliance assessment, document and report on easiness and difficulty
− **E3**: Simulate a product cyber resilience test, document and report on easiness and difficulty

---

[3] http://ssi.gouv.fr/uploads/2015/03/20150713_NP_ANSSI_SDE_firewall_short_term_v1.0-en.pdf
[4] http://ssi.gouv.fr/uploads/2016/08/sn_ase_cible_cspnv1.3.pdf

5 Drafting a Protection Profile

Input	Output	Actors
− Threats related to the field − Security requirements for the field − Use cases − Regulations (National, European, linked to the field, etc.)	− PP	− Developer community − Final user / integrator − ITSEF − Stakeholder − Certification Body

5.1 Stakes

A Protection Profile is a way for all the involved actors to agree on the security definition. That is defining the assets, threats and security objectives for a given set of products. A PP is indeed made for each category of product such as: firewalls, Programmable Logic Controller (PLC), VPN, Supervisory Control and Data Acquisition (SCADA) server, etc.

It is also a way for a costumer to easily compare products. If several products have been evaluated using the same PP, a costumer can be sure they have at least a minimum set of security functions in common, and he can therefore focus on the functions that are not in common.

5.2 Goal of a PP

A PP is to be used as a template for many different Security Targets, which in turn are to be used in different evaluations.

5.3 Methodology

The following figure details the model used to draft a PP.

Figure 2: Conceptual model of a Protection Profile
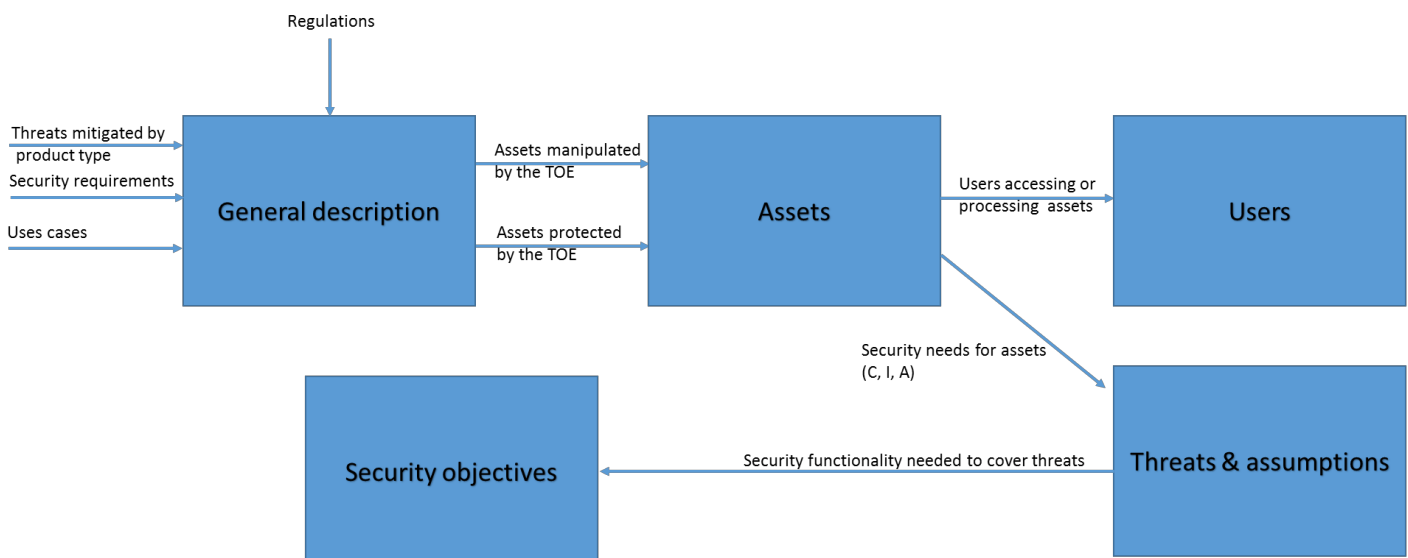
Involved Roles
− PP author
− PP approving
− Steering committee (Developer community, Final user / integrator, ITSEF, Stakeholder, Certification Body)

5.3.1 Drafting the PP

All actors need to achieve a common understanding about the product and its field of use. The way is to come up with questions about the product (users, assets, threats, security objectives, etc.) and have them answered inside the PP.

A PP shall have a general structure which is independent of the product, as the [ICCF] document details in section "Conceptual model of a Protection Profile". The following figure details the general sections a PP should have:

Figure 3: Protection Profile Contents
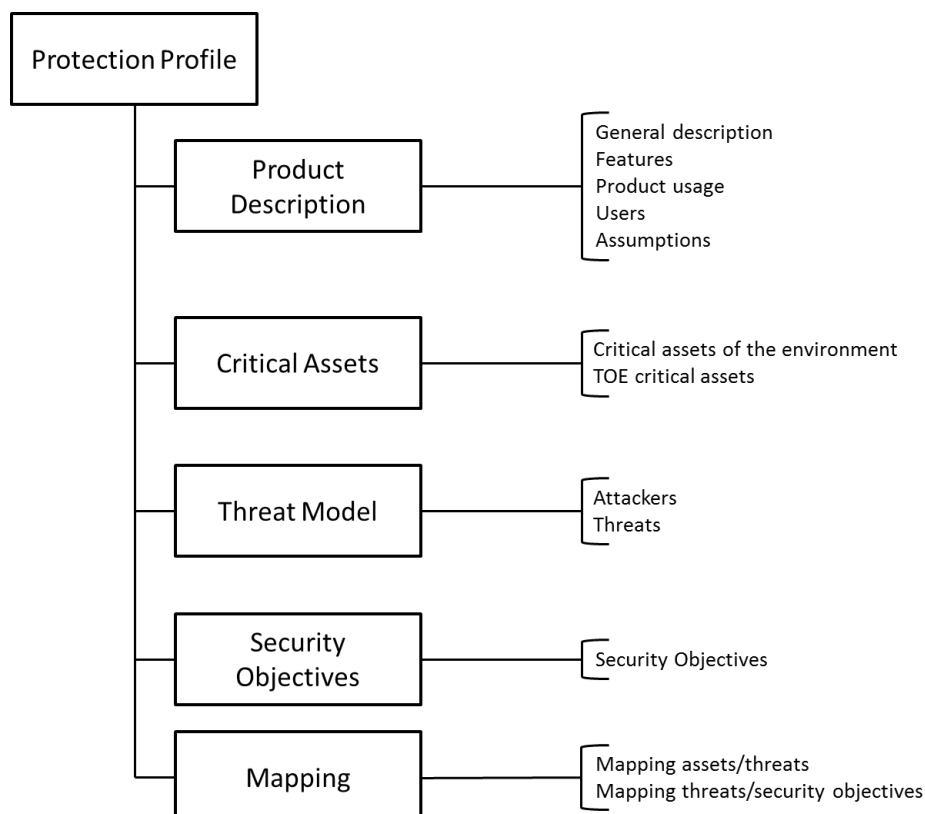
In order to fill out the general section listed in the above figure we have made the sections underneath. The objective is to make the link with the supporting document [PP], therefore to each of the following section is appended the actual paragraph in the [PP].

5.3.1.1   Product Description (PP§1.1)

Multiple products of the same category, for example industrial firewalls, may differ on certain aspects of their usage. But it is necessary, as well as important, to concentrate on what they have in common and what makes them industrial firewalls.

Example: They, of course, all have a filtering functionality, but they can also be managed remotely, so in such case an authentication on this administration interface is required.

5.3.1.2   Product usage (PP§1.3)

This section describes how and where the product is used.

5.3.1.3   Defining the users (PP§1.4)

All users interacting with the product shall be listed.

Warning: A user does not necessarily need to be a human. It can be a remote program interacting with the product such as a Logging server, or an administration access.

5.3.1.4   Defining the assumptions (PP§1.5)

Assumptions are formulated on the environment and how the product is used.

5.3.1.5   Defining the critical assets (PP§2)

The author must make a list of all sensitive assets the product is using. To do this he must identify if the product manipulates cryptographic keys, certificates, logins, passwords, firmware, logs, configuration files, etc.

Example: The author must put the product in its environment to understand the assets that could be shared, stored or acted upon by the product, but whose origins are external (also called *assets of the environment*). These assets are data, in the broadest sense, coming from a user, such as applications for examples, or a process interacting with the product, such as credentials to access a configuration server.

Of course the last step is to define the security criteria for each of the assets. The basic and most commonly used security criteria are: availability, confidentiality, integrity and authenticity. If a certain field requires a specific criterion it can of course be added.

5.3.1.6   Defining the threats (PP§3)

It is important to start by defining the threat agents. By doing so, we define the potential of the attacker and its positioning in the environment:

- Is he in the network?
- Does he have a physical access to the product?
- Can he steal the product?
- What rights does he have on the product?
- etc.

The next step is to take all critical assets previously listed and find one or multiple threats an attacker can have on them. The objective is to find threats that jeopardize the asset's security criteria.

Example: If a cryptographic key requires confidentiality there needs to be a threat challenging its confidentiality.

5.3.1.7 Defining security objectives (PP§4)

A security objective is here to counter a threat. Expressed in natural language, a security objective can counter one or multiple threats. The only rule is that all threats listed at section 5.3.1.6 must be countered by a security objective.

Again, this is a PP, so a security objective mustn't be specific, but rather generic. It will be the developer's goal to instantiate them when drafting the security target.

Example: Malformed input management: The Target of Evaluation has been developed in order to handle correctly malformed input, in particular malformed network traffic.

Warning: An assumption can reduce a threat, but it is mandatory that an objective of security covers this given threat. In other words, no threat can be covered only by an assumption.

5.3.1.8 Mapping (PP§Annex A and B)

Listing the mapping assets/threats and threats/security objectives is also important. It allows checking that nothing has been forgotten.

5.3.2 PP Verification

The Certification Body needs to verify the PP is not incoherent. Also writing a PP is an iterative process so several iterations might be needed to finalize the PP.

6 Drafting a Security Target

Input	Output	Actors
− PP − Product documentation: user guide, sales offer, data sheet, whitepaper, website, etc. − Product specification	− ST	− Developer − Final user/integrator − ITSEF

Warning: We wanted to highlight the information added to the Protection Profile in order to instantiate it as a Security Target. Therefore we chose to put in blue this additional information, which is of course not part of the PP.

6.1 Stakes

A Security Target defines the perimeter, the context of use of the product but also how the product is evaluated. That is, a product can have a dedicated configuration, where additional security measures are added or only a subpart of the cryptographic algorithm are taken into account for example. Therefore is it important for the final user to initialize the product with this specific configuration. Also, it is important to keep in mind that the ITSEF will evaluate the product with this given configuration.

From a final customer point of view, the security target also allows him to understand what the ITSEF evaluates.

6.2 Goal of a ST

A security target must answer a security need. This is done by detailing the product's assets, threats and security functions.

6.3 Methodology

Involved Roles
− ST author Can be the developer or ITSEF − ST approving Can be the developer or the Certification Body

6.3.1 Drafting the ST

The PP is only a framework, a template, as seen in section 5.2; the ST author needs to instantiate this framework with the actual data from the product. To do so he uses the developer's documentation to retrieve the product description, usage, assets, users and threats. The general idea is to instantiate the information listed in the PP with the developer's product.

Since the ST used here is based on PP it therefore follows the same structure. This structure is defined hereafter, which is roughly the one also described in section "Conceptual model of a Security Profile" of the [ICCF] document.

Figure 4: Security Target Contents
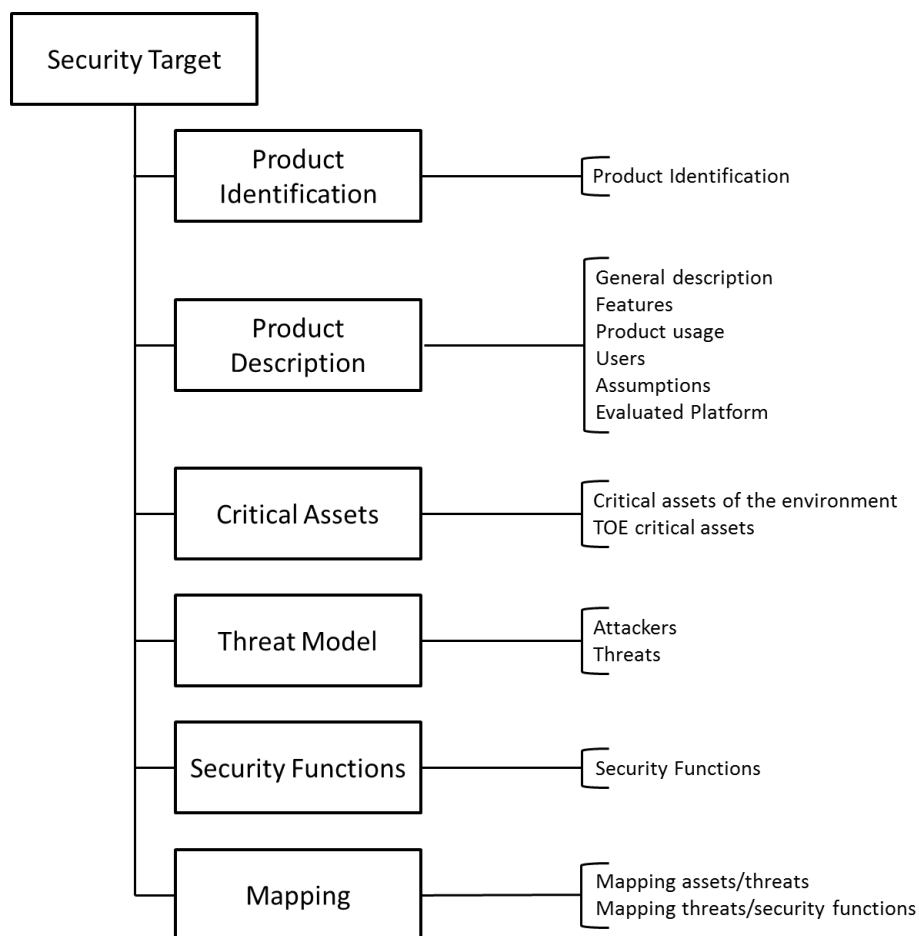
6.3.1.1 Product identification (ST§1)

The product identification shall also at least identify:

- Product's commercial name
- Product version
- Product category

It is important the ST details the product in terms of version. This is especially true when a product is composed of multiple bricks such as an Operating System (OS), libraries, configuration files, etc. So this particular version of the product will be linked to the version of the implemented bricks.

Example: If the version 1.2 of a given evaluated product is based on the Linux kernel 4.12, uses OpenSSL 1.1.0f and the Apache HTTP Server 2.4, then this freezes the version and it will therefore be the evaluated configuration and the certified configuration, if the certification occurs.

6.3.1.2 Evaluated platform (ST§1.6)

The product needs to be positioned inside its environment of use. This helps understanding how the product works, what interactions it has with its close environment and the possible human interactions.

Warning: This section is only present in the ST. This is due to the fact that the PP is generic; therefore it is up to the ST author to add this section.

Also, if a product is not autonomous and needs a connection to a remote server, or specific software needs to be used to interact with it, then theses dependencies need to be detailed in this section.

It is important for the ITSEF to have such information in order to be able to set up the platform and run the tests.

6.3.1.3 Product configuration (ST§1.7)

A configuration has to be defined. This configuration will be the one evaluated.

To do so, it may be possible to deactivate or change certain parameters in order to comply with the PP and its security objectives. More generally the author needs to think about the following:

- Are there multiple use cases of the product? If so, he will have to list them.
- Are there any unused services, for the ST perimeter? Is so, it may be useful to deactivate them, so the ITSEF will not be able to take advantage of them.
- Is there a service, that is out of scope and potentially vulnerable and still activated?
- Does the product have any dependencies with other components (configuration server, authentication server, etc.)? If so, take into account these connections (generally it requires the need for a security function such as "Secured communications").

6.3.1.4 Adding assets and/or threats (ST§2 and 3)

It is possible to add assets and/or threats in the Security Target to those defined in the Protection Profile, If the product contains more assets or is subject to more threats.

By adding threats, the ST author may have to add security functions if the one in the PP do not cover the new threats.

Warning: The ST author has to bear in mind that is not possible to delete any assets, threats or even security functions coming from the PP.

6.3.1.5 Security functions (ST§4)

The goal is to take the security objectives from the PP and instantiate them by using the product documentation. It is important to list for each function what it does:

- Does it perform encryption?
- If so, what algorithm?
- With which key?

- Where is stored the key?
- How is this key protected?
- etc.

> Warning: The author then needs to be sure the security functions implemented by the product do indeed meet the security objectives. For example, if the PP mandates the secure storage of confidential data but is not implemented by the product then a reimplementation of the product will of course be needed.

6.3.1.6 Mapping (ST§Annex A and B)

The mapping listed in the PP must be updated with the possible assets, threats and security functions added in the ST.

6.3.2 ST Verification

The Certification Body needs to verify that the ST is not misleading or incoherent with the PP.

7 Evaluation

Input	Output	Actors
− PP − ST − Product documentation: user guide, cryptographic specification, source code, etc. − Tools	− Evaluation Technical Report (see Remark)	− ITSEF − Certification Body − Developer

Remark: the output is normally an Evaluation Technical Report (ETR) but for this project we only provide a test plan (see [TPR]).

7.1 Goal of the Evaluation

The goal of the evaluation is twofold. The first one is to verify that the product performs its functions as described in the security target. This task is called the conformity assessment (see section 7.2.1). The second, the most important, is then to verify how resistant the product is. This task is called the resistance assessment (see section 7.2.2).

Both tasks are performed solely by the ITSEF. As mentioned is section 4.2, the evaluation is performed under constrained time. Therefore the ITSEF's previous knowledge is important here. The ITSEF evaluators decide what strategy to apply in order to fully evaluate the product. But they have to verify the conformity and assess the resistance of all security functions listed in the security target. How to perform the tests, in which order, in which depth, which attack path to use, etc. is up to them. The ITSEF can also rely on the developer in case he needs more information on the product, or needs help in its configuration for example.

Warning: At the end of the evaluation, all the evaluation information is put in the Evaluation Technical Report. This document is shared with the Certification Body, who then performs an analysis. If the CB decides the coverage is not complete for example, the ITSEF shall then perform additional tests.

7.2 Methodology

The following figure details the methodology used for a product evaluation under the CSPN scheme.

Figure 5: Evaluation Methodology

NOK => Additional tests required

ITSEF skills
State of the art

Testing strategy

Tools

Security Target

Product specification

Claimed Conformity

Resistance Tests

Conformity Tests

Effectiveness Checked

Conformity Checked

Tests review By Certification Body

OK => Evaluation Technical Report approved

Certification Body

TEST PLAN
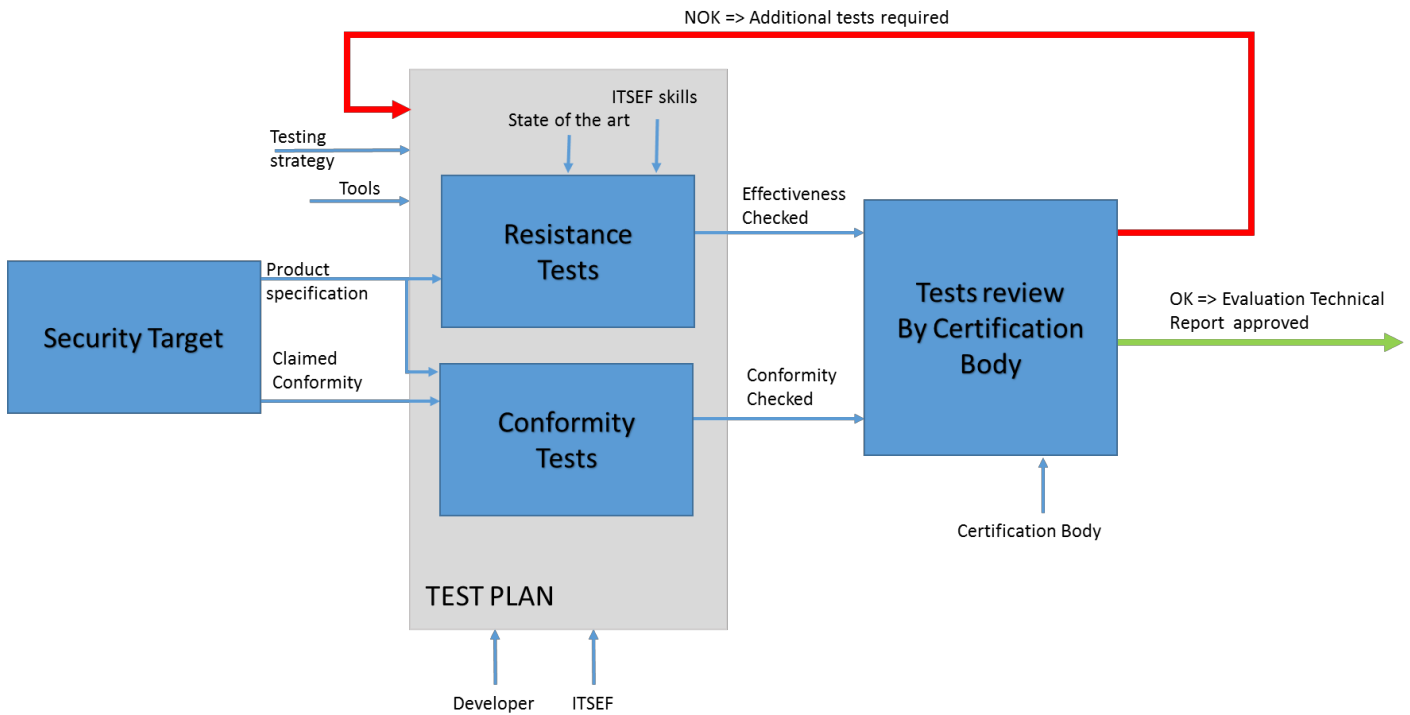
Developer   ITSEF

Involved Roles
− ITSEF
− Certification Body
− Developer

<u>Warning</u>: the evaluator that participated in the drafting of the ST cannot participate in the evaluation of the product.

7.2.1 Conformity

The objective of this phase is twofold, that is:

− First of all, to verify that the product conforms to its security specifications: all the non-conformities discovered must be traced and stated in the ETR

− Secondly, to enable the evaluator to fully understand the product in its entirety, so as to be relevant in the effectiveness analysis.

By doing so, the evaluator fills the "Compliance assessment" activity described in [ICCF].

Hereafter is a brief general-type list of what an evaluator has to verify:

− Is the platform the developer handed over to the ITSEF the one listed in the ST?
  o Version number?
  o Firmware version?
  o etc.
− Do all assets exist?
− Can all users described in the ST interact with the product?

- Do all security functions exist?
  - Do they conform to their description in the ST?
- Are all assumptions listed in the ST in line with how the product is used?
- Is the configuration defined in the ST easily applicable to the product?
  - Is this configuration defined inside the product's guides?
  - Is it easy to configure the product? Can the user be misled during the configuration?
  - Is the configuration listed in the ST already applied to the product when initialized?
    - If not, what are the differences with the configuration listed in the ST?
- Is the ST consistent with the PP?

The evaluator of course has to perform the conformity of all security functions. We have listed in section 7.2.3 the security functions and the type of conformity tests he could perform.

7.2.2 Resistance

Based on the ITSEF's knowledge on the type of product and the state of the art attacks, the evaluator's goal is to assess the following:

- The effectiveness of the security functions (also called *pentesting*)
- The impact of the product on the host system's security

By doing so, the evaluator fills the "Cyber resilience testing" activity described in [ICCF].

Concerning the effectiveness analysis the evaluator shall:

- Rate the resistance of the security functions and mechanisms and, where applicable, the cryptographic mechanisms
- Identify the vulnerabilities
- Provide an opinion on the risks of improper use
- Provide an expert opinion on the product's effectiveness
- Potentially, propose a configuration and a usage environment which limit the exploitability of the vulnerabilities and, in this case, give a second expert opinion on the product's effectiveness in its new usage environment.

Warning: One shall keep in mind that the ITSEF will use all available interfaces, all binary, any protocol flaw to take advantage of the product. Even if these flaws are not in the scope of the evaluation.

For example, if an administrator web interface is accessible, with an easily guessable login and password, he can use it to attack the product, even if this interface is not part of the evaluation scope. This can also be the case for physical interfaces, where a debug port can be forgotten by the developer, the evaluator can use it to retrieve critical assets.

The evaluator of course has to perform the resistance of all security functions. We have listed in section 7.2.3 the security functions and the type of tests he could perform.

7.2.3 Test Samples

Security Function	Example of conformity test	Example of resistance test
Malformed input management	Where does this input management take place? What policy is already in place? Is the policy really applied?	Focus on the fields that could potentially be used to inject data, or bypass authentications. Fuzzing techniques could be used to see how the product handles malformed data. Also the evaluator could try to send a large amount of malformed data to see how the product handles this amount of data.
Filtering policy enforcement	On what type of data is such filtering applied? Depending on the policy already in place does the filtering really apply? Does the filtering apply on all type of data?	For all the protocols the product filters, is it possible to try to send maliciously crafted data to see the robustness of such filter? Is it possible for example to bypass a filter?
Protocol conformity analysis	What protocols does the product filter (the ones described in the security target)? Does the product really filter these protocols?	If a flaw is detected in the protocol specification, is it also present in the implementation of the product? Is it possible to fuzz the protocol to find flaws?
Secure storage of secrets	What are the assets the product stores? Verify these assets are not stored in clear on the filesystem.	What are the secrets the product stores? What type of memory does the product have? Where could the data be stored on such memory?
Secure authentication on administration interface	How is this interface accessed? Does it take advantage of cryptography (HTTPS for example)?	Is the mechanism used to authenticate the administrator robust enough to prevent brute force attacks? Does the authentication mechanism use certificates; if so is it resistant against attacks based on modified certificates?
Access control policy	When the policy is applied, are the defined roles really implemented? Is all administration actions logged by the product?	Can a role have more privilege operations than the one defined? Given the roles, is an escalation possible? Is It is possible to bypass the policy?

Firmware signature	Is a valid firmware accepted by the product?	Depending on how the firmware structure is made, can a modification to the signature still allow a crafted firmware to be installed?
	Is an invalid firmware rejected by the product?	
	Is a revoked firmware rejected by the product?	Is it possible to take advantage of the parser that will find and compute the signature and the header of the file to make the product install a crafted firmware?
Configuration confidentiality and integrity	What assets shall be kept confidential and must not be modified?	What is the mechanism used to keep the confidentiality and integrity?
	Verify that such assets are indeed protected in confidentiality and integrity.	How resistant is it against an attacker who has a logical access to the filesystem?

7.2.4 Validation

When the evaluation is over, the ITSEF and CB initiate a discussion over the report. This discussion will cover the tests the ITSEF has performed, focusing on the following points:

- Have all security functions been tested in conformity and resistance?
- Do the tests performed fully cover the security functions or should more tests be performed?
- Are the conclusions correct?
- Are the attack rating correct?
- Etc.

Warning: It is very important for the Certification Body to have enough technical background in order to challenge the ITSEF on the technical field. By doing it, the CB can be sure the ITSEF is as much as possible up-to-date concerning the attack state-of-the-art.

If the certifier agrees with what the ITSEF has made, then the report is validated and the CB can then certify the product.

8 Conclusion

Our goal was to instantiate the ICCF process with a product, roles and a methodology in order to see how the framework fits in a real situation. The product has been chosen only when all roles were filed in. It seemed important for the group to have a stakeholder - as it is not always the case in certification projects - to get their input on the way they will use the product and therefore the security functions it will need to implement and of course the environment in which it will have to fit in.

We then needed to rely on a developer for the product. Having Stormshield in the group allowed us to have access to a variety of products and especially industrial-type products.

The group then focused on the PP. To do so we took the one already published, but focused on trying to see if it required an update. When done, the second task was the ST. The entire NET was gathered to discuss on what the product does and how the instantiation shall be done. We also took the [ICCF] document to check if the ST was compliant. The result is the accompanying [ST]. Also, to show how the instantiation is done, we decided to highlight it by using another color for the font. Therefore the blue one is specifically here for this matter.

Finally the step was to create a test plan. The usual report an ITSEF provides the ANSSI is an Evaluation Technical Report, as mentioned in Remark, but here only a test plan could be handed over to the project. The objective of this test plan is to provide a general idea on the conformity and resistance tests an ITSEF performs to assess a product's security.

8.1 Impacts on the framework (ICCF)

8.1.1 Process

As mentioned in the introduction, the [ICCF] document does not yet define how to perform both the "Compliance assessment" and the "Cyber resilience testing". This is where this works fits in. Its goal is to provide a test case, with an actual product, and try to supply a methodology. We tried as much as possible to describe what the French NET has done in term of process, for it to be reused by the ERNCIP as much as possible.

8.1.2 Methodology

No evaluation methodology is defined in the [ICCF] document. This is the reason why the French NET decided to use the [CSPN], as it is for us the best answer to both "Cyber resilience testing" and "Compliance assessment".

8.2 Open discussion

We have listed the following points as open for the ERNCIP group to discuss:

- Next step is to perform a full evaluation, conformity and resistance, of a product. It could be really interesting to perform a full analysis of a product. Should this product be the same for all NETs?
- Need for a common methodology? We find it interesting to share with the other NETs the methodology we used and the results we have, and initiate discussions over the ones they

used. This brings up the question: does a common methodology need to be worked on? And more broadly, how would a certification authority be able to certify a product that hasn't been assessed with a common methodology?

Test Plan Report

Table of Content

1. References

[FNR]   French NET Report

[RGS]   Référentiel Général de Sécurité, ANSSI

2. Methodology

The following security functions are listed in the ST:

- Malformed input management
- Filtering policy enforcement
- Protocol conformity analysis
- Secure storage of secrets
- Secure authentication on administration interface
- Access control policy
- Firmware signature
- Configuration confidentiality and integrity

The evaluator shall therefore first verify the conformity of these security functions and after test their resistance. The actual tests an evaluator would perform are enclosed in a test case where the following items are detailed:

- Reference: unique name of the test
- Objectives: what is to be performed
- Prerequisite: what is needed to perform the test
- Tools: tools used by the evaluator to perform the test
- Proceedings: high level steps the evaluator will put in place
- Expected result

3. Conformity

As mentioned in the lead document, the French NET Report ([FNR]), the conformity is mainly here to verify that the product delivered to the evaluator is compliant to what is mentioned in the security target (ST).

3.1 Product Identification

Product Identification	
Reference	**T.Product_ID**
Objectives	Identify the product, as well as its version.
Prerequisite	Web administration interface to access the product.
Tools	Browser
Proceedings	The evaluator shall use the web administration interface to retrieve the product name and its version.
Expected result	The product shall be the SNi40 and the version 3.3.1.

3.2 Asset Identification

Asset Identification	
Reference	**T.Asset_ID**
Objectives	Identify all the assets listed in the ST to verify that all are implemented by the product.
Prerequisite	Logical access to the product, in order to browse the filesystem.
Tools	SSH
Proceedings	After logging into the product, the evaluator shall identify all assets listed in the ST.
Expected result	All assets listed in the ST shall be implemented by the product.

3.3 Malformed input management

Malformed input management	
Reference	**T.CONF_INPUT**
Objectives	The goal of the tests is to verify the input management is implemented by the product.
Prerequisite	Fully functional product.
Tools	Python, scapy
Proceedings	Tools making it possible to simulate traffic or a previously captured traffic on which the fuzzing is applied.
Expected result	The product should have malformed input management in place.

3.4 Filtering policy enforcement

Filtering policy enforcement	
Reference	**T.CONF_FILTER**
Objectives	The goal of the tests is to verify that the filtering policy is enforced by the product.
Prerequisite	Fully functional product.
Tools	Python, scapy
Proceedings	Through the configuration interface, the evaluator shall verify that a policy can be implemented. When the policy is implemented and the filtering activated, by sending traffic, he shall verify the effect of such filtering policy.

Expected result	The product should have a filtering policy enforced.

3.5 Protocol conformity analysis

Protocol conformity analysis	
Reference	**T.CONF_PROTOCOL**
Objectives	The goal of the tests is to verify that the product does indeed rely on the protocols listed in the security target.
Prerequisite	Protocol specification
Tools	Python, scapy, wireshark
Proceedings	The evaluator shall monitor the incoming and outgoing traffic and verify that the protocols listed in the security target are indeed implemented by the product.
Expected result	The product shall implement the protocols listed in the security target.

3.6 Secure storage of secrets

Secure storage of secrets	
Reference	**T.CONF_SECRETS**
Objectives	The goal of the tests is to verify that the product does handle secrets.
Prerequisite	Fully functional product.
Tools	Browser
Proceedings	Through the configuration interface, the evaluator shall verify that the product can handle secrets such as passwords.
Expected result	The product shall implement the secure storage of secrets.

3.7 Secure authentication on administration interface

Secure authentication on administration interface	
Reference	**T.CONF_AUTH**
Objectives	The goal of the tests is to verify that the product implements a secure authentication on the administration interface.

Prerequisite	Fully functional product.
Tools	Browser
Proceedings	The evaluator shall verify the settings of such function. When activated, he shall verify that an authentication is indeed activated for the administrator.
Expected result	A secure authentication shall be implemented by the product.

3.8 Access control policy

Access control policy	
Reference	**T.CONF_ACCESS**
Objectives	The goal of the tests is to verify that the access control policy is enforced by the product.
Prerequisite	Fully functional product.
Tools	Browser
Proceedings	Through the configuration interface, the evaluator shall verify that an access control policy can be implemented.
	When the policy implemented and the filtering activated, the evaluator shall verify that is indeed in place.
Expected result	The product should have an access control policy enforced.

3.9 Firmware signature

Firmware signature	
Reference	**T.CONF_**
Objectives	The goal of the tests is to verify that the product implements firmware signature.
Prerequisite	Fully functional product with a set of valid firmwares and unsigned ones.
Tools	Browser
Proceedings	The evaluator shall verify the settings of such function. When activated, he shall verify that only signed firmwares are accepted by the product, unsigned firmware shall be rejected.
Expected result	The product shall verify and accept only signed firmwares.

3.10 Configuration confidentiality and integrity

Configuration confidentiality and integrity	
Reference	**T.CONF_**
Objectives	The goal of the tests is to verify that the filtering policy is enforced by the product.
Prerequisite	Fully functional product.
Tools	Browser
Proceedings	Through the configuration interface, the evaluator shall verify that the setting to protect the confidentiality and integrity is set.
Expected result	The product shall implement a confidentiality and integrity protection for the configuration.

4. Resistance

4.1 Malformed input management

Malformed input management	
Reference	**T.FUZZING**
Objectives	The objective of the tests is to see how the product reacts when malformed packets are sent. Fuzzing is generally used to discover vulnerabilities.
Prerequisite	Fully functional product.
Tools	Python, scapy, isic, tcpsic
Proceedings	Tools making it possible to simulate traffic or a previously captured traffic on which the fuzzing is applied.
Expected result	The behavior should not be different, even when the product is subject to malformed packets.

Malformed input management	
Reference	**T.STRESS**
Objectives	The objective of these tests is to identify if the product has a different behavior when it is subject to strong external stimulus.
Prerequisite	Fully functional product.
Tools	Python, scapy, wireshark, hping3

Proceedings	Tools making it possible to simulate an intense stress on the firewall are used.
	In parallel the evaluator tries to send an application package to the PLC which uses a writing function of Modbus.
Expected result	The behavior should not be different, even when the product is subject to strong external stimulus.

4.2 Filtering policy enforcement

Filtering policy enforcement	
Reference	**T.EVADE_TCPIP**
Objectives	The objective of these tests is to verify if it's possible to bypass the protocol detection carried out by the filtering module, with the intention to check if policy prohibited application packets can pass through, while exploiting TCP/IP sessions.
Prerequisite	The product has a filtering policy in place, which filters out the writing functions of Modbus.
Tools	Python, scapy, wireshark, hping3
Proceedings	The evaluator tries to send an application package to the PLC which uses a writing function of Modbus.
Expected result	The application packet shall be dropped by the product and shall not go to the PLC.

Filtering policy enforcement	
Reference	**T.EVADE_MODBUS**
Objectives	The objective of these tests is to verify if it's possible to bypass the protocol detection carried out by the filtering module, with the intention to check if a Modbus prohibited application packets can pass through.
Prerequisite	The product has a filtering policy in place, which filters out the writing functions of Modbus.
Tools	Mbtget, python, scapy, wireshark
Proceedings	The evaluator tries to send an application package to the PLC which uses a writing function of Modbus.
Expected result	The application packet shall be dropped by the product and shall not go to the PLC.

Filtering policy enforcement	
Reference	**T.EVADE_104**
Objectives	The objective of these tests is to verify if it's possible to bypass the protocol detection carried out by the filtering module, with the intention to check if an IEC 104 prohibited application packets can pass through.
Prerequisite	The product has a filtering policy in place, which filters out the STOPDT function.
Tools	Python, scapy, wireshark
Proceedings	The evaluator tries to send a STOPDT IEC 104 packet to the PLC
Expected result	The STOPDT IEC 104 packet shall be dropped by the product and shall not go to the PLC.

Filtering policy enforcement	
Reference	**T.EVADE_S7**
Objectives	The objective of these tests is to verify if it's possible to bypass the protocol detection carried out by the filtering module, with the intention to check if a S7 prohibited packets can pass through.
Prerequisite	The product has a filtering policy in place, which filters the S7 protocol.
Tools	Python, scapy, wireshark
Proceedings	The evaluator tries to send an application package using the S7 protocol to the PLC which uses a writing function.
Expected result	The application packet shall be dropped by the product and shall not go to the PLC.

4.3   Protocol conformity analysis

Protocol conformity analysis	
Reference	**T.PROTOCOL**
Objectives	The objective of these tests is to verify if the protocol conforms to the specification.
Prerequisite	Protocol specification
Tools	Python, scapy, wireshark
Proceedings	The evaluator tries to send packets that are slightly modified compared to the one of the protocol to see how the product handles them.
Expected result	The product shall drop packets that do not conform to the specification.

4.4 Secure storage of secrets

The conformity analysis has shown that two different dataset could be used to store the passwords. Therefore the evaluator has to check which one is actually the correct one.

Secure storage of secrets	
Reference	**T.PASSWD**
Objectives	The goal of the tests is to understand if the secure storage uses passwd.
Prerequisite	Logical access to the product, in order to browse the filesystem.
Tools	SSH
Proceedings	Use passwd to change password and see if any changes occur on passwd file.
Expected result	The user password should change.

Secure storage of secrets	
Reference	**T.PASSWD2**
Objectives	The goal of the tests is to understand if the secure storage uses pwd.db and/or spwd.db.
Prerequisite	Logical access to the product, in order to browse the filesystem.
Tools	SSH
Proceedings	Use passwd to change password and see if any changes occur on passwd file.
Expected result	The user password should change.

4.5 Secure authentication on administration interface

Secure authentication on administration interface	
Reference	**T.BRUTFORCE**
Objectives	Check if a mechanism used to prevent brute force attacks on the authentication page is implemented
Prerequisite	Connected to the administration network and have access to the administration Web interface.
Tools	Web browser, Burp Proxy Suite Pro (version 1.6.30)
Proceedings	Send several authentication requests to the server with invalid credentials.
Expected result	Mechanism against brute force or dictionary attacks is properly and

	efficiently implemented.

Secure authentication on administration interface	
Reference	**T.FAKECERTIF**
Objectives	Check if the authentication process is achieved when a client certificate signed by a certificate chain, which is not registered in the PKI of the TOE, is used.
Prerequisite	• Connected to the administration network and have access to the administration Web interface. • A certificate authority for the authentication, signed by the root certificate authority, installed in the TOE. A client certificate correctly signed by the authentication certificate authority and associated to an administration profile in the LDAP database.
Tools	OpenSSL
Proceedings	• Replicate a certificate chain (root certificate authority, authentication certificate authority and client certificate) outside the TOE but with the same information. • Install this chain on the web browser and submit the client certificate to the TOE during the authentication process.
Expected result	Authentication should fail indicating that Certificate is not allowed

Secure authentication on administration interface	
Reference	**T.AUTOCOMPLETEPWD**
Objectives	Check if the password field of the authentication formulary is properly configured to not store the password.
Prerequisite	Connected to the administration network and have access to the administration Web interface.
Tools	Web browser, Burp Proxy Suite Pro (version 1.6.30)
Proceedings	Perform an authentication request with valid credentials
Expected result	Authentication formulary should not auto complete password

4.6   Access control policy

Access control policy	
Reference	**T.ACP_CONFIG**

Objectives	The goal of the tests is to find where the access control policy is configured.
Prerequisite	Web administration interface to access the product. Logical access to the product, in order to browse the filesystem.
Tools	SSH, browser
Proceedings	Through the administration interface the evaluator can change the different access control settings and then see the impact it has on the filesystem.
Expected result	The access control policy should be stored in files.

Access control policy	
Reference	**T.ACP_BYPASS**
Objectives	The goal is to find if it is possible to bypass the policy in place. The evaluator wants to verify if a race condition or TOCTOU attacks could be used here.
Prerequisite	Web administration interface to access the product. Logical access to the product, in order to browse the filesystem.
Tools	SSH, browser
Proceedings	The evaluator needs to verify if the policy is applied instantly or not.
Expected result	Access control policy should not be bypassed.

4.7 Firmware signature

Firmware signature	
Reference	**T.MALFORMED_UPDATE**
Objectives	The goal is to test whether the product protects itself against malformed updates (incorrect signature, no signature, etc.).
Prerequisite	Web administration interface to access the product.
Tools	
Proceedings	The evaluator tries to force an update of the firmware with a malformed update.
Expected result	The product should not install the update.

4.8 Configuration confidentiality and integrity

Configuration confidentiality and integrity	
Reference	**T.FILESYSTEM**
Objectives	The goal is to verify the rights of the configuration files on the filesystem and estimate if they are well protected.
Prerequisite	Logical access to the product, in order to browse the filesystem.
Tools	SSH
Proceedings	Browse the filesystem to retrieve the rights of the configuration files.
Expected result	Files should only be accessible to "admin" user.

Configuration confidentiality and integrity	
Reference	**T.CSRF**
Objectives	A vulnerability was previously known on the administration interface. The goal is to check if this CSRF vulnerability is still here.
Prerequisite	The product is in place and has the administration interface available.
Tools	Browser, burp
Proceedings	The evaluator tries to take advantage of the CSRF vulnerability in the administration interface.
Expected result	The vulnerability should be present in the administration interface.

Protection profile of an industrial firewall

Version 1.0 short-term

GTCSI

July 13, 2015

Preface

In the whole document, the acronym ToE (Target of Evaluation) designates the component being evaluated.

Text in red differs from the mid-term version of the protection profile.

1 Product description

1.1 General description

In this protection profile, the ToE is an industrial firewall. It is designed for running in hostile environments where classical firewalls could not run properly due to heat, humidity or dust, for instance.

From a functional perspective, this firewall allows to interconnect an industrial network that has to be protected with another network with at least one of the following characteristics:

- a lesser control or a lesser level of trust;

- specific applications which do not interact with the industrial network;

- another industrial network with different functionalities;

- another domain of responsibility.

Depending on the architecture, this firewall can act as an IP router, a TCP proxy or an Ethernet bridge (stealth mode) for non-IP protocols. The firewall controls and filters the flows and can rewrites protocols from the layer 2 up to the applicative layer depending on supported and inspected protocols.

1.2 Features

The ToE includes the following features:

- **Network filtering:** The ToE supports dynamic filtering at layers 3 and 4 (stateful firewall). It also supports filtering at the layer 2 when the ToE is in stealth mode.

- **Protocol analysis:** The ToE checks that input packets are conform to the protocol specifications. This feature is not necessarily supported by all devices and the user should check that the right protocol is supported when they chose a device.

- **Administration functions:** The ToE includes administration functions in order to configure, or program the other functionalities of the ToE. Several administration interfaces are possible:

- thick-clients (sometimes also called, depending on the context, administration console, programming workstation...);

- web-clients;

- removable devices (USB drives, SD memory cards, etc.).

- **Local logging:** The ToE supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events.

- **Remote logging:** The ToE supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

1.3 Product usage

In accordance with the recommendations of ANSSI guide[1], the industrial firewall can be used to segregate networks of different criticalities (Class 1 and class 2). It can also be used to protect an Industrial Control System (ICS) from a management information system. Finally, it can be used for segregating different parts of an ICS. When the avaibility is critical, two firewalls can be used in redudancy in order to increase the resiliency of the interconnection. The use of a firewall is depicted on figure 1.

Figure 1: Use case of an industrial firewall

1.4 Users

The users that may interact with the ToE are the following:

- **Administrator:** user having the permission to modify the configuration of the ToE.

- **Auditor:** User having the permission to consult logs of the ToE.

- **Super-administrator:** User having all the privileges on the ToE. He can, in particular, create, modify or delete user accounts.

- **End-device:** End device directly or indirectly connected to the ToE.

Remark: A user is not necessary a human being, it may be a device or a third-party software. Moreover, the same person may own several user accounts corresponding to different profiles.

1.5 Assumptions

Assumptions on the environment and the use case of the ToE are the following:

- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the ToE.

- **Administrators:** ToE administrators are competent, trained and trustworthy.

---

[1] *The cybersecurity of ICSs: Classification method and main measures*, ANSSI, january 2014

- **Super-administrators:** Super-administrators are trained for performing the tasks they are responsible for. They follow instructions and administration manuals of the ToE and they are not hostile.

- **Premises:** The ToE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the ToE.

  Since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.

- **Filtering policy:** We assume that the filtering policy configured in the ToE is adapted to the use case.

- **Dimensioning:** We assume the ToE is properly dimensionned for its tasks.

- **Authentication servers:** When appropriate, the authentication servers used for authenticating users are assumed uncompromised and properly configured.

- **Active logging:** We assume that local and remote logging are operational and that local logs are not corrupted.

- **Unevaluated services disabled by default:** Services of the ToE which are not covered by the security target are disabled in the default configuration (also named factory default configuration).

- **Security documentation:** The ToE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization.

  All recommendations included in this documentation are applied prior to the evaluation.

2 Critical assets

2.1 Critical assets of the environment

The critical assets of the environment are the following:

- **Flows matrix:** Thanks to its filtering, the ToE controls the communication between end devices according to the defined flow matrix. For instance, for a layer 4 filtering, a rule contains source and destination addresses, the transport protocol (TCP, UDP. . .) and, when necessary, source and destination ports.

- **Conformity of protocols:** The ToE controls the protocol conformity of the flows identified in its configuration. In addition, the ToE may restrict the functionnalities of some protocols.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Flows matrix	X		X	
Conformity of protocols	X		X	
X: mandatory		(X): optional		

2.2 ToE critical assets

The critical assets of the ToE are the following:

- **Firmware:** In order to work properly, the firmware must be protected both in integrity and authenticity.

- **Configuration:** The configuration of the ToE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the ToE by other means than the ToE activity.

- **User authentication mechanism:** This mechanism can be based on a local database or on a remote authentication server. In both cases, the ToE must ensure the integrity and authenticity of the mechanism[2].

- **User secrets:** The user secrets can be passwords, certificates... They can be stored in the ToE or stored in a remote authentication server. In all cases, the ToE must ensure the integrity and confidentiality of these credentials.

- **Access control policy:** The policy can be stored locally or remotely on a authentication server. In both cases, the ToE must ensure the integrity of the access control policy.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
Configuration		X	X	
User authentication mechanism			X	X
User secrets		X	X	
Access control policy			X	
X: mandatory		(X): optional		

3 Threat Model

3.1 Attackers

The following attackers are considered:

- **Evil end-device:** A device connected to the ToE is controlled by the attacker.

- **Evil administration device:** A device plugged on the administration network is controlled by the attacker but the attacker may not have valid credentials on the ToE.

3.2 Threats

The following threats are considered:

- **Denial of service:** The attacker manages to generate a denial of service on the ToE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file...). This denial of service can affect the whole ToE or only some of its functions.

- **Filtering policy violation:** The attacker manages to violate the filtering policy of the ToE by performing an illegitimate data transfer or by blocking a legitimate flow.

- **Protocol conformity violation:** The attacker manages to make non-compliant protocols to transit through the ToE. The attacker manages to bypass the configured protocol limitations.

- **Firmware alteration:** The attacker manages to inject and run a corrupted firmware on the ToE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution.

---

[2]All authentication mechanisms offered by the ToE may not necessarily be part of the security target. However, those which are not included in the security target must be disabled by default.

A user may attempt to install that update on the ToE by legitimate means.

Finally, the attacker manages to modify the version of the firmware installed on the ToE without having the privilege to do so.

- **Configuation alteration:** The attacker manages to modify, temporary or permanently, the ToE configuration.

- **Configuration compromise:** The attacker manages to illegally obtain some parts of the ToE configuration.

- **Credentials theft:** The attacker manages to steal user credentials.

- **Authentication violation:** The attacker succeeds in authenticating himself without credentials.

- **Access control violation:** The attacker manages to obtain permissions that he does not normally have.

4 Security objectives

The following security objectives are considered:

- **Malformed input management:** The ToE has been developped in order to handle correctly malformed input, in particular malformed network traffic.

- **Filtering policy enforcement:** The ToE supports filtering between networks allowing to enforce the security policy of the IT system. Two types of filtering can be distinguished:

  Stateless filtering: Filtering decision depends on the packet content only. It can be performed at level 2 (Ethernet) or level 3 (IP), level 4 (TCP or UDP) and for some applicative protocols. This security function is available with the ToE redundant or not.

  Stateful firewall: After a stateless filtering action, the device can established a context depending on the flow and the associated protocol. This makes filtering more accurate. Stateful filtering can be only performed on flows above IP level and can take the transport protocol (TCP/UDP) into account. In some cases, it can also take applicative protocol into consideration. This security function is available with the ToE redundant or not.

- **Protocol conformity analysis:** The ToE checks the conformity of certain protocols exchanges. This analysis is perfomed at the transport layer (TCP, UDP...) and the application layer (HTTP, SMTP, FTP, Profinet, Modbus, EtherNet/IP...). The final user should check that the appropriate protocols are supported by the ToE and covered by the security target.

- **Secure connection with the authentication server:** The ToE supports secure connection with the authentication server. The secure connection allows authenticating both peers and protecting the integrity and the authenticity of exchanges. It guarantees also non replay of exchanges.

- **Secure storage of secrets:** User secrets are securely stored in the ToE. In particular, the compromise of a file is not sufficient for retrieving them.

- **Secure authentication on administration interface:** Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.

- **Access control policy:** The access control policy is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

- **Firmware signature:** At each update of the firmware, integrity and authenticity of the new firmware are checked before updating.

- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the ToE.

A Critical assets vs threats

	Flows matrix	Conformity of protocols	Firmware	Configuration	User authentication mechanism	User secrets	Access control policy
Denial of service	Av I	Av I					
Filtering policy violation	I						
Protocol conformity violation		I					
Firmware alteration			I Au				
Configuation alteration				I			
Configuration compromise				C C			
Credentials theft						C I C	
Authentication violation					I Au		
Access control violation							I
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity							

B Threats vs security objectives

	Denial of service	Filtering policy violation	Protocol conformity violation	Firmware alteration	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation
Malformed input management	X								
Filtering policy enforcement		X							
Protocol conformity analysis			X						
Secure connection with the authentication server								X	
Secure storage of secrets							X		
Secure authentication on administration interface					X	X	X	X	
Access control policy									X
Firmware signature				X					
Configuration confidentiality and integrity					X	X			

C   Contributors

This protection profile has been produced by the working group on cybersecurity for industrial systems, supervised by the French Network and Information Security Agency (ANSSI).

The following compagnies and organisms contributed to this document:

- Amossys

- ARC Informatique

- Belden

- DGA/MI

- Gimelec

- Oppida

- Phoenix Contact

- RATP

- Schneider Electric

- Siemens

- Sogeti

- Stormshield

- Thales

Stormshield Network Security

Industrial Firewall SNi40

Firewall Software Suite version 3.3.1

CSPN Security Target

DOCUMENT TRACKING

Version	Date	Modifications
2.1	01/12/2017	Minor updates for ERNCIP
2.0	03/11/2017	Update to TOE version 3.3.1
1.3	29/06/2016	Official Security Target Evaluated, TOE version = 2.3.4

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TERMINOLOGY AND ABBREVIATIONS

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Filter policy	Set of technical rules describing which entities are entitled to set up information flows with which entities.
Trusted network	A network is considered trusted if, due to the fact that it is under the control of the TOE operator, the internal security policy does not imply that there is a need to be protected from information flows originating from it, but on the contrary, implies that there is a need to protect information flows going to it.
Uncontrolled network	A network is considered uncontrolled if it is not under the control of the TOE operator, meaning that users need to be protected from information flows set up with devices from this network (the internet, for example)..
TOE	Target of Evaluation

REFERENCE DOCUMENTS

[PP_IPF]	Protection profile of an industrial firewall Version 1.0 short-term - GTCSI July 13, 2015
[ANSSI_GUIDE]	La cybersécurité des systèmes industriels Méthode de classification et mesures principales, ANSSI, janvier 2013

1 PRODUCT DESCRIPTION

Editor	Stormshield
Editor's website	www.stormshield.com
Product name	Stormshield Network Security
Evaluated version	Model SNi40 – Software suite version 3.3.1
Product category	Industrial Firewall

Table 1: Product Identification

1.1 General description

Stormshield Network Security UTM / NG-Firewalls is a range of appliances that provide security features allowing the interconnection between one or several trusted networks and an uncontrolled network, without compromising the level of security of any of the trusted networks.

It can be split into two groups of features:

- The firewall feature: filtering, attack detection, bandwidth management, security policy management, audit, accountability and strong authentication of administrators,

- The VPN (Virtual Private Network: encryption and authentication) feature implementing [ESP] in IPSec tunnel mode and securing the transmission of confidential data between remote sites, partners or mobile salespersons.

ASQ (Active Security Qualification) is a real-time intrusion prevention technology embedded in all Stormshield appliances of the Stormshield Network Security range. Based on a multi-layer analysis, ASQ detects and prevents the most sophisticated attacks without affecting the network performance and considerably lowers the number of false positives. This technology is backed up by alarm features which can be fully customized.

The ToE submitted to evaluation is an industrial firewall. It is designed for running in hostile environments where classical firewalls could not run properly due to heat, humidity or dust, for instance.

From a functional perspective, this firewall allows to interconnect an industrial network that has to be protected with another network with at least one of the following characteristics:

- a lesser control or a lesser level of trust;
- specific applications which do not interact with the industrial network;
- another industrial network with different functionalities;
- another domain of responsibility.

~~Depending on the architecture, This firewall can act as an IP router, a TCP proxy or anEthernet bridge (stealth mode) for non-IP protocols.~~

This firewall can act as an Ethernet bridge or an IP router for IP protocols.

The firewall controls and filters the flows and can rewrites protocols from the layer 3 ~~2~~ up to the applicative layer depending on supported and inspected protocols.

The Evaluation will only consider the following features:

- dynamic filtering of IP flow, at layer 3 and 4;
- analysis and inspection of major industrial protocols : *Modbus, S7 and IEC 104;*
- local authentication and management of the appliance administrators;
- The logging component.

The specific evaluated configuration is provided in section 1.7.

1.2   Features

Network filtering

The ToE supports dynamic filtering at layers 3 and 4 (stateful firewall). ~~It also supports filtering at the layer 2 when the ToE is in stealth mode.~~

Protocol analysis

The ToE checks that input packets are conform to the protocol specifications.

The TOE can check in particular: Modbus, S7 and IEC 104.

Administration functions

The Stormshield Web Manager administration tool allows, via an intuitive and user-friendly graphical interface, the installation and the configuration of the Stormshield appliances, an provides simplified monitoring and reporting functionalities.

In order to have strong administrator authentication, the Stormshield appliance manages a user database and provides authentication services against it.

Local logging:

The ToE supports the configuration of a local logging policy. ~~It is possible, in particular, to log security and administration events.~~

Remote logging

The ToE supports the definition of a remote logging policy. ~~In particular, it is possible to log security and administration events.~~ Events are sent in SYSLOG (UDP/TCP/TLS) or via SNMP traps.

1.3   Product usage

In accordance with the recommendations of [ANSSI_GUIDE], the industrial firewall can be used to segregate networks of different criticalities (Class 1 and class 2). It can also be used to protect an Industrial Control System (ICS) from a management information system. Finally, it can be used for segregating different parts of an ICS. When the availability is critical, two firewalls can be used in redundancy in order to increase the resiliency of the interconnection.

The use of a firewall is depicted on Figure 1.

Industrial facilities,
Workstations and Servers to protect

**Stormshield
UTM / NG-Firewall
SNi40**

Uncontrolled Network

Trusted Network
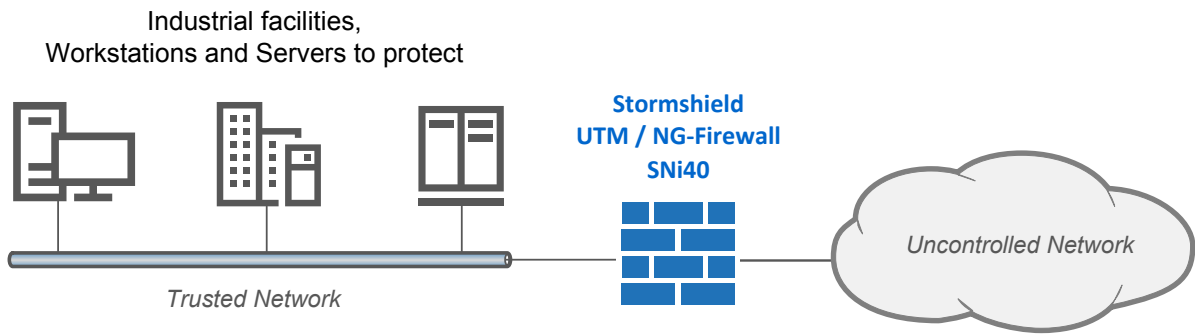
Figure 1: Example of use of the TOE

1.4 Users

The users that may interact with the ToE are the following:

Administrator: User having the permission to modify the configuration of the ToE. He can't modify other administrator accounts.

Auditor: User having the permission to consult logs of the ToE.

Super-administrator: User having all the privileges on the ToE. He can, in particular, create, modify or delete ~~user~~ administrator accounts.

End-device: End device directly or indirectly connected to the ToE.

Remark: A user is not necessary a human being, it may be a device or a third-party software. Moreover, the same person may own several user accounts corresponding to different profiles.

1.5 Assumptions

Logs checking

We assume that administrators check regularly the local and remote logs produced by the ToE.

Administrators

ToE administrators are competent, trained and trustworthy.

Super-administrators

Super-administrators are trained for performing the tasks they are responsible for. They follow instructions and administration manuals of the ToE and they are not hostile.

Premises

The ToE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the ToE. Since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.

Filtering policy

We assume that the filtering policy configured in the ToE is adapted to the use case.

Dimensioning

We assume the ToE is properly dimensioned for its tasks.

~~Authentication servers~~

~~When appropriate, the authentication servers used for authenticating users are assumed uncompromised and properly configured.~~

Active logging

We assume that local and remote logging are operational and that local logs are not corrupted.

Unevaluated services disabled by default

~~Services of the ToE which are not covered by the security target are disabled in the default configuration (also named factory default configuration).~~

Most of the available features but out of this security target are disabled in the default configuration (also called factory settings). Some, out of the target, needs to be disabled:

- The IPv4 DHCP server

- The IPS inspection for out of scope protocols.

The specific list of not evaluated features is provided in section 2.8.

Security documentation

The ToE is provided with a complete documentation for a secure usage. ~~In particular, all secrets are listed in order to allow their customization~~. In particular, the documentation highlights to change administrator's default password.

All recommendations included in this documentation are applied prior to the evaluation.

1.6 Evaluated platform

The evaluated platform includes:

- A Stormshield SNi40 Firewall.

- A Windows 7 administration console.

The selected internet browser is Microsoft Internet Explorer Version 9.

1.7 Product configuration and use case under evaluation

The usage mode subject to evaluation has the following characteristics:

- The local console is not used in production. Only the super-administrator can log on to it, and hypothetically, such interventions are performed only when a decision has been made to make an exception to the operating context – to conduct a maintenance operation or a re-installation.

- Workstations on which the Stormshield Web Manager will be launched are secured, dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them.

- All administrators are subject to an identification/authentication stage provided by the TOE and which may use: login/password authentication in a TLS channel or mutual authentication by X.509 certificate in a TLS channel.

- Certificates and CRLs are distributed manually (importing).

- The VPN functions of Stormshield appliance are not part of the evaluation

- When log events are sent via syslog, the server that receives them is not part of the evaluation.

- When alarms are sent via SNMP, only version v3 is enabled.

- The usage mode subject to evaluation excludes the fact that the TOE relies on services other than PKI, DNS and DHCP servers and proxies. The optional modules provided by Stormshield to manage these services are disabled by default and have to stay that way. Specifically, these are:

    - modules that allow handling external servers (e.g.: Kerberos, RADIUS, etc),
    - the dynamic routing module,
    - the static multicast routing module,
    - the internal public key infrastructure (PKI),
    - the SSL VPN module (Portal and Tunnel),
    - DNS cache,
    - antivirus engine (ClamAV or Kaspersky),
    - Active Update module,
    - SSH, DHCP, MPD and SNMPD servers,
    - the DHCP client and NTP daemon,
    - the DHCP relay,
    - WIFI connection for equipped devices,
    - The Geo-localization and IP/Host reputation
    - the bypass functionality
    - Any custom IPS patterns
    - FQDN objects (require external DNS services)
    - IPFIX messages

- The IPV4 DHCP Server shall be stopped after the appliance initialization.

- Despite being available, the IPv6 routing feature is disabled by default and shall stay disabled during the evaluation.

- Administrators' credentials are managed through an LDAP database within the Stormshield UTM / NG-Firewall firmware and which is part of the TOE. The LDAP access from outside the appliance itself is not included in the evaluation.

- Logs shall be either stored locally or sent to a SYSLOG server.

- ASQ technology implements contextual analyses at the application level, with the purpose of verifying compliance with the RFCs and countering attacks at the application level. Application analysis functions that are the focus of the evaluation are those associated with

    - At transport layer: TCP, UDP
    - At application layer:
        - IT protocols: FTP, HTTP, SMTP, DNS,
        - Industrial protocols: Modbus, S7, 104.

    The not evaluated protocols are blocked and kept this way.

- The ability provided by the filter policy to associate each filter rule with an application inspection (HTTP, SMTP, POP3 and FTP proxies) and as is the scheduling feature falls outside of the scope of this evaluation and must not be used.

- The ability provided by the filter policy to associate the "decrypt" action (SSL proxy) with a filter rule falls outside the scope of this evaluation and must not be used.

- The following features may be used, but are not considered as security functions:

    - Address translation (network address translation or NAT);
    - the vulnerability management module;
    - the high availability module;
    - the feature for viewing embedded reports;

- The cryptographic algorithms implemented are those in the default configuration:

    - Authentication/Integrity: 256-bit SHA-2
    - Key negotiation: Diffie-Hellman group 14
    - Encryption: 256-bit AES in CBC mode
    - PFS (Perfect Forward Secrecy): activated

2 CRITICAL ASSETS

2.1 Critical assets for the environment

Flows matrix

Thanks to its filtering, the ToE controls the communication between end devices according to the defined flow matrix. For instance, for a layer 4 filtering, a rule contains source and destination addresses, the transport protocol (TCP, UDP) and, when necessary, source and destination ports.

Conformity of protocols

The ToE controls the protocol conformity of the flows identified in its configuration. In addition, the ToE may restrict the functionalities of some protocols.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Flows matrix	●		●	
Conformity of protocols	●		●	

Table 2: Security requirements for environment critical assets

2.2 ToE critical assets

The critical assets of the ToE are the following:

Firmware

In order to work properly, the firmware must be protected both in integrity and authenticity.

Configuration

The configuration of the ToE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the ToE by other means than the ToE activity.

User authentication mechanism

This mechanism is based on a local database.

~~This mechanism can be based on a local database or on a remote authentication server. In both cases~~, The ToE must ensure the integrity and authenticity of the mechanism.

User secrets

~~The user secrets can be passwords, certificates. . . They can be stored in the ToE or stored in a remote authentication server. In all cases,~~ The ToE must ensure the integrity and confidentiality of ~~these~~ the appliance administrators' credentials.

Access control policy

The policy can be stored locally or remotely on an authentication server. In both cases, the ToE must ensure the integrity of the access control policy.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			●	●
Configuration		●	●	
User authentication Mechanism			●	●
User secrets		●	●	
Access control policy			●	

Table 3: Security requirements for TOE critical assets

3 THREAT MODEL

3.1 Attackers

The following attackers are considered:

Evil end-device

A device connected to the ToE is controlled by the attacker.

Evil administration device

A device plugged on the administration network is controlled by the attacker but the attacker may not have valid credentials on the ToE.

3.2 Threats

The following threats are considered:

Denial of service

The attacker manages to generate a denial of service on the ToE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file. . .). This denial of service can affect the whole ToE or only some of its functions.

Filtering policy violation

The attacker manages to violate the filtering policy of the ToE by performing an illegitimate data transfer or by blocking a legitimate flow.

Protocol conformity violation

The attacker manages to make non-compliant protocols to transit through the ToE. The attacker manages to bypass the configured protocol limitations.

Firmware alteration

The attacker manages to inject and run a corrupted firmware on the ToE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install that update on the ToE by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the ToE without having the privilege to do so.

Configuration alteration

The attacker manages to modify, temporary or permanently, the ToE configuration.

Configuration compromise

The attacker manages to illegally obtain some parts of the ToE configuration.

Credentials theft

The attacker manages to steal user credentials.

Authentication violation

The attacker succeeds in authenticating himself without credentials.

Access control violation

The attacker manages to obtain permissions that he does not normally have.

4 Security Functions

The following security objectives are considered:

Malformed input management

The ToE has been developed in order to handle correctly malformed input, in particular malformed network traffic.

At the Ethernet or IP level, upon receiving a malformed packet, an alarm will be raised. Depending on the trapped issue and the configuration of the alarm, the packet can be dropped or accepted

Example: A zero-size fragment or a Checksum error that could allow a DoS attack will be detected.

Filtering policy enforcement

The ToE supports filtering between networks allowing to set the security policy of the targeted IT system.

The TOE can do stateful filtering: after a stateless filtering action performed according the content of the paquet, the device can established a context depending on the flow and the associated protocol. This makes filtering more accurate.

Such feature allows the TOE to detect a response replay (i.e. receiving two responses for one single request). Another use case is being able to properly handle child connection (i.e. a connection created with information given by another connection), thus preventing the administrator to have to add rules for every single unknown future connection with a low level of restrictions.

Stateful filtering can be only performed on flows above IP level and can take into account the transport protocol (TCP/UDP) and applicative protocols (FTP, HTTP, SMTP, DNS, Modbus, S7, UMAS).

For example, the TOE gives the possibility to allow or prevent the use of « function codes » for Modbus, UMAS and S7. This offers:

- o The possibility to forbid every modification commands (writes) sent to the protected device
- o The possibility to forbid every maintenance commands (stop, updates) sent to the protected device.

This security function is available with the ToE redundant or not.

Protocol conformity analysis

The ToE checks the conformity of certain protocols exchanges. This analysis is perfomed:

- o at the transport layer: TCP, UDP;
- o and the application layer: HTTP, SMTP, FTP, DNS, Modbus, ~~EtherNet/IP~~, S7, IEC 104.

This analysis is usually called stateless analysis, its goal is to check that every field of the packet is correct accordingly of its description in the specification and against the rest of the packet. For example the announce length against the effective length, or that the announce length is within the specified values.

As an attack example reading outside the allowed registers values that could lead to a crash of the device and therefore a DoS.

Secure storage of secrets

User secrets (Administrator's credential) are securely stored in the ToE. In particular, the compromise of a file doesn't allow their retrieval.

Secure authentication on administration interface

Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.

Any log in event is logged.

Access control policy

The access control policy is strictly applied.

In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

For each and every administration action, the TOE controls that the user is allowed to perform it, according to five pre-defined roles: System, Network, User management, Filtering policy and monitoring.

Every administration action is logged.

Firmware signature

Firmware is digitally signed by accredited people within Stormshield. The signature certificate is factory installed.

For each update of the firmware, integrity and authenticity of the new firmware are checked before updating.

Installation is done by an administrator with the "system" role.

Every firmware update request action is logged.

Configuration confidentiality and integrity

Each administrator can have: no access, read only or full access permission on each of the five roles mentioned above.

Therefore, the access control prevents any unauthorized person to read or modify the TOE's configuration.

APPENDIX A: CRITICAL ASSETS VS THREATS

	Flows matrix	Conformity of protocols	Firmware	Configuration	User authentication mechanism	User secrets	Access control policy
Denial of service	Av I	Av I					
Filtering policy violation	I						
Protocol conformity violation		I					
Firmware alteration			I Au				
Configuration alteration				I			
Configuration compromise				C			
Credentials theft						C I	
Authentication violation					I Au		
Access control violation							I
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity							

Table 4: Critical assets vs threats

APPENDIX B: THREATS VS SECURITY OBJECTIVES

	Denial of service	Filtering policy violation	Protocol conformity violation	Firmware alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation
Malformed input management	●								
Filtering policy enforcement		●							
Protocol conformity analysis			●						
Secure connection with the authentication server								●	
Secure storage of secrets							●		
Secure authentication on administration interface					●	●	●	●	
Access control policy									●
Firmware signature				●					
Configuration confidentiality and integrity					●	●			

Table 5: Threats vs security objectives

ANNEX II – POLISH National Exercise Team

The Polish NET annex includes the following documents:

- Report on the results of experiments carried out by the Polish National Exercise Team (NET-PL) during phase 3 of ICCF.
- Appendix 1 of the final report by NET-PL: protection profile of a remote terminal unit (RTU), Version 1.0, Mikronika (NET-PL).
- Appendix 2 to the final report by NET-PL: protection profile of fire detection and fire alarm systems (FDAS) — Control and indication equipment (CIE) in distributed architecture, Version 1.0, Polon-Alfa (NET-PL).
- Appendix 3 to the final report by NET-PL: protection profile of a remote terminal unit (RTU), Version 2.1, NET-PL: Mikronika, GUT.

Report on the results of experiments carried out by the Polish National Exercise Team (NET-PL) during Phase 3 of ICCF[1]

Editor:

Janusz Górski, Gdansk University of Technlogy (NET-PL Leader)

Contributors (NET-PL participants)**:**

Piotr Chojnicki, Telbud

Paweł Florek, Kacper Karpiński, NCBOP

Michał Karolak, EY EMEIA Advisory Center

Izabela Lewandowska-Wiśniewska, PZU LAB

Krzysztof Politowski, Ministerstwo Cyfryzacji

Mariusz Sowiński, Polon-Alfa

Tomasz Szała, Mikronika

Andrzej Wardziński, Gdańsk University of Technology/Argevide

Disclaimer: This report represents the opinions of members of NET-PL and by no means should be considered as representing the official position of their institutions

---

[1] The European IACS components Cybersecurity Certification Framework (ICCF) proposed by ERNCIP (European Reference Network for Critical Infrastructure Protection) Project

About this document

This document presents the results of experiments carried out during Phase 3 of ICCF by the Polish National Exercise Team of Poland (NET-PL).

I.   Way of work

II.1 Composition of NET-PL

The following viewpoints were represented in NET-PL during the experiments:

- governmental agency,
- certification body,
- component producer,
- compliance testing,
- insurance,
- system integrator,
- industrial user.

II.2 The process

The process of carrying the experiments consisted of the following steps.

- **Step 1. Constitution of NET-PL**
  - During this step NET-PL has been constituted and an initial (virtual) meeting was carried out to discuss the objectives and the way forward, and to agree on the infrastructure supporting the further work
  - Duration: end of June- beginning of July 2017
- **Step 2. Implementing the supporting infrastructure and working on Protection Profiles**
  - During this step the following actions were undertaken
    - Implementation of the NET-PL Knowledge Base – this has been implemented in the NOR-STA system and made accessible to each NET-PL participant
      - The Knowledge Base contains all ICCF relevant documents, meetings minutes, relevant standards (IEC 62443 series), and NET-PL work products
    - Development of three Protection Profiles for two component classes offered by Mikronika and Polon-Alfa
      - Two Protection Profiles for class RTU (Remote Terminal Unit)
      - One protection Profile for class CIE (Control and Indication Equipment)
  - Duration: July-October 2017
- **Step 3: Experiments**
  - During this step, a Questionnaire for collecting data related to the ICCF experiments, E1, E2, E3 and E4 has been designed and distributed to the NET-PL participants.
  - While filling the Questionnaire, the NET-PL participants were asked to observe the following rules:
    - Responding from the perspective represented by own institution

- Not feeling obliged to give responses to all questions – responding to only these questions were one feels competent
- Remembering that this is not an official statement by the own institution (expressing more the personal opinion that the official position of the institution)
  - The received responses were processed and then sent back to all participants for their approval

The approved answers were included to the NET-PL report submitted to ICCF

- ***Step 4: Additional exercise***
  - During this step, the conformance argumentation template has been derived from the Protection Profile for RTU version 2.1 (See the Appendix 3)
  - The template is represented in the NOR-STA tool supporting development, maintenance and assessment of evidence based arguments

II. The results

The results achieved by NET-PL encompass:

1. Three Protection Profiles related to two classes of IACS components: RTU and CIE (for RTU: Version 1.0 and Version 2.1, the latter following recommendations of IEC 62443-4-2)
2. The data collected by means of the Questionnaire covering the scope of experiments E1, E2, E3 and E4.
3. The conformance argumentation template for a selected Protection Profile (PP for RTU version 2.1)
   a. The template can be accessed at https://tct.nor-sta.eu/ with the credentials
      i. login: iccf
      ii. password: q7T4miS23e

III. The Questionnaire

The following text summarizes the opinions of NET-PL participants collected by means of the Questionnaire. The Questionnaire has been structured in accordance with the experiments E1, E2, E3 and E4 foreseen for Phase 3 of ICCF. The opinions of NET-PL are expressed by text given in *Italic*.

E1: PP/SP development

1. **Management of component families**

   a) Parties involved and their roles

   Selection of component families should be under supervision of the National Cybersecurity Authority – NCA (such body is not yet formally existing in Poland). NCA should cooperate with the Critical Infrastructure operators and possibly component producers and system integrators to collect requests related to new component families and to collect and process the feedback related to the existing ones. The approved specification of component families should be accessible to the CI operators, system integrators and component producers.

   Distinguishing and agreeing on the functional classes of components and the related Protection Profiles should be a process involving different stakeholders and a consensus building procedure. It is important to involve all relevant stakeholders in the process of identifying component families and defining and approving their Protection Profiles. Agreeing on Protection Profiles at the European level is even a bigger challenge and requires information exchange, coordination and support from the Member States governments.

   Another concern is that different components, sharing the same functional profile (in terms of their purpose and functionality) may be used in different target environments which expose the components to different risks. This differentiation of risk profiles could (and should) be reflected by having different Protection Profiles for the same functional class of components. The notion of "security levels" could be relevant here

   Information on component classes and the related Protection Profiles should be maintained in the public domain. However, the information on the components and their Protection Profiles selected for a given Critical Infrastructure should be kept confidential and disclosed on the need-to-know basis.

   In particular the following parties should be involved in the process:

   - *Operators of Critical Infrastructures, System integrators, component producers*
     - *Defining the needs and selecting component classes*
   - *IACS component producers*
     - *Initiating the process of conformance assessment and certification*
   - *Insurance*
     - *Communicating on which conditions the insurance would be keen to take over the associated risks*
   - *Governmental and possibly EU level agencies*
     - *Organizational provisions, legal regulations, accreditation*

   General guidance on how to select component classes and to develop the related Protection Profiles should be accompanied with additional help (more detailed guidance, best practices to follow etc.)

   b) Criteria for distinguishing component families

   The following criteria should be considered:

   - *Do we really need to distinguish yet another family of components? (what is the difference with respect to the already existing component families)*
   - *What is the scope of cybersecurity risks to be addressed? (associated risk profiles related to potential target environments)*

- *Is there a sufficient demand for such new family of components? (e.g. the number of potentially interested users and suppliers)*

2. **Protection Profile development effort estimation**

   a) effort related to PPs developed by NET-PL

   – *Protection Profile for RTU version 1 (Mikronika) – 2 Man-Days (retrospection on a ready component)*

   – *Protection Profile for RTU version 2 (GUT/Mikronika) – 2 Man-Weeks (reorientation of the RTU version 1 Protection Profile towards the requirements of IEC 62443-4-2)*

   – *Protection Profile for CIE (Polon-Alfa) – 1-2 Man-Month (in situation where a representative of the class is almost implemented but the related protection profile not yet existed)*

   b) factors having impact on the effort

   It seems that there is a big difference between the situation where Protection Profile is defined retrospectively, from an already existing component (for which risk analysis and other security oriented issues have already been covered) and a newly created component//family of components where risk analyses, countermeasure selection etc. have to be covered starting from scratch. In the latter case the effort to create a Protection Profile would be significantly bigger.

   Building Protection Profiles for classes of components that are foreseen for the target environments with high cybersecurity risk profiles will need more effort and higher competencies.

   Another factor influencing the effort is the skills and competencies of the involved personnel, availability of an inventory of good practices, higher management support for this objective and others.

   A knowledge base covering the issues relevant to Protection Profile creation and adequate tool support could help to reduce the effort and to maintain high and even level of quality.

3. **PP development, maintenance and distribution process**

   a) Roles related to PP development

   Protection Profiles should result from a teamwork involving different perspectives at IACS components (regulators, users of components, producers of components, accreditation, auditors and certifiers). A common standard of representing Protection Profiles supplemented by a guidelines, best practices examples etc. would be very helpful. Tool support could be considered too.

   Recommendations of ISO 15408 could provide an initial input.

   b) Storage and maintenance of PPs

   – Rules of PP distribution

   Storing and distribution of Protection Profiles should be governed by agreements between interested parties. Technically, Protection Profiles should be accessible through Internet following a defined and published access policy respecting the IP rights.

   It is also important that the producers, users and other interested parties adequately represent the cyber-security viewpoint in their organizational structure, commit sufficient resources and provide continuous management support.

To provide sufficient supply of competencies, some changes in education, including the university curricula can be necessary.

– Main characteristics for change management process

Changing a Protection Profile should be a formalized process

The changes should be endorsed by all relevant stakeholders contributing to the Protection Profile

Users of the Protection Profile should be able to demonstrate that their change management processes are able to follow the changes on the Protection Profile side (this could be an aspect verified during certification)

4. SP development, maintenance and distribution process

a) Development, storage and maintenance of Security Profiles

Security Profiles should reflect more specific requirements which are elated to specific means used to implement the (higher level) requirements of the related Protection Profile. In this sense Security Profile can be considered as a specialization of the Protection Profile towards a more fine groups of components (a single component) belonging to the family of components the Protection Profile refers to.

Storage of Security Profiles should be solved mostly between the producers and users. A user selects a specific Protection Profile of interest and (possibly in cooperation with potential suppliers/producers) specifies it further towards a complete Security Profile.

b) SP development effort estimation, main effort factors

NET-PL does not have practical experience in this respect.

5. Business model for PP/SP management

Government – better control over cyber security of critical infrastructures

Component producers – improvement of market position (meeting the demands for cybersecurity certificates by their clients)

Operators of Critical Infrastructures – possibility to demonstrate that secure (certified) components are in use (which can be used to strengthen the argument about infrastructure security), self-assurance that security of a given critical infrastructure is being addressed meeting the requirements imposed by regulators

Insurance – mapping certificates on the risk levels would help to activate the market for 'cybersecurity insurance certificates' where higher-level certificates would imply lower insurance costs.

The costs of introducing Protection Profiles/Security Profiles and the related certification schemes will be paid mostly by the end users of the components. Depending on the regulatory context this may slow down the process of adopting the framework of certification.

E2: Compliance assessment

1. **The compliance assessment process model**

   a) Main actors involved in compliance assessment

   Component producer – responsible for collecting and submitting the evidence demonstrating that the component meets the requirements of the related Security Profile

   The Security Profile together with the evidence should be submitted to the Certifying Institution for assessment. The Certifying Institution can arrange for audit visits at the component producer's site to collect the evidence from the production site. The Certifying Institution can involve external specialized laboratories (for instance, testing labs) in the assessment process, if necessary.

   The process of achieving conformity (with the requirements of Security Profile) and demonstrating conformity should be well understood on both sides (producers and certifiers) to avoid misinterpretations of the requirements and misunderstandings related to what constitutes a sufficient evidence do demonstrate conformity.

   Responsibility to make sure that the certification processes comply with the expected standards is delegated to the Accreditation Body.

   b) Main steps of compliance assessment

   Certifying Institution perspective:

   1. *Analysis of the Security Profile and the evidence submitted by the client*
   2. *Assessment if the submitted evidence gives sufficient support for the Security Profile requirements*
   3. *Possible contact with the client (component producer) if collecting the evidence onsite is needed*
   4. *Issuing the final assessment*
   5. *Possibly granting a certificate*
   6. *Monitoring conformity (if repeated assessments are needed to maintain the certificate validity)*

   Component producer perspective:

   1) *Self-assessment of conformity*
   2) *Applying for a third party assessment and certificate*
   3) *Cooperating in the assessment process (if onsite visits are necessary)*
   4) *Receiving the assessment result and possibly a certificate*

   Government/Accreditation Body perspective

   1) *Issuing the regulations related to certification*
   2) *Appointing accredited certifying Institutions*
   3) *Making sure that the certification processes comply with stated quality criteria*
   4) *Improved monitoring of security maturity of critical infrastructures*

   c) Inputs to the process

   For the whole process:

   - *The list of accredited certifying institutions*

   For an instantiation of the process

- *Identification of the component subjected to certification*
- *The criteria to be used during certification (a particular Security Profile)*
- *The evidence demonstrating the fulfillment of the requirements of the Security Profile (for instance, the design documentation, test results, results of product analyses etc.)*
- *Onsite access for the auditors (if requested)*

d) Outputs from the process

Self-declaration (C1) or third party certificate (C2) confirming that the component meets the requirements of SP.

It is desirable that the result of the process gives in addition more detailed information on the results of assessing the particular requirements of SP.

If relevant, the client (component producer) should be also informed about the period of validity of the certificate and the requirements to be met if this period is to be extended

e) Assessment process standardization

It is highly recommended that there is a common model of the assessment and certification process that is communicated to and agreed upon by all interested parties.

The initiative should be from the government side with early involvement of all relevant stakeholders.

Such standard should be supported by a clear business model for each participant.

Adequate tools support is necessary to implement certification as a continuous process following rapid and often unexpected changes (which is characteristic for the cyber-security domain)

2. **Change management**

Requirements on how to manage changes in components with respect to the granted certificates should be a part of related regulations (of some help here could be ISO 9000 standards).

Certification requirements should have in their scope the assessment of change management process at component producer.

In case of component change, the producer should be obliged to notify the users and the Certifying Institution issuing the certificate.

The decision if and when the introduced change implies the need for re-certification should be left to the Certifying Institution.

3. **Business model for compliance assessment**

Accredited Certifying Institutions could offer third party certification services on the commercial basis

However, if certification is not requiring full resilience testing, its value for Critical Infrastructure operators can be problematic which will also decrease the value of such certificate for producers.

Together with the system for granting certificates there should be an enforcement mechanism protecting against unfair certificates (and even introducing penalization of such cases)

The certificates, if recognized by the insurers, can have influence on the insurance fees.

E3: Cyber resilience testing

1. **The cyber resilience testing process model**

   a) Main actors involved in cyber resilience testing

   Testing could be performed on request of the producer or the user of the component. It could also be ordered by a certifying institution (if the scope of certificate to be issued covers resilience testing).

   If producer is involved in the testing process, it can submit sufficiently detailed documentation of the component together with the results of the routine tests performed in the production process.

   The scope of the tests to be performed should be unambiguously reflected in the Security Profile against which the tests are to be performed.

   If needed, the user of the component should provide access to the target environment where the component is to be installed and used.

   Insurers would be interested in the results of tests to assess the risks of insuring the systems containing such components

   b) Main steps of cyber resilience testing process

   1) *Formal request to perform the tests*
   2) *Analysis of the Security Profile to derive the test cases*
   3) *Preparation of tests*
   4) *Execution of tests*
   5) *Analysis and evaluation of test results*
   6) *Issuing the formal report from testing*

   c) Inputs to the process

   1) *Security Profile*
   2) *The component subjected to tests*
   3) *component documentation*
   4) *The results of manufacturer's tests*
   5) *C1/C2 level certificate if already granted to the component*

   d) Outputs from the process

   1) *Formal resilience testing report*

   e) Testing process standardization

   Should be an extension of compliance assessment process standardization.

   Possible standardization should cover procedural aspects and tool aspects as well. This is an important issue to prevent that different testing procedures and testing environments are applied across by different laboratories performing tests

2. **Change management**

   For planned component changes (e.g. resulting from its roadmap), the full scope of resilience tests should be included into the regression testing suite and performed by the producer before releasing a new version of the component.

   An alternative is that while introducing a new version, the producer is obliged to notify the testing laboratory and the users of the components possibly requesting a renewal of the cyber-security resilience certificate.

It could be also admitted that the producer has the right to introduce some (insignificant) changes without being obliged to renew the certificate but the precise specification of the scope of such 'insignificant' changes can be very hard.

An issue requiring special attention are changes of threats and vulnerabilities related to a component which are then addressed by component changes (for instance, by releasing new patches). Such changes are very difficult to predict and the usual practice is that they are being handled on the reactive base. Re-certification after each such change is practically infeasible. A solution to this problem could be that certification covers not only a component but also the processes of security risk identification (new vulnerabilities, new threats) and analysis related to such component and implemented by its producer and the management of the related changes of the component.

3. **Business model for resilience testing**

Such services could be offered by (accredited) testing laboratories on the commercial basis.

For component producers and users (Critical Infrastructure operators) the cyber-resilience testing certificate can have a business value.

The testing laboratories could offer their services on a commercial base.

The certificates, if recognized by the insurers, can have influence on the insurance fees.

E4: Development and manufacturing process assessment

1. **The development and manufacturing process assessment model**

   a. Main actors involved in development and manufacturing process assessment

   The subject of assessment is the component development/manufacturing process of the producer.

   The assessment and the certificate is to be issued by the Certifying Institution (possibly accredited)

   Insurers can be interested in in setting criteria for such certificates

   Users (Critical Infrastructure operators) can be also interested to have influence on the criteria for such certificates.

   b. Main steps of development process assessment

   1) *Formal request issued by the producer or the user to perform the development/manufacturing process assessment*
   2) *Analysis of the Security Profile to derive the requirements to be checked*
      i. *Assessment of security of the component design process*
      ii. *Assessment of security of the component manufacturing process*
      iii. *Assessment of security of the component packaging and shipping process*
      iv. *Assessment of the quality assurance process of the component*
      v. *Assessment of the configuration management process related to the component*
      vi. *Assessment of the change management process related to the component*
      vii. *Assessment of security of the personnel involved in development/manufacturing*
      viii. *Assessment of the physical security related to development/manufacturing*
   3) *Analysis and evaluation of the results*
   4) *Issuing the certificate*
   5) *Maintaining the certificate validity*

   c. Inputs to the process

   Documentation of development and manufacturing processes

   Availability of the people involved in the processes for interviews

   Onsite audit results

   d. Outputs from the process

      1)Development/manufacturing process security certificate
      2)Rules related to the validity of the certificate

   e. Standardization of development process security assessment

   Some standards could provide a starting point in this respect, for instance:
   - *Building Security In Maturity Model (BSIMM), https://www.bsimm.com/*
   - *ISO/IEC 27034 series Application security http://www.iso27001security.com/html/27034.html*
   - *IEC 62443-4-1 4-1: Secure product development life-cycle requirements*

- *Microsoft Security Development Lifecycle (SDL), https://www.microsoft.com/en-us/sdl/*

2. Change management

This seems to be a very difficult (and potentially costly) problem. Assuring and certifying the development/production processes can involve significant costs and effort which will inevitably be reflected in component prices.

3. Business model for development process assessment

The cost of achieving high security maturity of the development/manufacturing processes can be high and difficult to afford by producers

> *Components with compliance, resilience and process security certificates can be recognized by the Critical Infrastructure operators and therefore can give better business chances for their producers*

> *The certificates, if recognized by the insurers, can have influence on the insurance fees.*

IV. Additional Exercise

The objective of this exercise was to demonstrate that Protection Profile can be used to derive from it the argumentation structure about conformity to the security requirements imposed by the Protection Profile.   Such argumentation structure is called *conformance argument template*. It can be then reused while demonstrating conformity of the components belonging to the family represented by the Protection Profile.

In this exercise we used the Protection Profile for RTU version 2.1. (see Appendix 3). The conformance argument template was developed with the help of the NOR-STA tool developed by Gdansk University of Technology.

Example screenshots of the RTU Protection Profile conformance argumentation template are shown below:
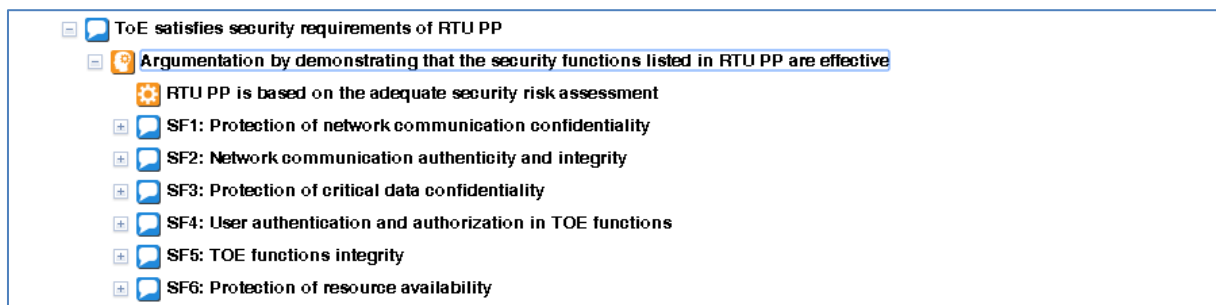
```
SF4: User authentication and authorization in TOE functions
  Argumentation by referring to the Foundational Requirements identified in RTU PP as relevant for this SF
    SFs were selected by 'grounding' them in FRs, following the agreed Guideline
  Requirements retated to FR1: "Identification and authentication control" are satisfied
    Argumentation by referring to the related component requirements from IEC 62443-4-2
      IEC 62443 is an internationally recognized standard supporting selection of security requirements for IACS components
      CR 1.1: Human user identification and authentication
      CR 1.2: Software process and device identification and authentication
      CR 1.3: Account management
      CR 1.4: Identifier management
      CR 1.5: Authenticator management
      CR 1.11: Unsuccessful login attempts
      CR 1.12: System use notification
  Requirements retated to FR2: "Use control" are satisfied
    Argumentation by referring to the related component requirements from IEC 62443-4-2
      IEC 62443 is an internationally recognized standard supporting selection of security requirements for IACS components
      CR 2.1: Authorization enforcement
      CR 2.3: Use control for portable and mobile devices
      CR 2.5: Session lock
      CR 2.6: Remote session termination
      CR 2.7: Concurrent session control
      CR 2.8: Auditable events
      CR 2.9: Audit storage capacity
      CR 2.10: Response to audit processing failures
      CR 2.11: Timestamps
      CR 2.12: Non-repudiation
      CR 2.13: Use of phyasical diagnostic and test interfaces
```

V.   General Comments

1. *From the Critical Infrastructures perspective the primary interest is in cyber-security of systems; components are of less importance (certified components do not imply a certified system).*

2. *In practice it often happens that the meaning of a certification depreciates in time and at some moment such certificate has no business value (in other words, everyone can have such certificate and no one pay attention to it). Therefore the ICCF framework should be supported by some mechanisms preventing such depreciation.*

3. *In practice it is very difficult (if not impossible) to be 'standards agnostic' at the Protection Profile level (not mentioning the Security Profile). To illustrate this we have developed two versions of Protection Profile for RTU (version 1.0 and version 2.1) and we have found that building version 2.1 (which follows the recommendations of IEC 62443-4-2) was more appealing.*

4. *It is not clear if the certificates C1, C2 and B will be recognized by the Operators of Critical Infrastructures. It is likely that they will mostly be interested in the certificate A which covers the full scope of cyber-security assessment (compliance, resilience and process security).*

5. *It seems sensible that the A certificate be differentiated depending on the security level foreseen for the component subjected to certification.*

6. *Change management and maintenance of certificates seems to be a real challenge. To cope with this problem a solution could be making certification a continuous process instead of being it a one-shot activity. This however would require significant changes in current certification practices and an extensive tool support would be inevitable.*

7. *The rules governing development and maintenance of Protection Profiles and   Security Profiles should be imposed by National Cybersecurity Authority*

VI. Appendices

Three Protection Profiles were elaborated by NET-PL, for two different component families. The difference between Protection Profile version 1.0 and Protection Profile version 2.1 is that the latter has stronger reference to IEC 62443-4-2.   In particular, the Security Functions of PP RTU version 2.1 were selected based on the Foundational Requirements defined in IEC 62443-4-2 whereas the Security Functions of PP RTU version 1.0 were selected based on the expertise of the authors of this Protection Profile.

Appendix 1: Protection Profile of a Remote Terminal Unit (RTU), version 1.0

Appendix 2: Protection Profile of fire detection and fire alarm system (FDAS) – Control and Indication Equipment (CIE) in distributed architecture, version 1.0

Appendix 3: Protection Profile of a Remote Terminal Unit (RTU), version 2.1

Appendix 1 of the Final Report by NET-PL

Protection Profile
of a Remote Terminal Unit (RTU)

Version 1.0

Mikronika (NET-PL)

15.09.2017

About this document

This Protection Profile (PP) specifies an implementation-independent set of security requirements associated with a family of products. In the whole document, the acronym FoP (Family of Products) designates the type of components that may be evaluated

This PP is considered during experiments carried out by the Polish National Exercise Team (NET-PL) within Task 3: *ICCF tests run by National Exercise Teams* of the 2017-2018 ICCF Work Plan. For the details of the ICCF project see *Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)* [ICCF]:

(https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC102550_introduction-to-iccf_erncip-iacs-tg-onlineversion.pdf)

1   Family of products description

Family of products: **Remote Terminal Unit** (RTU)

Component type: Embedded device (following IEC 62443-4-2 classification)

1.1   Main features

RTU monitors and controls instruments in SCADA systems used in industrial and critical infrastructure processes, like oil and gas pipelines, electric power generation and transmission, chemical manufacturing, physical and technical security systems, water treatment and many others.

RTU main functions:

1. collecting measurements from sensors,

2. execution of logic and control calculations,

3. user program execution,

4. issuing control commands that modify a process,

5. communicating with external applications and other devices,

6. administration functions to configure or program the other functionalities of the TOE; several administration interfaces are possible:

    a) thick-clients (sometimes also called an administration console),

    b) programming workstation,

    c) web-clients,

    d) removable devices (USB drives, SD memory cards, etc.),

7. local logging (in particular, to log security and administration events),

8. remote logging (in particular, to log security and administration events).

1.2 TOE parts

RTU communicates with sensors and actuators to control the process and also communicates with the supervision system and other RTUs.

Figure 1. TOE in its environment; the diagram shows TOE its interfaces and other relevant objects.

The parts interfacing RTU to its environment are the following:

1. **Control-command of the process**: the interface and process of TOE communication with the supervision system which can control TOE configuration (including modifications of user program logic) and update firmware.

2. **Data exchange between the TOE and the supervision**: the interface and process TOE controls and commands controlled processes by reading inputs and sending commands to actuators.

3. **Data exchange between the TOE and other RTUs**: the interface and process of connected RTUs to exchange data on the controlled processes or for remote logging.

4. **Engineering workstation flow**: the interface and process a user or administrator can connect directly to TOE to operate it, manage its configuration and update.

RTU consists of the following software/data parts, as presented in Figure 2.

Remote Telecontrol Unit (RTU)	
8. User authentication mechanism	10. Access control policy
6. Firmware	7. Configuration
5. Operating system (kernel)	9. User secrets
11. Local logging	13. Local logs
12. Remote logging	14. Remote logs
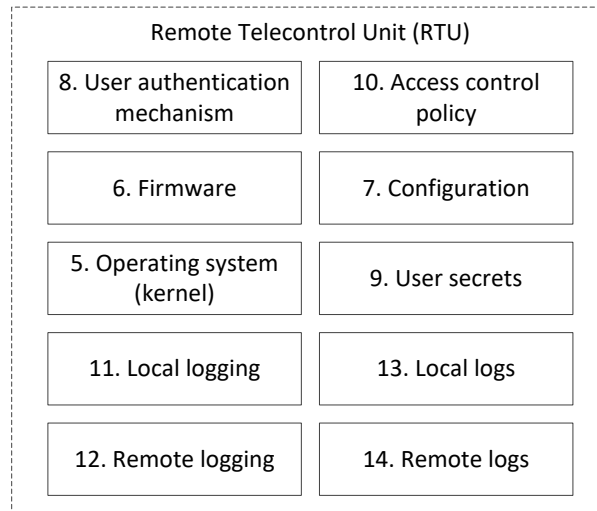
Figure 2. RTU structure

The parts are as follows:

5. **Operating system (kernel)**: the software controlling the hardware of RTU and providing services for firmware

6. **Firmware**: the software layer that manages RTU resources and provides runtime environment for users

7. **Configuration**: user programs and their data running on RTU

8. **User authentication mechanism**: the functionality (software) responsible for authentication of RTU users

9. **User secrets**: the credentials used to authenticate users

10. **Access control policy**: data and programs responsible for user authorization (assigning access rights to authenticated users)

11. **Local logging**: software responsible for logging selected events in accordance with the defined policy

12. **Local logs**: repositories keeping the logged data

13. **Remote logging**: software responsible for sending/receiving logging data to/from other devices (RTUs and the supervision system)

14. **Remote logs**: repositories for logging data received from other devices

1.3 Assumptions

The following assumptions are assumed for the TOE environment.

1. TOE is placed in a non-secured physical location.

2. TOE is placed in a physical environment that meets the vendor's specifications for temperature, humidity, and other environmental factors.

3. TOE will be provided with power that meets its required specifications.

4. TOE is installed within the network enabling access to all devices and systems it should communicate with.

5. Users being authenticated via passwords or other means effectively secure their credentials against access by any unauthorized subjects.

2 Critical assets

Following [ICCF] critical assets are the critical security characteristics of the parts of TOE.

2.1 Security characteristics

The required security characteristics of TOE are as follows:

- **Availability** – property of ensuring timely and reliable access to and use of information and functionality (IEC 62443-1-1)

- **Confidentiality** – assurance that an information is not disclosed to unauthorized individuals, processes, or devices (IEC 62443-1-1)

- **Integrity** – logical completeness of the hardware and software, consistency of the data structures and occurrence of the stored data (IEC 62443-1-1)

- **Authenticity** - truthfulness of origins and attributes

2.2 Critical assets of the environment

In the following table, the critical assets are identified by the 'x' symbol in the entry of the table given below.

Table 1. Critical assets of TOE environment

Security characteristic / Part	Availability	Confidentiality	Integrity	Authenticity
1. Control-command of the process interface	x		x	x
2. Data exchange between the ToE and the supervision interface	x	x	x	x
3. Data exchange between the ToE and other RTUs interface	x	x	x	x
4. Engineering workstation flow interface		x	x	x

Rationale:

1. **Control-command of the process interface**: The Availability, Integrity and Authenticity of the actions performed through this interface must be protected.

2. **Data exchange between the TOE and the supervision interface**: The Availability, Integrity and Authenticity of the data exchange between the TOE and the supervision must be protected.

3. **Data exchange between the TOE and other RTUs interface**: The Availability, Integrity and Authenticity of the exchange between the TOE and other RTUs must be protected.

4. **Engineering workstation flow interface**: The flow between the TOE and the engineering workstation must be protected concerning its Integrity, Confidentiality and Authenticity.

2.3 TOE critical assets

In the following table, the critical assets are identified by the 'x' symbol in the entry of the table given below.

Table 2. Critical assets of TOE

Security characteristic / Part	Availability	Confidentiality	Integrity	Authenticity
5. Operating system (kernel)			x	x
6. Firmware		x	x	x
7. Configuration		x	x	x
8. User authentication mechanism			x	x
9. User secrets		x	x	
10. Access control policy			x	
11. Local logging	x			
12. Remote logging	x			
13. Local logs			x	x
14. Remote logs			x	x

Rationale:

5. **Operating system (kernel)**: The OS must be protected concerning its Integrity and and Authenticity.

6. **Firmware**: In order to work properly, the firmware must be protected concerning its Integrity, Availability and Authenticity.

7. **Configuration**: The configuration of the TOE must be protected concerning its Confidentiality, Integrity and Authenticity. The attacker must not be able to discover the configuration of the TOE by other means than the ToE activity. Configuration includes also program logic.

8. **User authentication mechanism**: This mechanism can be based on a local database or on a remote authentication server. In both cases, Integrity, Availability and Authenticity of the mechanism must be protected.

9. **User secrets**: The user secrets can be passwords, certificates etc.. They can be stored in the TOE or stored in a remote authentication server. In all cases Integrity and Confidentiality of these credentials must be protected.

10. **Access control policy**: The policy can be stored locally or remotely on an authentication server. In both cases, Integrity of the access control policy must be protected.

11. **Local logging**: Once configured, the local logging must remain operational, i.e. its Availability must be protected

12. **Remote logging**: The TOE is capable of remote logging. Once configured, the logging must remain operational, i.e. its Availability must be protected.

13. **Local logs**: The Integrity of the local logs must be protected.

14. **Remote logs**: Integrity and Authenticity of the remote logs entries submitted by the TOE must be protected. (for instance, a mechanism must be present to detect the absence of a message in a sequence of properly received messages).

3   Threat Model

3.1   Attackers

The following attackers are considered:

1. **Attacker on the supervision network**: The attacker controls a device plugged to the supervision network of the TOE (Part 2. Data exchange between the TOE and the supervision interface).

2. **Attacker on the process network**: The attacker controls a device plugged to the process network (Part 1. Control-command of the process interface).

3. **Evil user**: The attacker has compromised an unprivileged account and tries to bypass the access control policy of the TOE.

4. **Attacker with physical access to the TOE**: The attacker has physical access to the TOE.

3.2   Threats

The following threats have been identified:

1. **Denial of service**: The attacker manages to generate a denial of service on the TOE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file). This denial of service can affect the whole TOE or only some of its functions.

2. **Operating system / firmware alteration**: The attacker manages to inject and run a corrupted OS / firmware on the TOE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install an update on the TOE by legitimate means. Finally, the attacker manages to modify the version of the OS / firmware installed on the TOE without having the privilege to do so.

3. **Configuration compromise**: The attacker manages to obtain some parts of the TOE configuration by other means than the observation of the activity of the TOE.

4. **Configuration alteration**: The attacker manages to modify, temporarily or permanently, the TOE configuration.

5. **Credentials theft**: The attacker manages to steal user or other credentials.

6. **Authentication violation**: The attacker manages to authenticate itself without credentials.

7. **Access control violation**: The attacker manages to obtain permissions that he does not normally have.

8. **Local logs alteration**: The attacker manages to delete or modify a local log entry without being authorized by the access control policy of the TOE.

9. **Remote logs alteration**: The attacker manages to delete or modify a remote log entry without the receiver (the component hosting the log) being able to notice it.

10. **Parameters or command injection**: The attacker manages to modify parameters in the TOE configuration or to transmit commands (through the Control-command of the process interface) without being authorized.

11. **Flows alteration**: The attacker manages to corrupt exchanges between the TOE and an external component without being detected.

12. **Flows compromise**: In case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the TOE and the supervision or other RTU.

4 Critical assets vs. threats

The table below presents the relationship between the threats and the critical assets affected directly by these threats. Considering Security Profile for a specific device one should consider also indirect impact of threats on TOE parts. For example flow compromise may compromise confidentiality of user secrets.

Table 3. Critical assets affected by the threats

Threats \ Parts	1. Control-command of the process interface	2. Data exchange between the ToE and the supervision interface	3. Data exchange between the ToE and other RTUs interface	4. Engineering workstation flow interface	5. Operating system (kernel)	6. Firmware	7. Configuration	8. User authentication mechanism	9. User secrets	10. Access control policy	11. Local logging	12. Remote logging	13. Local logs	14. Remote logs
1. Denial of service	Av	Av	Av	Av							Av	Av		
2. Operating system / firmware alteration					I, Au	I, Au								
3. Configuration compromise							C							
4. Configuration alteration							I, Au							
5. Credentials theft									C					
6. Authentication violation								I, Au						
7. Access control violation									C	I				
8. Local logs alteration													I, Au	
9. Remote logs alteration														I, Au
10. Parameters or command injection	I, Au	I, Au	I, Au											
11. Flows alteration	I, Au	I, Au	I, Au	I, Au										
12. Flows compromise		C	C	C										

Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity

5 Security functions

Security functions are intended to protect critical assets against the threats. They correspond to Foundational Requirements (FR) of IEC 62443-4-2 specific to the type of critical assets and identified threats.

The following security functions are considered:

1. **Malformed input management**: The TOE has been developed in order to handle correctly malformed input, in particular malformed network traffic. The security function ensures that any malformed input will have minimal effect on availability of any other services or functions.

    a) This function corresponds to FR3 *System integrity* and FR7 *Resource availability*

2. **Secure storage of secrets**: User and other secrets are securely stored in the TOE. In particular, the compromise of a file is not sufficient for retrieving them.

    a) This function corresponds to FR3 *System integrity* and FR4 *Data confidentiality*

3. **Secure authentication on administration interface**: Required credentials ensure strong protection. Function prevents brute force attacks. The identity and the permissions of the user account are systematically checked before any privileged action.

    a) Note: secure authentication from remote devices depends on security function 8 "Secure communication"

    b) This function corresponds to FR1 *Identification and authentication control* and FR4 *Data confidentiality*

4. **Access control policy**: The access control policy, based on RBAC (role-based access control) is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

    a) This function corresponds to FR2 *Use control* and FR3 *System integrity*

5. **Firmware signature**: At each update of the firmware, the integrity and authenticity of the new firmware are checked before updating. The integrity and authenticity of the firmware are also checked at boot time.

    a) This function corresponds to FR3 *System integrity* and FR4 *Data confidentiality*

6. **Configuration access control**: The access control prevents any unauthorized person to read or modify the configuration of the TOE.

    a) This function corresponds to FR2 *Use control,* FR3 *System integrity* and FR4 *Data confidentiality*

7. **Command authorization**: The TOE must ensure that only authorized command can be executed by TOE.

    a) This function corresponds to FR2 *Use control*

8. **Secure communication**: The TOE supports secured communication, protected in integrity and authenticity. If required, confidentiality is enforced with external components. Session tokens are protected against hijacking and replay. They have a short lifespan.

    a) *This function corresponds to* FR1 *Identification and authentication control*, FR4 *Data confidentiality* and FR5 *Restricted data flow*

9. **Logs integrity**: The integrity of the generated local logs is ensured and only the superadministrator is permitted to modify them.

    a) This function corresponds to FR2 *Use control*

10. **Remote log protection**: The TOE supports secure remote logging where authenticity and integrity are ensured. The transmission is also protected against replay and a mechanism is implemented for detecting missing logs.

    a) *This function corresponds to FR4 Data confidentiality*

6 Threats vs security functions rationale

Table 4. Protection against threats provided by the security functions

Security functions	1. Denial of service	2. Operating system / firmware alteration	3. Configuration compromise	4. Configuration alteration	5. Credentials theft	6. Authentication violation	7. Access control violation	8. Local logs alteration	9. Remote logs alteration	10. Parameters or command injection	11. Flows alteration	F12. lows compromise
1. Malformed input management	x									x		
2. Secure storage of secrets					x							
3. Secure authentication on administration interface				x	x	x	x					
4. Access control policy		x										
5. Firmware signature		x										
6. Configuration access control			x	x								
7. Command authorization										x		
8. Secure communication					x					x	x	x
9. Logs integrity								x				
10. Remote log protection									x			

Symbol 'x' in the table entry identifies that the critical function protects against given threat).

7 Component requirements

Security functions have been mapped to corresponding IEC 62443-4-2 requirements.

Note: satisfaction of IEC 62443-4-2 requirements does not mean that security functions objectives are met.

Table 5. Security requirements

Security function	IEC 62443-4-2 requirement	
1. Malformed input management	CR 3.5	Input validation
	CR 7.1	Denial of service protection
	CR 7.2	Resource management
2. Secure storage of secrets	CR 3.11	Physical tamper resistance and detection
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography

Security function	IEC 62443-4-2 requirement	
3. Secure authentication on administration interface	CR 1.1	Human user identification and authentication
	CR 1.2	Software process and device identification and authentication
	CR 1.3	Account management
	CR 1.4	Identifier management
	CR 1.5	Authenticator management
	CR 1.7	Strength of password-based authentication
	CR 1.8	Public key infrastructure certificates
	CR 1.9	Strength of public key authentication
	CR 1.10	Authenticator feedback
	CR 1.11	Unsuccessful login attempts
	CR 1.12	System use notification
	CR 1.14	Strength of symmetric key authentication
	CR 4.3	Use of cryptography
4. Access control policy	CR 2.1	Authorization enforcement
	CR 2.5	Session lock
	CR 2.6	Remote session termination
	CR 2.7	Concurrent session control
	CR 3.9	Protection of audit information
5. Firmware signature	CR 3.4	Software and information integrity
	CR 3-10	Support for updates
	CR 3-14	Integrity of boot process
	CR 4.3	Use of cryptography
6. Configuration access control	CR 2.1	Authorization enforcement
	CR 3.4	Software and information integrity
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography
7. Command authorization	CR 2.1	Authorization enforcement
	CR 2-5	Session lock
	CR 2.12	Non-repudiation
8. Secure communication	CR 1.1	Human user identification and authentication
	CR 1.2	Software process and device identification and authentication
	CR 3.1	Communication integrity
	CR 3.8	Session integrity
	CR 4.1	Information confidentiality
	CR 5.1	Network segmentation
	CR 4.3	Use of cryptography
	CR 7.6	Network and security configuration settings
9. Logs integrity	CR 2.1	Authorization enforcement
10. Remote log check	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography

Appendix 2 of the Final Report by NET-PL

Protection profile of fire detection and fire alarm systems (FDAS) –

Control and indication equipment (CIE) in distributed architecture

Version 1.0

Polon-Alfa (NET-PL)

20.03.2018

About this document

This Protection Profile (PP) specifies an implementation-independent set of security requirements associated with a family of products. In the whole document, the acronym FoP (Family of Products) designates the type of components that may be evaluated

This PP is considered during experiments carried out by the Polish National Exercise Team (NET-PL) within Task 3: *ICCF tests run by National Exercise Teams* of the 2017-2018 ICCF Work Plan. For the details of the ICCF project see *Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)* [ICCF]:

(https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC102550_introduction-to-iccf_erncip-iacs-tg-onlineversion.pdf)

1   Family of products description

Family of products: **Control and indication equipment (CIE)**

Context of use: Fire detection and fire alarm systems (FDAS)

Component type: Embedded device (following IEC 62443-4-2 classification)

1.1   General description

The addressable, interactive CIE fire alarm system is a set of latest technology equipment, designed for very fast detection and signaling of fire, precise indication of fire origin, control of fire protection safety devices, and information of appropriate intervention services or building guards about fire. It enables protection of mid-size, large and very large facilities, especially so called "intelligent" buildings with huge amount of fire protection safety devices. CIE can be easily integrated with many existing building management systems. Due to its specific features it enables to arrange perfect set of necessary devices, well-fitted to building conditions.

All devices of the CIE meet requirements of EN 54 European Standard.

1.2   Features

The CIE includes the following features:

- **Detectors and manual call points management**: The CIE is able to read states detectors and manual call points.

- **Input/output management**: The CIE is able to read local or remote inputs and to write local or remote outputs. The I/O can be digital or analog. These I/O allows the CIE controlling and commanding the fire protection equipment.

- **User scenario execution in case of fire risk**: The application in CIE runs a user scenario. This scenario processes the inputs and updates the outputs to fire protection devices.

- **Communication with the supervision**: The CIE communicate with the BMS (Building Management System) for transmitting process data.

- **Administration functions**: The CIE administration functions in order to configure CIE for proper operation according to a programmed fire scenario or program the other functionalities of the CIE. Several administration interfaces are possible:

  — Thick-clients (administration console, programming workstation …);

  — Removable devices (USB drives, SD memory cards, etc).

- **Local logging**: The CIE supports the configuration of a local logging policy. It is possible in particular, to log security and administration events and fire alarm system events.

- **Remote logging**: The CIE supports the configuration of a remote logging policy. It is possible in particular, to log security and administration events and fire alarm system events.

1.3   Product usage

The CIE can be used in diverse architecture.

One of them is **distributed architecture**. It consists of many unified modules of various types, installed inside standardized cabinets. Cabinets can be arranged as separate units or combined in sets (so called nodes) and can be located in different places of protected building, even if those locations are distant. All modules within one node and nodes between themselves are connected with a common, doubled (redundancy) digital communication bus. Each control panel can be flexibly assembled with modules and nodes well-fitted to individual building requirements. Such solution enables the arrangement of the control panel equipment, installed in required locations. This provides maximum optimization of the system, reduction of cost of installation while the system is still extremely reliable and functional. All that is possible thanks to implementation of doubled main processor controllers, communication buses and cable connections between nodes. Operator panels and modules are installed inside the cabinets with standard dimensions, which can be mechanically connected.

The communication between nodes is provided by means of doubled cable connection (for example RS-485) or doubled fiber optic cables. Each node shall be equipped – depending on the size of node and expected current consumption – with one or more supply modules. Each node can contain line modules with connected detection lines, input-output modules for direct control or supervision of fire safety devices. In each external node the operator panel can be implemented, acting as the parallel operation panel.

The model range detectors are the analogue detectors with programmable sensitivity (from the control panel level). This ability enables adjustment of fire detection response time to the phenomena occurring in detector vicinity. All detectors are equipped with automatic sensitivity self-compensation mechanism that maintains constant sensitivity during progressing dirt build-up in the measuring chamber and also during changes of air pressure and vapor condensation. The applied built-in microprocessor and the proper detector

software guarantee that the entire fire phenomenon within the vicinity of the detector will be analyzed quickly and false alarms will be eliminated.

The CIE firmware updates and user configuration can, in general, be loaded on the CIE through the network, thanks to a serial bus or a removable device (SD memory cards, USB keys instance).

This network should be physically isolated from other networks or, at least, logically isolated. In practice, an engineering workstation is often plugged on the supervision network. This engineering workstation should not be permanently plugged but only when it is necessary.

FDAS architecture and functionality is shown on figure 1.
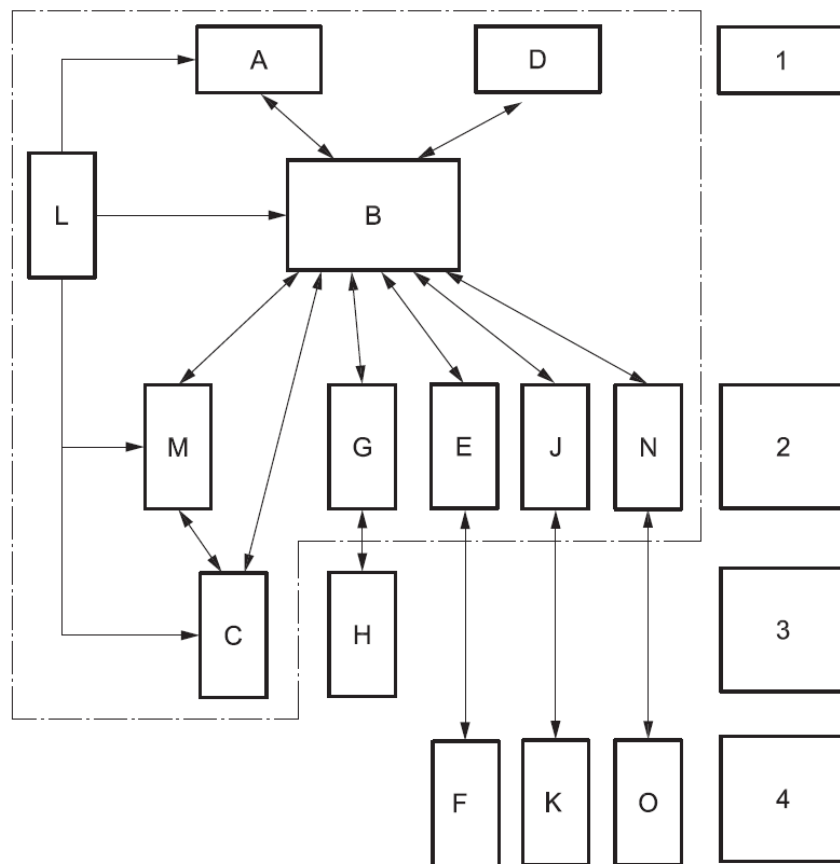
Key

1	detection and activation functions	G	control function for fire protection system or equipment
2	control functions for actions	H	fire protection system or equipment
3	local associated functions	J	fault warning routing function
4	remote associated functions	K	fault warning receiving function
A	automatic fire detection function	L	power supply function
B	control and indication function (**CIE**)	M	control and indication function for alarm annunciation
C	fire alarm function	N	ancillary input or output function
D	manual initiating function	O	ancillary management function
E	fire alarm routing function	⟷	exchange of information between functions
F	fire alarm receiving function		

NOTE   The functions that are included within the FDAS are shown inside the dotted line.

Figure 1 — Fire detection and fire alarm system and associated systems, functions and equipment (source: EN 54-1)

1.4 Users

European Standard EN 54-2 defines access levels for the indications and controls relating to functions. In some cases alternatives are offered (e.g. AL1 or AL2). This is because either may be appropriate in different operational circumstances. The purpose of the different access levels is not specified in EN 54-2. However, in general they are expected to be used as follows:

- **AL1**: For use by members of the general public, or persons having a general responsibility for safety supervision, who might be expected to investigate and initially respond to a fire alarm or a fault warning.

- **AL2**: For use by persons having a specific responsibility for safety, and who are trained and authorized to operate the CIE in the:
    - quiescent condition;
    - fire alarm condition;
    - fault warning condition;
    - disabled condition;
    - test condition (when provided).

- **AL3**: For use by persons who are trained and authorized to:
    - re-configure the site-specific data held within the CIE or controlled by it (e.g. labelling, zoning, alarm organization);
    - maintain the CIE in accordance with the manufacturer's published instructions and data.

- **AL4**: For use by persons who are trained and authorized by the manufacturer either to repair the CIE, or to alter the electronic circuitry or the program, thereby changing its basic mode of operation.

1.5 Assumptions

Assumptions on the environment and the use case of the CIE are the following:

- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the CIE.

- **Administrators:** CIE administrators are competent, trained and trustworthy.

- **Premises:** The CIE is not necessarily in secured premises and the attacker can have access to all physical interfaces of the CIE. Similarly, the attacker can plug a trapped device (for instance, a USB drive or a SD card) on any physical port of the CIE. Conversely, the attacker cannot disassemble the CIE or perform physical attacks on it. Since identical products to the CIE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.

- **Unevaluated services disabled by default:** Services of the CIE which are not covered by the security target are disabled in the default configuration (also named factory standard configuration).

- **Security documentation:** The CIE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization.

All recommendations included in this documentation are applied prior to the evaluation.

2 Critical assets

2.1 Critical assets of the environment

The critical assets of the environment are the following:

- **Control fire detection and fire alarm system process**: The CIE controls a fire detection and fire alarm system process by reading states of detectors and manual call points. The availability and integrity of these actions must be protected.

- **Control-command of the fire protection system process**: The CIE controls and commands a fire protection equipment system process by reading inputs and sending commands to outputs. The availability and integrity of these actions must be protected.

- **Data exchanges between the CIE and the supervision**: The integrity and authenticity of the exchanges between the supervision and the CIE must be protected.

- **Engineering workstation flows**: The flows between the CIE and the engineering workstation must be protected in integrity, confidentiality and authenticity.

- **Data exchanges between the CIE and another Control Indication Equipment:** For the communication between the CIE and another Control Indication Equipment, the use of dedicated I/O should be prefered. In the case where these exchanges should transit on a mutualized infrastructure, they must be protected in integrity and authenticity.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Control fire detection and fire alarm system process	X		X	
Control-command of the fire protection system process	X		X	
Data exchanges between the CIE and the supervision			X	X
Engineering workstation flows		O	X	X
Data exchanges between the CIE and another Control Indication Equipment			X	X

X: mandatory, O: optional

2.2   CIE critical assets

The critical assets of the CIE are the following:

- **Firmware**: In order to work properly, the firmware must be protected both in integrity and authenticity.

- **User scenario**: The CIE runs a scenario written and loaded by the users. Its integrity, confidentiality and authenticity must be protected.

- **Configuration**: The configuration of the CIE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the CIE by other means than the CIE activity.

- **Execution mode**: The integrity and authenticity of the execution mode of the CIE must be protected.

- **User authentication mechanism:** This mechanism can be based on a local database or on a remote authentication server. In both cases, the CIE must ensure the integrity and authenticity of the mechanism.

- **User secrets:** The user secrets can be passwords, certificates, etc. They can be stored in the CIE or stored in a remote authentication server. In all cases, the CIE must ensure the integrity and confidentiality of these credentials.

- **Access control policy:** The policy can be stored locally or remotely on a authentication server. In both cases, the CIE must ensure the integrity of the access control policy.

- **Local logging:** Once configured, the local logging must remain operational.

- **Remote logging:** The CIE is capable of remote logging. Once configured, the logging must remain operational.

- **Local logs:** The integrity of the local logs must be ensured by the CIE.

- **Remote logs:** The remote logs generated by the CIE must be protected in integrity and authenticity. A mechanism must be present to detect the absence of a message in a sequence of properly received messages.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
User scenario		O	X	X
Configuration		O	X	
Execution mode			X	
User authentication mechanism			X	X
User secrets		O	X	
Access control policy			X	
Local logging	X			
Remote logging	X			
Local logs			X	X
Remote logs			X	X

X: mandatory, O: optional

3   Threat Model

3.1   Attackers

The following attackers are considered:

- **Attacker on the supervision network**: The attacker controls a device plugged on the supervision network of the CIE.

- **Attacker on the process network (fire protection system)**: The attacker control a device plugged on the field fire protection system network.

- **Evil user**: The attacker has compromised an unprivileged account and tries to bypass the access control policy of the CIE.

3.2   Threats

The following threats are considered:

- **Denial of service:** The attacker manages to generate a denial of service on the CIE by performing an unexpected action or by exploiting a vulnerability.

- **Firmware alteration:** The attacker manages to inject and run a corrupted firmware on the CIE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install that update on the CIE by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the CIE without having the privilege to do so.

- **Execution mode alteration:** The attacker manages to modify the execution mode of the CIE without being authorized.

- **User scenario compromise:** The attacker manages to obtain some parts of the scenario configuration of the CIE by other means than the observation of the activity of the CIE.

- **User scenario alteration:** The attacker manages to modify, temporarily or permanently, the user scenario.

- **Configuration alteration:** The attacker manages to modify, temporary or permanently, the CIE configuration.

- **Configuration compromise:** The attacker manages to illegally obtain some parts of the CIE configuration.

- **Credentials theft:** The attacker manages to steal user credentials.

- **Authentication violation:** The attacker succeeds in authenticating himself without credentials.

- **Access control violation:** The attacker manages to obtain permissions that he does not normally have.

- **Local logs alteration:** The attacker manages to delete or modify a local log entry without being authorized by the access control policy of the CIE.

- **Remote logs alteration:** The attacker manages to modify a remote log entry without the receiver being able to notice it. The attacker manages to delete a remote log message without the receiver being able to notice it.

- **Parameters or command injection:** The attacker manages to modify parameters in the CIE or to transmit commands without being authorized.

- **Flows alteration:** The attacker manages to corrupt exchanges between the CIE and an external component (detectors, manual call points, I/O devices) without being detected.

- **Flows compromise:** In case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the CIE and an external component (detectors, manual call points, I/O devices).

4 Critical assets vs threats

Critical assets → vs threats ↓	Control fire detection and fire alarm system process	Control-command of the fire protection system process	Data exchanges between the CIE and the supervision	Engineering workstation flows	Data exchanges between the CIE and another Control Indication Equipment	Firmware	User scenario	Configuration	Execution mode	User authentication mechanism	User secrets	Access control policy	Local logging	Remote logging	Local logs	Remote logs
Denial of service	Av	Av											Av	Av		I Au
Firmware alteration						I Au										
Execution mode alteration									I							
User scenario compromise							(C)									
User scenario alteration		I					I Au									
Configuration alteration								I								
Configuration compromise								(C)								
Credentials theft											I C					
Authentication violation										I Au						
Access control violation												I				
Local logs alteration															I Au	
Remote logs alteration																
Parameters or command injection	Av I	Av I	I Au													
Flows alteration	Av I	Av I	I Au	I Au	I Au											
Flows compromise			(C)													
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity, (…): optional																

5 Security functions

The following security functions are considered:

- **Malformed detectors/manual call points management:** The CIE has been developed in order to handle correctly malformed states of detectors and manual call points, in particular malformed network traffic.

- **Malformed inputs management:** The CIE has been developed in order to handle correctly malformed inputs, in particular malformed network traffic.

- **Secure storage of secrets:** User secrets are securely stored in the CIE. In particular, the compromise of a file is not sufficient for retrieving them.

- **Secure authentication on administration interface:** The identity and the permissions of the user account are systematically checked before any privileged action (AL1 – AL4).

- **Access control policy:** The access control policy is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

- **Firmware signature:** At each update of the firmware, the integrity and authenticity of the new firmware are checked before updating. The integrity and authenticity of the firmware are also checked at boot time.

- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the CIE.

- **Integrity and authenticity of the user scenario configuration:** The CIE ensure the integrity of the user scenario configuration. Only authorized users (AL3-AL4) can modify it.

- **Confidentiality of the user scenario configuration:** The CIE protects the confidentiality of the user scenario configuration. Only authorized users (AL3-AL4) can access it.

- **Integrity and authenticity of commands to output:** The CIE must ensure that the execution mode of the CIE can only be modified by authorized users. This implies, in particular, that they are authenticated.

- **Secure communication:** The CIE supports secured communication to BMS, protected in integrity and authenticity. If required, confidentiality is enforced with external components.

- **Logs integrity:** The integrity of the generated local logs is ensured and only the super administrator is permitted to modify them.

- **Alarms integrity:** The CIE supports secure remote logging where authenticity and integrity are ensured. The transmission is also protected against replay and a mechanism is implemented for detecting missing logs.

6   Threats vs security functions

Threats → vs security functions ↓	Denial of service	Firmware alteration	Execution mode alteration	User scenario compromise	User scenario alteration	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration	Parameters or command injection	Flows alteration	Flows compromise
Malformed detectors/manual call points management	X														
Malformed inputs management	X														
Secure storage of secrets								X							
Secure authentication on administration interface						X	X	X	X						
Access control policy										X					
Firmware signature	X														
Configuration confidentiality and integrity						X	X								
Integrity and authenticity of the user scenario configuration					X										
Confidentiality of the user scenario configuration				X											
Integrity and authenticity of commands to output			X												
Secure communication													X	X	X
Logs integrity											X				
Alarms integrity												X			

7 Component requirements

Security functions have been mapped to corresponding IEC 62443-4-2 requirements.

Note: satisfaction of IEC 62443-4-2 requirements does not mean that security functions objectives are met.

Security function	IEC 62443-4-2 requirement	
Malformed detectors/manual call points management	CR 3.5	Input validation
	CR 3.6	Deterministic output
	CR 3.7	Error handling
Malformed inputs management	CR 3.5	Input validation
	CR 7.1	Denial of service protection
	CR 7.2	Resource management
Secure storage of secrets	CR 3.11	Physical tamper resistance and detection
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography
Secure authentication on administration interface	CR 1.1	Human user identification and authentication
	CR 1.2	Software process and device identification and authentication
	CR 1.3	Account management
	CR 1.4	Identifier management
	CR 1.5	Authenticator management
	CR 1.7	Strength of password-based authentication
	CR 1.8	Public key infrastructure certificates
	CR 1.9	Strength of public key authentication
	CR 1.10	Authenticator feedback
	CR 1.11	Unsuccessful login attempts
	CR 1.12	System use notification
	CR 1.14	Strength of symmetric key authentication
	CR 4.3	Use of cryptography
Access control policy	CR 2.1	Authorization enforcement
	CR 2.5	Session lock
	CR 2.6	Remote session termination
	CR 2.7	Concurrent session control
	CR 3.9	Protection of audit information
Firmware signature	CR 3.4	Software and information integrity
	CR 3-10	Support for updates
	CR 3-14	Integrity of boot process
	CR 4.3	Use of cryptography
Configuration confidentiality and integrity	CR 2.1	Authorization enforcement
	CR 3.4	Software and information integrity
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography
Integrity and authenticity of the user scenario configuration	CR 2.1	Authorization enforcement
	CR 2-5	Session lock
	CR 2.12	Non-repudiation

Protection profile of fire detection and fire alarm systems – Control and indication equipment
in distributed architecture

Security function	IEC 62443-4-2 requirement	
Confidentiality of the user scenario configuration	CR 2.1	Authorization enforcement
	CR 3.4	Software and information integrity
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography
Integrity and authenticity of commands to output	CR 2.1	Authorization enforcement
	CR 3.5	Input validation
	CR 3.6	Deterministic output
	CR 3.7	Error handling
	CR 7.2	Resource management
	CR 7.5	Emergency power
	CR 7.7	Least functionality
Secure communication	CR 1.1	Human user identification and authentication
	CR 1.2	Software process and device identification and authentication
	CR 3.1	Communication integrity
	CR 3.8	Session integrity
	CR 4.1	Information confidentiality
	CR 5.1	Network segmentation
	CR 4.3	Use of cryptography
	CR 7.6	Network and security configuration settings
Logs integrity	CR 2.1	Authorization enforcement
	CR 4.1	Information confidentiality
	CR 4.3	Use of cryptography
Alarms integrity	CR 3.1	Communication integrity
	CR 3.6	Deterministic output
	CR 3.7	Error handling
	CR 3.9	Protection of audit information
	CR 4.1	Information confidentiality
	CR 4.2	Information persistence
	CR 4.3	Use of cryptography

Appendix 3 of the Final Report by NET-PL

Protection Profile
of a Remote Terminal Unit (RTU)

Version 2.1

NET-PL: Mikronika, GUT

17.10.2017

About this document

This Protection Profile (PP) specifies a family of products that may be considered a Target of Evaluation (TOE) during cyber-security evaluation.

This PP is considered during experiments carried out by the Polish National Exercise Team (NET-PL) within Task 3: *ICCF tests run by National Exercise Teams* of the 2017-2018 ICCF Work Plan. For the details of the ICCF project see *Introduction to the European IACS components Cybersecurity Certification Framework (ICCF):* (https://erncip-project.jrc.ec.europa.eu/sites/default/files/ JRC102550_introduction-to-iccf_erncip-iacs-tg-onlineversion.pdf)

The Protection Profile can be applied for conformance with any security standard however some parts of this document refer to the requirements of IEC 62443 series of standards.

- sections 1 to 4 are independent from any security standard;
- sections 5 and 6 refer to Foundational Requirements specified in IEC 62443-1-1;
- section 7 refers to Component Requirements specified in IEC 62443-4-2.

1 Family of products description

Family of products: **Remote Terminal Unit** (RTU)

Component type: Embedded device (following IEC 62443-4-2 classification)

1.1 Main features

RTU monitors and controls instruments in SCADA systems used in industrial and critical infrastructure processes, like oil and gas pipelines, electric power generation and transmission, chemical manufacturing, physical and technical security systems, water treatment and many others.

RTU main functions:

1. collecting measurements from sensors,
2. execution of logic and control calculations,
3. user program execution,
4. issuing control commands that modify a process,
5. communicating with external applications and other devices,
6. administration functions to configure and/or program other functionalities of the RTU (several administration interfaces are possible):
    a) thick-client (sometimes also called an administration console),
    b) programming workstation,
    c) web-clients,
    d) removable devices (USB drives, SD memory cards, etc.),

7. local logging (in particular, to log security and administration events),

8. remote logging (in particular, to log security and administration events).

1.2 TOE parts

RTU communicates with sensors and actuators to control the process and also communicates with the supervision system and other RTUs.
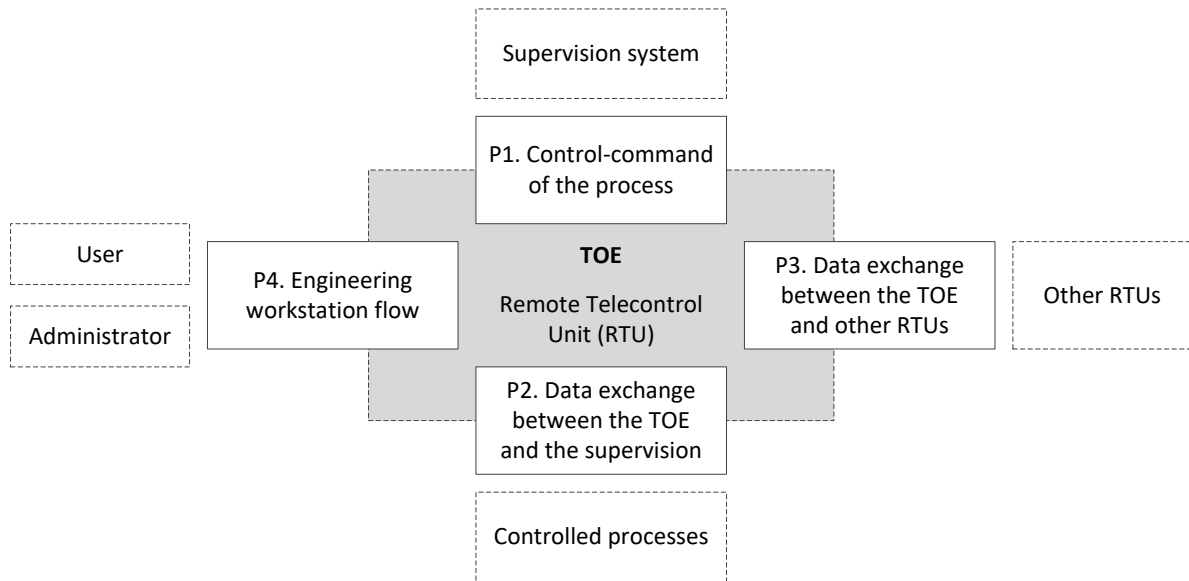

Figure 1. TOE in its environment; the diagram shows TOE, its interfaces and other relevant objects.

The parts interfacing RTU to its environment are the following:

P1. **Control-command of the process**: the interface and process of TOE communication with the supervision system which can control TOE configuration (including modifications of user program logic) and update firmware.

P2. **Data exchange between the TOE and the supervision**: the interface and process TOE controls and commands controlled processes by reading inputs and sending commands to actuators.

P3. **Data exchange between the TOE and other RTUs**: the interface and process of connected RTUs to exchange data on the controlled processes or for remote logging.

P4. **Engineering workstation flow**: the interface and process a user or administrator can connect directly to TOE to operate it, manage its configuration and update.

RTU consists of the following firmware/software/data parts, as presented in Figure 2.
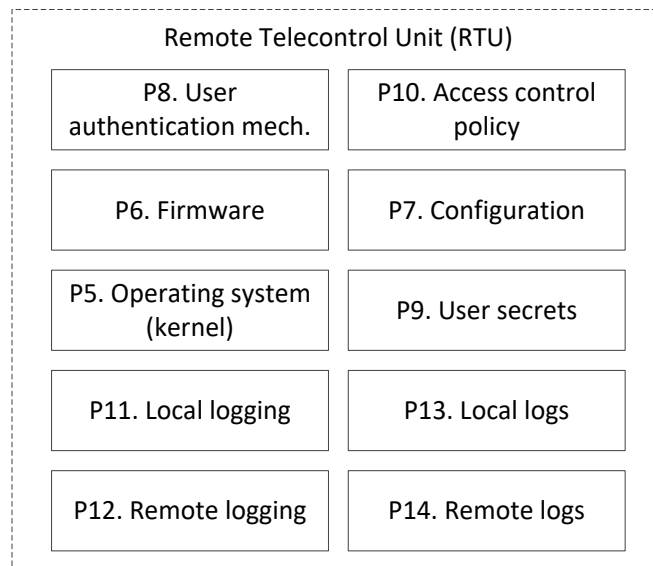

Figure 2. RTU structure

The parts are as follows:

P5. **Operating system (kernel)**: the software controlling the hardware of RTU and providing services for firmware

P6. **Firmware**: the software layer that manages RTU resources and provides runtime environment for users

P7. **Configuration**: user programs and their data running on RTU

P8. **User authentication mechanism**: the functionality (software) responsible for authentication of RTU users

P9. **User secrets**: the credentials used to authenticate users

P10. **Access control policy**: data and programs responsible for user authorization (assigning access rights to authenticated users)

P11. **Local logging**: software responsible for logging selected events in accordance with the defined policy

P12. **Local logs**: repositories keeping the logged data

P13. **Remote logging**: software responsible for sending/receiving logging data to/from other devices (RTUs and the supervision system)

P14. **Remote logs**: repositories for logging data received from other devices

1.3 Assumptions

The following assumptions are assumed for the TOE environment.

1. TOE is placed in a non-secured physical location.

2. TOE is placed in a physical environment that meets the vendor's specifications for temperature, humidity, and other environmental factors.

3. TOE will be provided with power that meets its required specifications.

4. TOE is installed within the network enabling access to all devices and systems it should communicate with.

5. Users being authenticated via passwords or other means effectively secure their credentials against access by any unauthorized subjects.

2 Critical assets

Following [ICCF] critical assets are the critical security characteristics of the parts of TOE.

2.1 Security characteristics

The required security characteristics of TOE are as follows:

− **Availability** – property of ensuring timely and reliable access to and use of information and functionality (IEC 62443-1-1)

− **Confidentiality** – assurance that an information is not disclosed to unauthorized individuals, processes, or devices (IEC 62443-1-1)

− **Integrity** – logical completeness of the hardware and software, consistency of the data structures and occurrence of the stored data (IEC 62443-1-1)

− **Authenticity** - truthfulness of origins and attributes

2.2 Critical assets of the environment

In the following table, the critical assets are identified by putting the 'x' symbol in the entry of the table given below.

Table 1. Critical assets of TOE environment

Security characteristic / Part	Availability	Confidentiality	Integrity	Authenticity
P1. Control-command of the process interface	x		x	x
P2. Data exchange between the TOE and the supervision interface	x	x	x	x
P3. Data exchange between the TOE and other RTUs interface	x	x	x	x
P4. Engineering workstation flow interface		x	x	x

Rationale:

P1. **Control-command of the process interface**: The Availability, Integrity and Authenticity of the actions performed through this interface must be protected.

P2. **Data exchange between the TOE and the supervision interface**: The Availability, Integrity and Authenticity of the data exchange between the TOE and the supervision must be protected.

P3. **Data exchange between the TOE and other RTUs interface**: The Availability, Integrity and Authenticity of the exchange between the TOE and other RTUs must be protected.

P4. **Engineering workstation flow interface**: The flow between the TOE and the engineering workstation must be protected concerning its Integrity, Confidentiality and Authenticity.

2.3 TOE critical assets

In the following table, the critical assets are identified by putting the 'x' symbol in the entry of the table given below.

Table 2. Critical assets of TOE

Security characteristic Part	Availability	Confidentiality	Integrity	Authenticity
P5. Operating system (kernel)			x	x
P6. Firmware		x	x	x
P7. Configuration		x	x	x
P8. User authentication mechanism			x	x
P9. User secrets		x	x	
P10. Access control policy			x	
P11. Local logging	x			
P12. Remote logging	x			
P13. Local logs			x	x
P14. Remote logs			x	x

Rationale:

P5. **Operating system (kernel)**: The OS must be protected concerning its Integrity and and Authenticity.

P6. **Firmware**: In order to work properly, the firmware must be protected concerning its Integrity, Availability and Authenticity.

P7. **Configuration**: The configuration of the TOE must be protected concerning its Confidentiality, Integrity and Authenticity. The attacker must not be able to discover the configuration of the TOE by other means than the TOE activity. Configuration includes also program logic.

P8. **User authentication mechanism**: This mechanism can be based on a local database or on a remote authentication server. In both cases, Integrity, Availability and Authenticity of the mechanism must be protected.

P9. **User secrets**: The user secrets can be passwords, certificates etc.. They can be stored in the TOE or stored in a remote authentication server. In all cases Integrity and Confidentiality of these credentials must be protected.

P10.   **Access control policy**: The policy can be stored locally or remotely on an authentication server. In both cases, Integrity of the access control policy must be protected.

P11.   **Local logging**: Once configured, the local logging must remain operational, i.e. its Availability must be protected

P12.   **Remote logging**: The TOE is capable of remote logging. Once configured, the logging must remain operational, i.e. its Availability must be protected.

P13.   **Local logs**: The Integrity of the local logs must be protected.

P14.   **Remote logs**: Integrity and Authenticity of the remote logs entries submitted by the TOE must be protected. (for instance, a mechanism must be present to detect the absence of a message in a sequence of properly received messages).

3 Threat Model

3.1 Attackers

The following attackers are considered:

Attacker on the supervision network: The attacker controls a device plugged to the supervision network of the TOE (Part 2. Data exchange between the TOE and the supervision interface).

Attacker on the process network: The attacker controls a device plugged to the process network (Part P1. Control-command of the process interface).

Evil user: The attacker has compromised an unprivileged account and tries to bypass the access control policy of the TOE.

Attacker with physical access to the TOE: The attacker has physical access to the TOE.

3.2 Threats

The following threats have been identified:

T1. **Denial of service**: The attacker manages to generate a denial of service on the TOE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file). This denial of service can affect the whole TOE or only some of its functions.

T2. **Operating system / firmware alteration**: The attacker manages to inject and run a corrupted OS / firmware on the TOE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install an update on the TOE by legitimate means. Finally, the attacker manages to modify the version of the OS / firmware installed on the TOE without having the privilege to do so.

T3. **Configuration compromise**: The attacker manages to obtain some parts of the TOE configuration by other means than the observation of the activity of the TOE.

T4. **Configuration alteration**: The attacker manages to modify, temporarily or permanently, the TOE configuration.

T5. **Credentials theft**: The attacker manages to steal user or other credentials.

T6. **Authentication violation**: The attacker manages to authenticate itself without credentials.

T7. **Access control violation**: The attacker manages to obtain permissions that he does not normally have.

T8. **Local logs alteration**: The attacker manages to delete or modify a local log entry without being authorized by the access control policy of the TOE.

T9. **Remote logs alteration**: The attacker manages to delete or modify a remote log entry without the receiver (the component hosting the log) being able to notice it.

T10. **Parameters or command injection**: The attacker manages to modify parameters in the TOE configuration or to transmit commands (through the Control-command of the process interface) without being authorized.

T11. **Flows alteration**: The attacker manages to corrupt exchanges between the TOE and an external component without being detected.

T12. **Flows compromise**: In case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the TOE and the supervision or other RTU.

4 Critical assets vs. threats

The table below presents the relationship between the threats and the critical assets that can be directly compromised by these threats (for instance, the critical asset *Integrity of Firmware* can be directly compromised by the *Operating system/firmware alteration* threat).

Table 3. Critical assets affected by the threats

Threats \ Parts	P1. Control-command of the process interface	P2. Data exchange between the TOE and the supervision interface	P3. Data exchange between the TOE and other RTUs interface	P4. Engineering workstation flow interface	P5. Operating system (kernel)	P6. Firmware	P7. Configuration	P8. User authentication mechanism	P9. User secrets	P10. Access control policy	P11. Local logging	P12. Remote logging	P13. Local logs	P14. Remote logs
T1. Denial of service	Av	Av	Av	Av							Av	Av		
T2. Operating system / firmware alteration					I, Au	I, Au								
T3. Configuration compromise							C							
T4. Configuration alteration							I, Au							
T5. Credentials theft									C					
T6. Authentication violation								I, Au						
T7. Access control violation									C	I				
T8. Local logs alteration													I, Au	
T9. Remote logs alteration														I, Au
T10. Parameters or command injection	I, Au	I, Au	I, Au											
T11. Flows alteration	I, Au	I, Au	I, Au	I, Au										
T12. Flows compromise		C	C	C										

Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity

5 Security functions

Security functions are intended to protect the component (its parts) against the threats presented in Section 3..

Security functions are determined by first selecting the Foundational Requirements (FR) of IEC 62443-4-2 that provide adequate protection of the identified critical assets and then assigning these requirements to the (groups of) parts of the component.

5.1 Assigning Foundational Requirements

Foundational Requirement, if satisfied, provide component capabilities to protect given security characteristics of critical assets against threats. The scope of Foundational Requirements is as follows (for a detailed specification see IEC 62443-4-2):

FR1: *Identification and authentication control* (IAC): necessary capabilities to reliably identify and authenticate all users (humans, software processes and devices) attempting to access the ToE shall be provided.

- satisfaction of FR1 is required to achieve authenticity of an asset

FR2: *Use control* (UC): necessary capabilities to enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the system or assets and monitor the use of these privileges shall be provided.

- satisfaction of FR2 is required to achieve authenticity of an asset

FR3: *System integrity* (SI): necessary capabilities to ensure the integrity of the ToE to prevent unauthorized manipulation shall be provided.

- satisfaction of FR3 is required to achieve integrity of an asset

FR4: *Data confidentiality* (DC): necessary capabilities to ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure shall be provided.

- satisfaction of FR4 is required to achieve confidentiality of an asset

FR5: *Restricted data flow* (RDF): necessary capabilities to segment the control system via zones and conduits[1] to limit the unnecessary flow of data shall be provided.

- satisfaction of FR5 is required for components participating in separation of information flow restrictions between zones

FR6: *Timely response to events* (TRE): necessary capabilities to respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered shall be provided.

- satisfaction of FR6 is required for assets related to security events

FR7: *Resource availability* (RA): necessary capabilities to ensure the availability of the control system against the degradation or denial of essential services shall be provided.

- satisfaction of FR7 is required to achieve availability of an asset

---

[1] 'conduit' is an abstraction representing communication channels (internal and external) of ToE

Table 4. Foundational Requirements assigned to protect critical assets

Parts / Threats	P1. Control-command of the process interface	P2. Data exchange between the TOE and the supervision interface	P3. Data exchange between the TOE and other RTUs interface	P4. Engineering workstation flow interface	P5. Operating system (kernel)	P6. Firmware	P7. Configuration	P8. User authentication mechanism	P9. User secrets	P10. Access control policy	P11. Local logging	P12. Remote logging	P13. Local logs	P14. Remote logs
T1. Denial of service	Av: **FR7**	Av: **FR7**	Av: **FR7**	Av: **FR7**							Av: **FR7 FR6**	Av: **FR7 FR6**		
T2. Operating system / firmware alteration					Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**								
T3. Configuration compromise							C: **FR4**							
T4. Configuration alteration							Au: **FR1 FR2** I: **FR3**							
T5. Credentials theft									C: **FR4**					
T6. Authentication violation								Au: **FR1 FR2** I: **FR3**						
7. Access control violation										C: **FR4**	I: **FR3**			
T8. Local logs alteration													Au: **FR1 FR2** I: **FR3 FR6**	
T9. Remote logs alteration														Au: **FR1 FR2** I: **FR3 FR6**
T10. Parameters or command injection	Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**											
T11. Flows alteration	Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**	Au: **FR1 FR2** I: **FR3**										
T12. Flows compromise		C: **FR4**	C: **FR4**	C: **FR4**										

5.2 Selecting Security Functions

Foundational requirements identified in Section 5 to protect ToE assets have been grouped into a set of Security Functions. The requirements are classified to belong to one security function when they relate to the same type of component parts and it is expected the protection will be based on the same implementation mechanism.

Security function	Protected critical assets	Foundational requirements	Addressed Threats
SF1. *Protection of network communication confidentiality*	***Confidentiality of:*** P2. Data exchange between the TOE and the supervision interface P3. Data exchange between the TOE and other RTUs interface P4. Engineering workstation flow interface	FR 4 Data confidentiality	T12. Flows compromise
SF2. *Network communication authenticity and integrity*	***Authenticity and integrity of***: P1. Control-command of the process interface P2. Data exchange between the TOE and the supervision interface P3. Data exchange between the TOE and other RTUs interface P4. Engineering workstation flow interface	FR 1 Identification and authentication control FR 2 Use control FR 3 System integrity	T10. Parameters or command injection T11. Flows alteration
SF3. *Protection of critical data confidentiality*	***Confidentiality of:*** P7. Configuration P9. User secrets	FR 4 Data confidentiality	T3. Configuration compromise T5. Credentials theft T7. Access control violation
SF4. *User authorization in TOE functions*	***Authenticity of:*** P5. Operating system (kernel) P6. Firmware P7. Configuration P8. User authentication mechanism P13. Local logs P14. Remote logs	FR 1 Identification and authentication control FR 2 Use control	T2. Operating system / firmware alteration T4. Configuration alteration T6. Authentication violation T8. Local logs alteration T9. Remote logs alteration
SF5. *TOE functions integrity*	***Integrity of:*** P5. Operating system (kernel) P6. Firmware P7. Configuration P8. User authentication mechanism P10. Access control policy P13. Local logs P14. Remote logs	FR 3 System integrity FR 6 – Timely response to events	T2. Operating system / firmware alteration T4. Configuration alteration T6. Authentication violation T7. Access control violation T8. Local logs alteration T9. Remote logs alteration
SF6. *Protection of Resource Availability*	***Availability of:*** P1. Control-command of the process interface P2. Data exchange between the TOE and the supervision interface P3. Data exchange between the TOE and other RTUs interface P4. Engineering workstation flow interface P11. Local logging P12. Remote logging	FR 6 – Timely response to events FR 7 Resource availability	1. Denial of service

6 Component requirements

Security functions have been mapped to corresponding IEC 62443-4-2 requirements. For each security function component requirements (CRs) related for FRs specified in Table 4 have been examined. If a given CR is not relevant for satisfaction of the security function's FRs, it can be excluded (marked with grey color) and a rationale provided.

Table 5. Security requirements

Security function	IEC 62443-4-2 requirements	Rationale
SF1. Protection of network communication confidentiality	CR 4.1 – Information confidentiality CR 4.2 – Information persistence CR 4.3 – Use of cryptography	*CR 4.2 excluded as it doesn't apply for networks*
SF2. Network communication authenticity and integrity	CR 1.1 – Human user identification and authentication CR 1.2 – Software process and device identification and authentication CR 1.3 – Account management CR 1.4 – Identifier management CR 1.5 – Authenticator management CR 1.6 – Wireless access management CR 1.7 – Strength of password-based authentication CR 1.8 – Public key infrastructure certificates CR 1.9 – Strength of public key authentication CR 1.10 – Authenticator feedback CR 1.11 – Unsuccessful login attempts CR 1.12 – System use notification CR 1.13 – Access via untrusted networks CR 1.14 – Strength of symmetric key authentication CR 2.1 – Authorization enforcement CR 2.2 – Wireless use control CR 2.3 – Use control for portable and mobile devices CR 2.4 – Mobile code CR 2.5 – Session lock CR 2.6 – Remote session termination CR 2.7 – Concurrent session control CR 2.8 – Auditable events CR 2.9 – Audit storage capacity CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps CR 2.12 – Non-repudiation CR 2.13 – Use of physical diagnostic and test interfaces CR 3.1 – Communication integrity CR 3.2 – Protection from malicious code CR 3.3 – Security functionality verification CR 3.4 – Software and information integrity CR 3.5 – Input validation CR 3.6 – Deterministic output CR 3.7 – Error handling CR 3.8 – Session integrity CR 3.9 – Protection of audit information CR 3.10 – Support for updates CR 3.11 – Physical tamper resistance and detection CR 3.12 – Provisioning product supplier roots of trust CR 3.13 – Provisioning asset owner roots of trust CR 3.14 – Integrity of the boot process	*CR 1.1 excluded as human user identification is a higher level of service then the network services.* *…* *Rationale why CRs in grey are excluded from the scope of the security function*
SF3. Protection of critical data confidentiality	CR 4.1 – Information confidentiality CR 4.2 – Information persistence CR 4.3 – Use of cryptography	*Rationale why CRs in grey are excluded from the scope of the security function*

Security function	IEC 62443-4-2 requirements	Rationale
SF4. *User authorization in TOE functions*	CR 1.1 – Human user identification and authentication CR 1.2 – Software process and device identification and authentication CR 1.3 – Account management CR 1.4 – Identifier management CR 1.5 – Authenticator management CR 1.6 – Wireless access management CR 1.7 – Strength of password-based authentication CR 1.8 – Public key infrastructure certificates CR 1.9 – Strength of public key authentication CR 1.10 – Authenticator feedback CR 1.11 – Unsuccessful login attempts CR 1.12 – System use notification CR 1.13 – Access via untrusted networks CR 1.14 – Strength of symmetric key authentication CR 2.1 – Authorization enforcement CR 2.2 – Wireless use control CR 2.3 – Use control for portable and mobile devices CR 2.4 – Mobile code CR 2.5 – Session lock CR 2.6 – Remote session termination CR 2.7 – Concurrent session control CR 2.8 – Auditable events CR 2.9 – Audit storage capacity CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps CR 2.12 – Non-repudiation CR 2.13 – Use of physical diagnostic and test interfaces	*Rationale why CRs in grey are excluded from the scope of the security function*
SF5. *TOE functions integrity*	CR 3.1 – Communication integrity CR 3.2 – Protection from malicious code CR 3.3 – Security functionality verification CR 3.4 – Software and information integrity CR 3.5 – Input validation CR 3.6 – Deterministic output CR 3.7 – Error handling CR 3.8 – Session integrity CR 3.9 – Protection of audit information CR 3.10 – Support for updates CR 3.11 – Physical tamper resistance and detection CR 3.12 – Provisioning product supplier roots of trust CR 3.13 – Provisioning asset owner roots of trust CR 3.14 – Integrity of the boot process CR 6.1 – Audit log accessibility CR 6.2 – Continuous monitoring	*Rationale why CRs in grey are excluded from the scope of the security function*
SF6. *Protection of Resource Availability*	CR 6.1 – Audit log accessibility CR 6.2 – Continuous monitoring CR 7.1 – Denial of service protection CR 7.2 – Resource management CR 7.3 – Control system backup CR 7.4 – Control system recovery and reconstitution CR 7.5 – Emergency power CR 7.6 – Network and security configuration settings CR 7.7 – Least functionality CR 7.8 – Control system component inventory	*Rationale why CRs in grey are excluded from the scope of the security function*

ANNEX III – SPANISH National Exercise Team

The Spanish NET annex contains the following document: Spanish NET report on E1 to E3 ICCF tests.

- This report includes the following contents:
    - Exercises 1, 2 and 3 goals, assumptions, principles, methodology and results: this document presents the overall process of the exercise (composition of the NET, methodology of the elaboration of the security profile, methodology of the compliance and cyber resilience evaluation of the product and conclusions for each exercise).
    - Security profile for the SIMATIC RTU3030C — V2.0.20 (Annex A): this document presents the ToE and its usage, the associated critical assets, the corresponding threat model, the security objectives and how these elements may relate to one another.

ICCF cyber resilience evaluation technical report for the SIMATIC RTU3030C — V2.0.20 (Annex B): this report includes an example of the contents that a cyber resilience evaluation technical report could deliver.

SPANISH NET REPORT ON E1 TO E3 ICCF TESTS

Version: 1.0
Date: 2017-11-30

DOCUMENT VERSION CONTROL

Version	Date	Description
0.1	30/10/2017	Initial draft
0.2	16/11/2017	Applus+ Revision
0.3	21/11/2017	Revision after the Friday 17th NET meeting at Siemens.
0.4	23/11/2017	Revision of the E3 test methodology
0.5	28/11/2017	Feedback from Siemens
1.0 (draft)	30/11/2017	Initial draft release – Some modifications are expected

INDEX

1   COMPOSITION OF THE SPANISH NET

The Spanish NET is composed of the following members:

Role	Organization/Company
National cybersecurity agency	CCN
Vendor	Siemens
Evaluation Laboratory	Applus+ Laboratories
Certification Body	CCN
Industry User	UPCT
Industrial Organization	CCI

2   SPANISH NET MEETING PROJECT MILESTONES

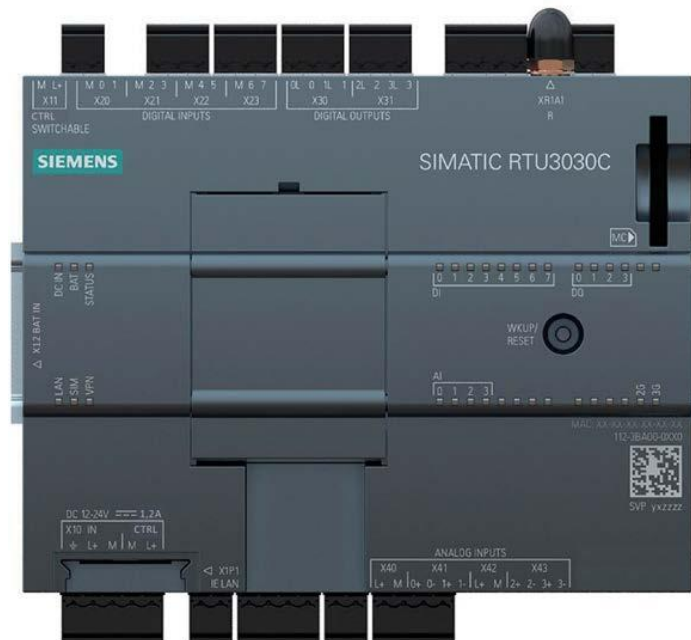| Date	Meeting Topic
13-07-2017	F2F KO Meeting
06-09-2017	Follow-up Conference call
22-09-2017	Nets Meeting in Brussels
31-10-2017	First Results Discussion Meeting
03-11-2017	First revision of the Security Profile
17-11-2017	NET meeting in the Madrid SIEMENS HQ, to showcase the selected product, review the NET report and activities, simulate the exercises and coordinate further testing efforts.
24-11-2017	End of commenting period
30-11-2017	Deliver of draft report to ERNCIP after NET review

3 TESTS PERFORMED

The Spanish NET has performed the ICCF component tests E1+E2+E3, defined as:

- E1 – Elaborate a protection profile and a security profile and report on its level of difficulty.[1]

- E2 – Simulate a product compliance assessment, document and report on its level of difficulty.

- E3 – Simulate a product cyber resilience test, document and report on its level of difficulty.

4 BASELINE USE CASE

The product chosen for executing the E1+E2+E3 tests is: SIMATIC RTU3030C[2].

A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

---

[1] Only the security profile has been elaborated

[2] http://w3.siemens.com/mcms/industrial-communication/en/industrial-remote-communication/telecontrol/remote-terminal-unit/pages/rtu-3030c.aspx

The TOE includes the following features:

- User program execution: the TOE runs a simple controller program. This program processes the inputs via program blocks.
- Input/output management: the TOE is able to read 8 digital and 4 analog local inputs, and write 4 digital local outputs. These I/O allows the TOE to control and command the industrial process.
- Administration functions: the TOE includes administration functions in order to configure or program the other functionalities of the TOE. One administration interface is possible:
  - web-client, via WBM (Web Based Management)
- Local logging: the TOE supports the configuration of an optional local logging policy, in a local SD card.
- Control room communication: the TOE supports the definition of a remote communications partner. The following protocols are available:
  - TeleControl Basic (without VPN possible)
  - DNP3
  - IEC 60870-5-104
  - ST7 via TIM 1531 nodestation and WinCC with additional plugin.
- Mobile network connection: The TOE will be able to connect to a UMTS / GSM network, by including a SIM card inside the appliance.
- Other communication mechanisms: the TOE supports additional communication protocols
  - SMS (inbound and outbound) for wake-up
  - Secure Email (outbound)
  - Secure FTP Client to send e.g. log files
  - OpenVPN client (legacy or via SINEMA RC with auto enrollment)
  - HTTP and HTTPS

5 EXERCISE 1 - ELABORATE A SECURITY PROFILE AND REPORT ON ITS LEVEL OF DIFFICULTY

5.1 GOALS, ASSUMPTIONS & PRINCIPLES OF THE TEST: E1 (ONLY SECURITY PROFILE)

The objective of this test was to **elaborate a security profile** for the baseline product, SIMATIC RTU3030C.

CSPN has been chosen as the reference methodology to develop the security profile. A CSPN security target consists on (see section 3.2 of [CRITERIA]):

- Product's commercial name and unique references, to clearly identify the product and version under evaluation.
- An overview containing
  - The product expected usage
  - Typical users of the product
  - Product usage environment
- Security Problem
  - Assumptions
  - Assets
  - Threats
  - Environment security measures
- Product's security functions/mechanisms

That information should be enough to give the final customer a clear understanding of the product's purpose, its threat model and the security mechanisms used as countermeasures to those threats.

As stated on the CSPN, the security functions/mechanism must be at least informally specified in natural language.

5.2 METHODOLOGY OF THE TEST E1 (ONLY SECURITY PROFILE)

Writing a security profile is a task to be done by the developer. In order to do it, the developer has to keep in mind the expected content of the security profile (see *section 5*).

The security profile first two points identify and briefly overview the product. It is important to clearly indicate the environment where the product will be used and the components that the product will need to work which are not under evaluation (e.g. system requirements, third party applications…). This will help potential clients to understand the scope of the evaluation.

Going forward, the following point consists of a short threat model of the product under evaluation. The developer must identify the assets, threats to those assets and assumptions. Besides that, the developer will have to describe the security measures derived from the environment. This section will determine the scope of the evaluation. The security profile last point consists of describing the product's security functions to mitigate previous threats. A detailed description is not necessary, it should only be clear enough to let the evaluator understand how the security functions cover the entire threat model.

5.3 FINDINGS: KEY RESULTS, CONFIDENCE, RECOMMENDATIONS FOR ICCF IMPROVEMENTS

The assessment related to this exercise has been focused on the feasibility of writing a security profile for someone that has not previous background in certification.

The final conclusion of the NET is that following the approach of CSPN, the effort required to write a Security Profile is acceptable. Therefore, the NET considers that the approach is the right one.

6 EXERCISE 2 - SIMULATE A PRODUCT COMPLIANCE ASSESSMENT, DOCUMENT AND REPORT ON ITS LEVEL OF DIFFICULTY

6.1 GOALS, ASSUMPTIONS & PRINCIPLES OF THE TEST: E2

The objective of this test was to determine which documentation analysis should be done to demonstrate on paper (compliance assessment) that requirements specified on the Security Profile have been addressed by appropriate measures.

The developer will have to provide the laboratory with the Security Profile and a document based on the requirements described on the methodology (see *section 6.2*).

The description of the security requirements, as well as the developer documentation, will not have to be written in semiformal language, as done in IEC 62443-4-2, Common Criteria or NIST SP800-82.

Instead, a **natural language approach**, similar to how the security functions are defined on the CPSN, will be used. Of course any standard/methodology such as the mentioned above can be used by the developer to have a starting point for elaborating the documentation.

6.2 METHODOLOGY OF THE TEST E2

The first evaluator activity will be to verify that the security functions in the Security Profile are consistent with the security problem definition (assumptions, threats and security measures of the environment). This activity will determine whether the developer has to include, delete or modify any of the security functions. Evaluator's tasks related to this can be found at section 4.1 [CRITERIA].

Once this activity has been successfully completed, the evaluator will have to verify the documentation delivered by the developer. This documentation should contain a rationale written by the developer describing how each security function is addressed by the product's measures.

In order to do so, the developer will have a supporting guide developed by the certification scheme describing expected requirements for each security measure. A similar approach as that used in FIPS or FIDO.

Below is an example of a fragment of a potential evaluation methodology:

"*For instance, secure storage of secrets, firmware signature and secure communication are three security functions (see Annex 1) which are implemented using cryptographic*

mechanisms. The supporting guide should contain a section describing the requirements for cryptographic mechanism:

- *Use of approved algorithms by SOG-IS*
- *Key length*
- *Key generation method*
- *Key protection measures*

Another example could be a security function based on password authentication, the supporting guide should describe requirements for password protection:

- *Minimum bit length*
- *Lifespan*

The evaluator's activity will consist on verifying that the developer rationale is based on supporting guide requirements. It can be the case where a security function uses a mechanism not included on the supporting guide. The evaluator should provide a rationale justifying the effectiveness of that measure."

The output of these activities should be a compliance assessment matrix of the security functions and the justification rationale if required.

6.3 FINDINGS: KEY RESULTS, CONFIDENCE, RECOMMENDATIONS FOR ICCF IMPROVEMENTS

After the simulation, it was concluded that the existence of a precise evaluation methodology for the conformance assessment was crucial to ensure the repeatability of the results among different labs/certification bodies.

The decision of allowing the developer to write the security requirements as specified in CPSN instead of following formal security standards (Common Criteria or IEC 62443-4-2) is to make the certification process easier for the developers. Based on our experience, this requires that the developer has some knowledge on those standards, but that will not be necessary if those requirements can be expressed through natural language.

This will probably require more work on the laboratory's side, because each developer could describe the same mechanism using different descriptions, but we think one of the goals of this new certification process must be to make things easier for developers.

Moreover, the Compliance assessment as a stand-alone documentation evaluation cannot be considered a solid compliance evaluation. Our proposal is an approach closer to what is required at CSPN including functional testing.

A minimum amount of functional testing should be required in order to avoid awkward situations, for instance: the TOE has been assessed before the TOE version has been frozen or with some functionality not included in the final release.

In conclusion, it should be confirmed that the security functionality stated in the documentation is actually implemented in the TOE.

It is important to perform a minimum documentation and functional testing. This evaluation task not be done in depth, but will be enough to, at least, verify the correctness of the information provided by the developer.

Our proposal, stated below, is aligned with the Collaborative Protection Profile as described in CC and the certification approach of the National Information Assurance Partnership (NIAP): documental revision and functional testing.

6.3.1 PROPOSAL FOR METHODOLOGY FOR THE COMPLIANCE ASSESSMENT

The proposal is based on CSPN methodology [CRITERIA].

For this evaluation activity, the developer must send to the evaluator, at least, the security profile, installation guide and the necessary documentation to understand the design of the product. These documents can be written informally in natural language but they should be clear enough to let the evaluator perform the required analysis.

This activity will comprise the following phases (as stated in [CRITERIA]):

- o Phase 1 – Security Profile analysis (following the methodology described on [CRITERIA])
- o Phase 2 – Product installation
    - o Sub-Phase - Ease of use analysis (insecure use/configuration analysis)
- o Phase 3 – Documentation analysis (following the methodology explained in the E2 exercise)
- o Phase 5 – Product testing (functional testing)

The output of this activity should be a report where the evaluator describes:

1. The correctness of the documentation

2. Non-conformities encountered during the evaluation

7 EXERCISE 3 - SIMULATE A PRODUCT CYBER RESILIENCE TEST, DOCUMENT AND REPORT ON ITS LEVEL OF DIFFICULTY

7.1 GOALS, ASSUMPTIONS & PRINCIPLES OF THE TEST: E3

The objective of this test has been to determine which activities should be performed by the evaluator to demonstrate the effectiveness of an IACS product's cybersecurity and cyber-defense mechanisms. This test should be considered complimentary to the E2 test: on E2, the evaluator has to perform functional testing (in our approach) while on E3, they must perform security testing.

A simulation of these activities was performed over the baseline product SIMATIC RTU3030C (see *Annex B*). Some modifications have been introduced into CSPN methodology, to define the evaluator guideline for those activities.

7.2 METHODOLOGY OF THE TEST E3

Testing the cybersecurity and cyber defense mechanisms of the evaluated product should be the main activity of the certification process. This task corresponds to Phases 6 and 7 of the CSPN [CRITERIA], with some heavy modifications, based on IEC 62443 and CC.

The proposed testing comprises three main tasks

1. A rationale of the resistance of the security mechanisms (Similar to the CSPN)
2. A *tiered* vulnerability analysis
3. A *tiered* penetration testing

The proposed *tiered methodology* is a bottom-up approach:

First the focus is on the physical aspects of the TOE and the applied physical security[3]. This tier comprises every aspect related to the tangible TOE and properties. Special attention should be given to the physical interfaces of the TOE. Pure software-based TOEs would omit this analysis, but would specify the necessary hardware features.

The next tier is the TOE logical layer. This layer relates to all the software in the TOE, including the undelaying Operative System, as well as third party components. Special attention should be given to the external communication interfaces of the TOE.

---

[3] If relevant, always taking into account the evaluation scope. If the TOE assumptions clearly state that the physical perimeter is out of the evaluation, as the TOE should be located in secure premises, it would be a clear case for the omission of physical security measures. (Such as Anti-vandalism / Tamper-proofing / etc.)

The following two tiers are dependent on the evaluated TOE, and therefore could be omitted altogether.

The third tier comprises the TOE operation environment. This tier is limited to TOEs where the environment plays a critical role on the protection of the Assets, or if the TOE is conformed of several elements, tightly integrated with their environment as well. As a reference, specialized equipment for critical infrastructure (or the control software) would need to include this tier.

The fourth tier (Additional System Interactions, ASI) is related to highly interconnected TOEs, such as SCADA mainframes/servers, plant management, fire panels and such. The TOE itself does not contribute to a production process, but instead it controls several subsystems. These specially critical elements should have the interactions with subsystems properly tested. Network-managed security solutions should be reviewed in this tier as well.
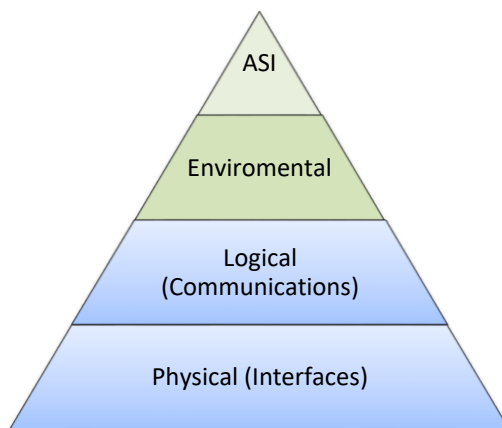
Security analysis and testing tiers

An example of a Cyber Resilience Testing Report is provided in Annex B, with proposed sections and contents, as a "simulated" TOE evaluation, for the same equipment as for the E1 test.

7.2.1 RESISTANCE OF THE SECURITY MECHANISMS

The rationale of the resistance of the security mechanisms consists of Phase 6 of [CRITERIA] where the evaluator has to identify the security mechanisms and provide a rationale of its resistance based on a scoring table (copied from the CSPN below). Once each security mechanism is ranked, the resistance could be scored as Basic/Elementary, Medium/Average or High.

The CSPN table is included for reference:

Factor	Interval	Value for identification of a vulnerability	Value for exploitation of a vulnerability
	< 0,5 hours	0	0
	< 1 day	2	3
	< 1 month	3	5
	> 1 month	5	8
Time taken for	Impracticable	* (High)	* (High)
	Layman	0	0
	Proficient	2	2
Attacker expertise	Expert	5	4
	Any	0	0
Knowledge necessary for the attacker	Public information	2	2
	Sensitive information	5	4
	< 0.5 hours	0	0
	< 1 day	2	4
	< 1 month	3	6
TOE access by the attacker	> 1 month	4	9
	Impracticable	* (High)	* (High)
	None	0	0
	Standard	1	2
Type of equipment necessary	Specialized	3	4
	Specific	5	6

If a * (High) element is found, the final score instantly is graded High.

Sum of values	Resistant to an attacker having an attack potential	Level of functions resistance
0 to 9	No ranking	
10 to 17	Low	Basic / Elementary
18 to 24	Moderate	Medium / Average
> 24	High	High

Taking into consideration the importance of the products under evaluation, the proposed minimum function resistance level should be **Medium/Moderate (18 to 24 points)[4]**.

7.2.2 VULNERABILITY ANALYSIS

---

[4] Normally, the CSPN methodology requires a Basic/Low (10 to 17 points) function resistance level.

CSPN Tasks 1 & 2 already are basic testing activities in other certification programs related with IACS products like the ISASecure IEC 62443 Certification (Vulnerability Identification Test (VIT))

One important modification of our methodology compared with the CSPN is the inclusion of the design analysis task. The CSPN methodology main evaluation activities consist of different testing approaches over the product under evaluation. We believe that is an important phase of a cybersecurity evaluation but it is not enough.

Design analysis has been proven very valuable when doing the security assessment of many solutions. For instance, the recent WPA2 attack (KRACK) is based on a re-evaluation of the four-way handshake protocol.

As previously related, it should not be mandatory to ask the developer for detailed and formal documentation (as in a CC evaluation). The documentation should be clear enough to provide a good understanding of internal details which in turn will allow the evaluator to develop a solid rationale about the security of the product. Meetings between the evaluation actors may be used to gain this knowledge.

Otherwise, we cannot ensure that the security analysis is sufficiently complete.

For all possible vulnerabilities encountered in this phase, an attack potential calculation should be made, according to the Common Criteria [CEM (B.4.2.3 Calculation of attack potential)] guidance. This applies to all the tiers.

7.2.2.1 PHYSICAL VULNERABILITY ANALYSIS (PHY-VA)

The first tier analysis consists of physical interfaces (ports, buttons…) search and analysis, detailing which of them affect the operation of the device (power, management, communications, debug…).

When all the physical properties have been established, the operating physical perimeter is analyzed to finally determine if the physical security solution is sufficient. A list of the physical protections available in the TOE, such as security labeling, internal sensors, screw types, enclosure sealing… should be described, if the physical perimeter is relevant for the security of the assets.

Finally, the physical tier analysis should review the major components that compose the logic board(s). The developer should provide diagrams or pictures of these boards; clearly

labeling the debug and other interface ports; as well as port pinouts[5] to uncover possible undocumented interfaces in the Penetration testing phase.

7.2.2.2 LOGICAL VULNERABILITY ANALYSIS (LOG-VA)

The second tier consists on the analysis of the software and its logical interfaces like communication, file operations... For this purpose, the developer should provide a list of:

- The used communication protocols and Operative System in use by the TOE (if applicable).
- A description of the cryptographic primitives in use, if any, including their configuration parameters, if any.
- A list of the TOE files and configuration files, including the logical location in the TOE filesystem.
- A list of the third party components being used to compile/link/assemble the TOE, with their exact version detailed.

The evaluator will analyze this information in order to try to detect vulnerabilities, by reviewing public sources for publicly known vulnerabilities, taking previous design analysis flaws and documenting them in the report, and elaborate other possible attack strategies.

To complement this information, and in order to detect other latent vulnerabilities, the evaluator will execute a source code audit (CSPN Task 3). This audit might be subsampled only to the sections where security functionality is being implemented, so complete access to the vendor IP is not needed.

The security assurance of an evaluation without a source code audit is limited. Black box evaluations are important but cannot give a full understanding of what is really happening inside the device. This is the reasoning behind the reason why some sort of source code audit must be mandatory.

7.2.2.3 ENVIRONMENTAL VULNERABILITY ANALYSIS (ENV-VA)

If the product security is tightly interconnected with its environment, this analysis tier should be executed.

---

[5] Especially for proprietary connectors.

The evaluator shall devise potential threats to the environment, specifically to the aspects that would affect the TOE security. The evaluator should also elaborate a list of minimum environmental security requirements for the TOE.

The expected result would be some kind of checklist or guidance, which would have to be followed by the final client to ascertain that the expected environmental protections are set in place.

7.2.2.4 ADDITIONAL SYSTEMS INTERACTIONS VULNERABILITY ANALYSIS (ASI-VA)

If the TOE is mainly a networking product, or its functionality is dependent on external elements, such as sensors, this analysis tier should be executed. This would specifically apply to plant management solutions, i.e., SCADA software.

The evaluator shall analyze the protocols used by the elements, and present attack scenarios, such as the malicious substitution of the elements. This analysis will aid itself on the design analysis, in order to detect poor design choices (such as not verifying the integrity of communication from remote elements, or allowing configuration changes from any element in a supposedly secure local network, such as LON or CAN).

This tier might only be executed in ICCS-A evaluations, please refer to the conclusions.

7.2.3 PENETRATION TESTING

The penetration testing by the evaluator shall try to exploit the previously identified potential vulnerabilities from the Vulnerability Analysis, if the attack potential needed for the attack (calculated from the CC CEM attack potential) less than High.

The potential vulnerabilities with an attack potential of High or beyond will not need to be tested (although they may be tested if it deemed interesting by the developer or the Certification Body). These vulnerabilities will be deemed as "Residual".

The evaluation tiers will be the same as in the Vulnerability Analysis phase. For each of the tiers, a final verdict will be emitted. If the tier was not executed, a "Not Executed (Pass)" grade will be given. If a tier contains residual vulnerabilities, it will be graded as "Residual (Pass)".

Networked appliances should execute the ISA 62443 Communication Robustness Testing (CRT).

For documental brevity, the ICCAR functional tests may be included in the Penetration Testing.

7.2.4 EVALUATOR OUTPUT AND FOLLOW-UP VENDOR ACTIONS

A sample document is included as a reference of the resulting ETR (ICCF Cyber Resilience Evaluation Technical Report)

The resulting ETR includes all the elements described in the methodology. This live document should contain all the information related to the security

After penetration testing, all vulnerabilities must be resolved by the developer, with the exception of those whose punctuation is higher than 24 points (the Medium/Average level). In that case, the vulnerability will be named a "residual vulnerability" and the developer will not be forced to solve it.

If a product after the evaluation contains residual vulnerabilities, these should be clearly stated on the certification report.

7.3 FINDINGS: KEY RESULTS, CONFIDENCE, RECOMMENDATIONS FOR ICCF IMPROVEMENTS

The main conclusion obtained through the NET simulation testing exercise is that the evaluation period must have an upper boundary on the testing effort. The evaluation should be concluded in 20 to 40 days, not including the 10 days used for the functional testing and documental compliance devised in the E2 test of this document.

The amount of days should be adjusted and reviewed after a real testing effort of a product, but the maximum boundary should be kept in place, in order to limit the cost for all the parties involved in the evaluation.

The approach to be followed is slightly different to the CSPN [CRITERIA]. Two main phases have been defined: Vulnerability Analysis and Penetration Testing. Guidance on how to conduct this methodology has been provided.

The vendor seemed concerned about the source code analysis. Whole source code will not be provided but critical parts/portions of the code (e.g. integrity protection mechanism). Although, this would need further discussion about how to do it.

As previously mentioned, the laboratory proposal is to carry out the review in the vendor facilities, by sending the evaluators equipped with the appropriate tools (static code analyzers, code analysis tools, fuzzing frameworks, etc.) during a week (suggested), to collaboratively work with the vendor in the evaluation.

Another approach could be to have an optional source code review, as CSPN, but indicating on the product certification stamp whether the evaluation involved source code review. The reason is to be transparent with the final user.

ANNEX A: SECURITY PROFILE

ICCF Security Profile
FOR ERNCIP TEST E1 USAGE ONLY

SIMATIC RTU3030C – V2.0.20

Version: 1.0 (draft)
Date: 2017-11-30

Document version control

Version	Date	Description
0.1	2017-11-02	Initial draft
0.2	2017-11-14	Small cover and header changes, product identification updated
0.3	2017-11-16	Applied ISO 8601 dates
0.4	2017-11-25	Updated with SIEMENS feedback
0.5	2017-11-27	Updated documentation links
1.0 (draft)	30/11/2017	Initial draft release – Some modifications are expected

Table of Contents

1   INTRODUCTION

1.1   CONTEXT OF THIS DOCUMENT

This document is written for the ICCF scheme certification for the product "SIMATIC RTU3030C".
The product is implemented by Siemens.

1.2   PRODUCT IDENTIFICATION

Editor	SIEMENS AG Industry Sector – Drive Technologies Division Gleiwitzerstr. 555 90325 Nürnberg GERMANY
Link	http://www.siemens.com
Product	SIMATIC RTU3030C (Order number 6NH3112-3BA00-0XX0)
Firmware version	V2.0.20 Four versions of this firmware exist, for the 4 supported network protocols: DNP3, IEC60870-5,TeleControl Basic and SINAUT ST7
Firmware link	Authorized credentials are needed to download the firmware files General Site: https://support.industry.siemens.com/cs/document/109751600/sales-release-of-simatic-rtu3010c-and-firmware-version-2-0-for-simatic-rtu30x0c?lc=en-US&pnid=21767
	DNP3: https://support.industry.siemens.com/cs/attachments/109751600/RTU1123BA00_V2.0.20_DNP3_OSS.zip SHA512 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	IEC60870-5-104: https://support.industry.siemens.com/cs/attachments/109751600/RTU1123BA00_V2.0.20_I870_OSS.zip SHA512 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	TeleControl Basic: https://support.industry.siemens.com/cs/attachments/109751600/RTU1123BA00_V2.0.20_WDCP_OSS_.zip SHA512 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	SINAUT ST7: - Not yet available - SHA512 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Product usage manual	C79000-G8976-C382-04 https://support.industry.siemens.com/cs/attachments/109750942/BA_RTU3030C_76.pdf SHA512 d4d13080e20bfb5d5deb2a6f2e6b3723f6c5409d402feab08d56447a6daccfa2fa733a60ceb808707b78e33cd516f313b4035ef9e7a500b78c87b4606b03acf6
Product category	Industrial Remote Communications Terminal

2 PRODUCT DESCRIPTION

2.1 GENERAL DESCRIPTION

A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

> The considered target of evaluation (TOE) is the SIMATIC RTU3030C developed by Siemens.
>
> The TOE is managed with SINAUT ST7cc // WinCC OA // SIMATIC PCS 7 TeleControl and SIMATIC WinCC/TeleControl.

2.2 FEATURES

The TOE includes the following features:

- User program execution: the TOE runs a simple controller program. This program processes the inputs via program blocks.
- Input/output management: the TOE is able to read 8 digital and 4 analog local inputs and write 4 digital local outputs. These I/O allow the TOE to control and command the industrial process.
- Administration functions: the TOE includes administration functions in order to configure or program the other functionalities of the TOE. One administration interface is possible:
   - web-client, via WBM (Web Based Management)

- Local logging: the TOE supports the configuration of an optional local logging policy, in a local SD card.
- Control room communication: the TOE supports the definition of a remote communications partner. The following protocols are available:
  - TeleControl Basic (without VPN possible)
  - DNP3
  - IEC 60870-5-104
  - ST7 via TIM 1531 nodestation and WinCC with additional plugin.
- Mobile network connection: The TOE will be able to connect to a UMTS / GSM network, by including a SIM card inside the appliance.
- Other communication mechanisms: the TOE supports additional communication protocols
  - SMS (inbound and outbound) for wake-up
  - Secure Email (outbound)
  - Secure FTP Client to send e.g. log files
  - OpenVPN client (legacy or via SINEMA RC with auto enrollment)
  - HTTP and HTTPS

2.3 PRODUCT USAGE

An RTU can be used to monitor connected inputs and emit outputs as programmed by local controller programs

The RTU is managed with a local or remote engineering workstation. Firmware updates and user programs can be loaded on the RTU though the network or locally, thanks to the WBM administration.

A basic architecture is depicted on the figure below, using the IEC 60870-5-104 protocol.
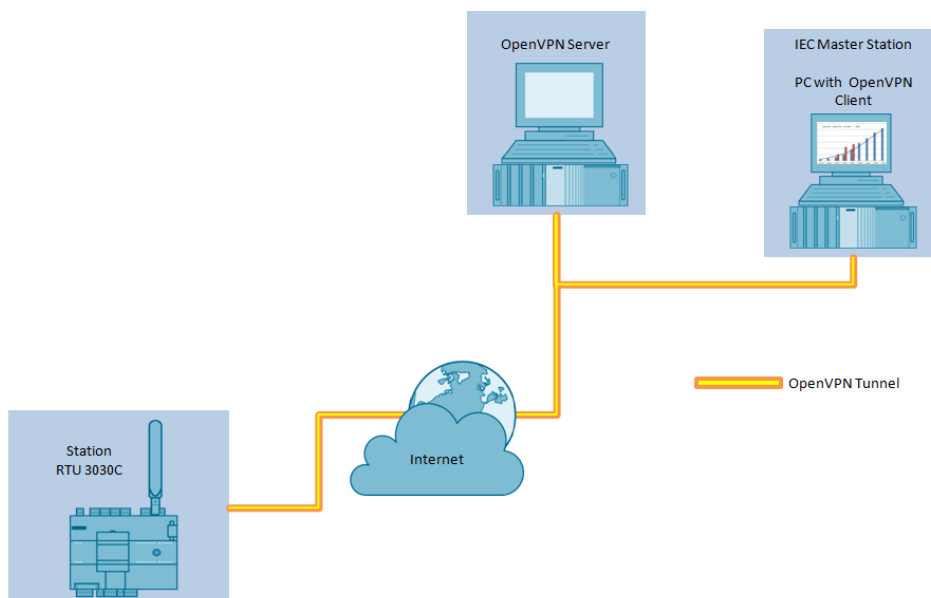
3 SECURITY PERIMETER

3.1 USERS

The users that may interact with the TOE are the following:

- **Administrator**: This user has maximum privileges. He can change all the other user accounts stored in the system.

Remark: All WBM users are administrators.

3.2 ASSUMPTIONS

Assumptions on the environment and the use case of the TOE are the following:

- **Premises:** The TOE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the TOE.
- **Backup and configuration files:** The user has to store the files in a secure way. Since products identical to the TOE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.
- **Administrators:** The administrators are competent, trained and trustworthy.
- **Logging**: It is assumed that local and remote logging are operational and that local logs are not corrupted
- **Availability of GMS/UMTS interface:** It is intended for the control function to work independently on the GSM connection. The device stores measurement values and controls the process also if the GSM interface is not available.
- **Security documentation**: the TOE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization. These documents are as follows:
    - https://support.industry.siemens.com/cs/document/109479322
    - https://support.industry.siemens.com/cs/document/109481154
    - https://support.industry.siemens.com/cs/document/109481299

All recommendations included in this documentation are applied prior to the evaluation.

4   CRITICAL ASSETS

4.1   ENVIRONMENT CRITICAL ASSETS

The environment critical assets are the following:

- **Command and Control of the monitored industrial process**: the TOE monitors and commands sensors related to industrial processes, by reading inputs and sending commands to actuators. The availability and integrity of these actions must be protected.
- **Management flows**: The data flow between the TOE and the management system must be protected in integrity, confidentiality and authenticity. Additional availability is provided by alternative communication means.
- **Wireless contract and network**: The TOE must have a SIM card with an active contract inserted. The TOE must be located inside the coverage of the contracted wireless network of the carrier.
- **OpenVPN**: The TOE should be connected to the TeleControl master via OpenVPN. The OpenVPN server must fulfill, at least, SL 2 requirements according to the IEC 62443.

The security requirements for the critical assets are the following:

Assets	Availability	Confidentiality	Integrity	Authenticity
Control-command of the industrial process	X	X	X	X
Engineering workstation flows		X	X	X
OpenVPN		X	X	X

Note: Environmental Critical Assets are not required by CSPN. They are included to provide more information of the environment

4.2   TOE CRITICAL ASSETS

The critical assets of the TOE are the following:

- **Firmware**: The firmware must be protected in both integrity and authenticity.
- **User controller programs**: The TOE runs a program designed by the users. Its integrity, confidentiality and authenticity must be protected.
- **Configuration**: The TOE configuration and policies must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the TOE by any other means than by observing the TOE activity.
- **User authentication mechanism**: The TOE must ensure the availability, integrity and authenticity of the authentication mechanism.

- **User secrets**: The user passwords must be stored in the TOE, and the TOE must ensure the integrity and confidentiality of these credentials.
- **SIM card PIN**: The TOE must store the SIM card PIN, and must ensure the integrity and confidentiality of the PIN.
- **Authorized users information:** The TOE must store the Information about authorized telephone numbers and e-mail address, and ensure the integrity and confidentiality of this information.

Assets	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
User controller programs		X	X	X
Configuration		X	X	
User authentication mechanism	X		X	X
User secrets		X	X	
SIM card PIN		X	X	
Authorized users information		X	X	X

5 THREAT MODEL

5.1 ATTACKERS

The following attackers are considered:

- **Attacker on the communications network**: The attacker can connect to the TOE carrier network, but does not know the OpenVPN or TeleControl keys.

5.2 THREATS

The following threats are considered:

- **Denial of service**: the attacked manages to generate a denial of service on the TOE by performing an unexpected action or by exploiting a vulnerability. This denial of service can affect the whole TOE or some of its functions.
- **Firmware modification**: the attacker manages to inject and run a corrupted firmware on the TOE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install that update on the TOE by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the TOE without having the privilege to do so.
- **Controller program compromise**: the attacker manages to obtain some parts of the configuration of the TOE by means other than the observation of the activity of the TOE.
- **Controller program alteration**: the attacker manages to modify, temporarily or permanently, the controller program.
- **Configuration alteration**: the attacker manages to modify, temporary or permanently, the TOE configuration.
- **Configuration compromise**: the attacker manages to illegitimately obtain some parts of the TOE configuration.
- **Credentials theft**: the attacker manages to steal user credentials.
- **Authentication violation**: the attacker succeeds in authenticating himself without credentials.
- **Flows alteration**: the attacker manages to corrupt exchanges between the TOE and an external component without being detected.
- **Flows compromise**: in case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the TOE and an external component.

5.3 SECURITY FUNCTIONS

The following security objectives are considered:

- **Malformed input management**: The TOE has been developed in order to correctly handle malformed input, in particular malformed network traffic.
- **Secure storage of secrets**: User secrets are securely stored in the TOE. In particular, the compromise of a file is not sufficient for retrieving them.
- **Secure authentication on administration interface**: Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action session.

- **Firmware signature**: At each update of the firmware, the integrity and authenticity of the new firmware are checked before updating. The integrity and authenticity of the firmware are also checked at boot time.
- **Configuration confidentiality and integrity**: The access control prevents any unauthorized person from reading or modifying the configuration of the TOE.
- **Integrity and authenticity of the controller program**: The TOE ensures the integrity of the controller program. Only authorized users can modify it.
- **Confidentiality of the controller program**: The TOE protects the confidentiality of the controller program. Only authorized users can access it.
- **Secure communication**: The TOE supports secured communication, protected in integrity, confidentiality and authenticity.

ANNEX B: CYBER RESILIENCE TEST SIMULATION AND EFFORT REPORT

ICCF Cyber Resilience Evaluation Technical Report
FOR ERNCIP TEST E3 USAGE ONLY

SIMATIC RTU3030C – V2.0.20

Version: 1.0 (draft)
Date: 2017-11-30

Version control

Version	Date	Description
0.1	2017-11-14	Initial draft
0.2	2017-11-16	Structural Changes, ISO 8601 dates.
0.3	2017-11-21	Added potential vulnerabilities and analysis
0.4	2017-11-21	Modified the document structure
0.5	2017-11-23	Updated the test methodology
0.6	2017-11-24	Document cleanup
0.7	2017-11-27	Updated to the latest Security Profile
1.0 (draft)	2017-11-30	Initial draft release – Some modifications are expected

TABLE OF CONTENTS

1   INTRODUCTION

This report is shown as an example of content that a Cyber Resilience Evaluation Technical Report could contain. None of the contents related to the TOE should be considered as valid, as this is just a sample report.

Moreover, some of the sections have not been completed. It may be used as a draft document.

1.1 PRODUCT IDENTIFICATION

Editor	SIEMENS AG Industry Sector – Drive Technologies Division Gleiwitzerstr. 555 90325 Nürnberg GERMANY
Link	http://www.siemens.com
Product	SIMATIC RTU3030C (Order number 6NH3112-3BA00-0XX0)
Firmware version	V2.0.20 Four versions of this firmware exist, for the 4 supported network protocols: DNP3, IEC60870-5,TeleControl Basic and SINAUT ST7

1.2 CERTIFICATION IDENTIFICATION

Certification Scheme	ICCS-B
ICCF Protection Profile (PP) Conformity	No PP is being used.
Product category	Industrial Remote Communications Terminal
Evaluation Laboratory	LGAI Technological Center S.A. (A-63207492) Campus UAB–Ronda de la Font del Carme, s/n 08193, Bellaterra, Barcelona (Spain) Tel: +34 93 567 20 00 www.applus.com
Certification Body/ National Information Security Agency	Organismo de Certificación (Centro Criptológico Nacional) C/Argentona 30 28023, Madrid (Spain)
Project Identification Code	ICCS-ES-2017-1

1.3 EVALUATION TECHNICAL REPORT IDENTIFICATION

ETR Reviewer	Reviewer Name
ETR Approver	Technical Leader Name
Security Profile (SP)	Version 0.5 – 2017-11-27

1.4 PENETRATION TESTING RESULTS OVERVIEW

Physical security (PHY-PT)	Pass
Logical security (LOG-PT)	Residual (Pass)
Environmental security (ENV-PT)	Not tested (Pass)
Additional systems interaction (ASI-PT)	Not tested (Pass)
Final evaluation score	Pass

1.5 RELATED DOCUMENTS

Product usage manual	09/2017 C79000-G8976-C382-04

2 SECURITY MECHANISM SCORING

This section includes the CSPN Phase 6 Security Mechanism scoring, as related in the section "7.2.1. Resistance of the Security Mechanisms".

2.1 FIRMWARE SIGNATURE (NAME OF THE SECURITY MECHANISM)

A description of the security mechanism should be included here, explaining possible attack vectors, and a brief scoring rationale. This is based on the CSPN evaluation of security mechanisms.

FOR EXAMPLE: The TOE implements a digital signature check in order to validate the authenticity of the incoming firmware file. This file is being signed under the Microsoft Authenticode Standard [AUTHENTICODE], and contains a digital PKCS #7 signature.

In order for an attacker to forge this signature, access to the private signing key is required. No other specialized access is required.

Factor	Interval	Value
Elapsed Time	> a month	5
Expertise	Expert	5
Knowledge of TOE	Sensitive information	5
Window of Opportunity	<1 day	2
Equipment	Standard	1
	Total Value	18 (High)
	Is the resistance High?	YES

3 VULNERABILITY ANALYSIS

3.1 PHYSICAL VULNERABILITY ANALYSIS (PHY-VA)

3.1.1 PHYSICAL EXTERNAL OVERVIEW
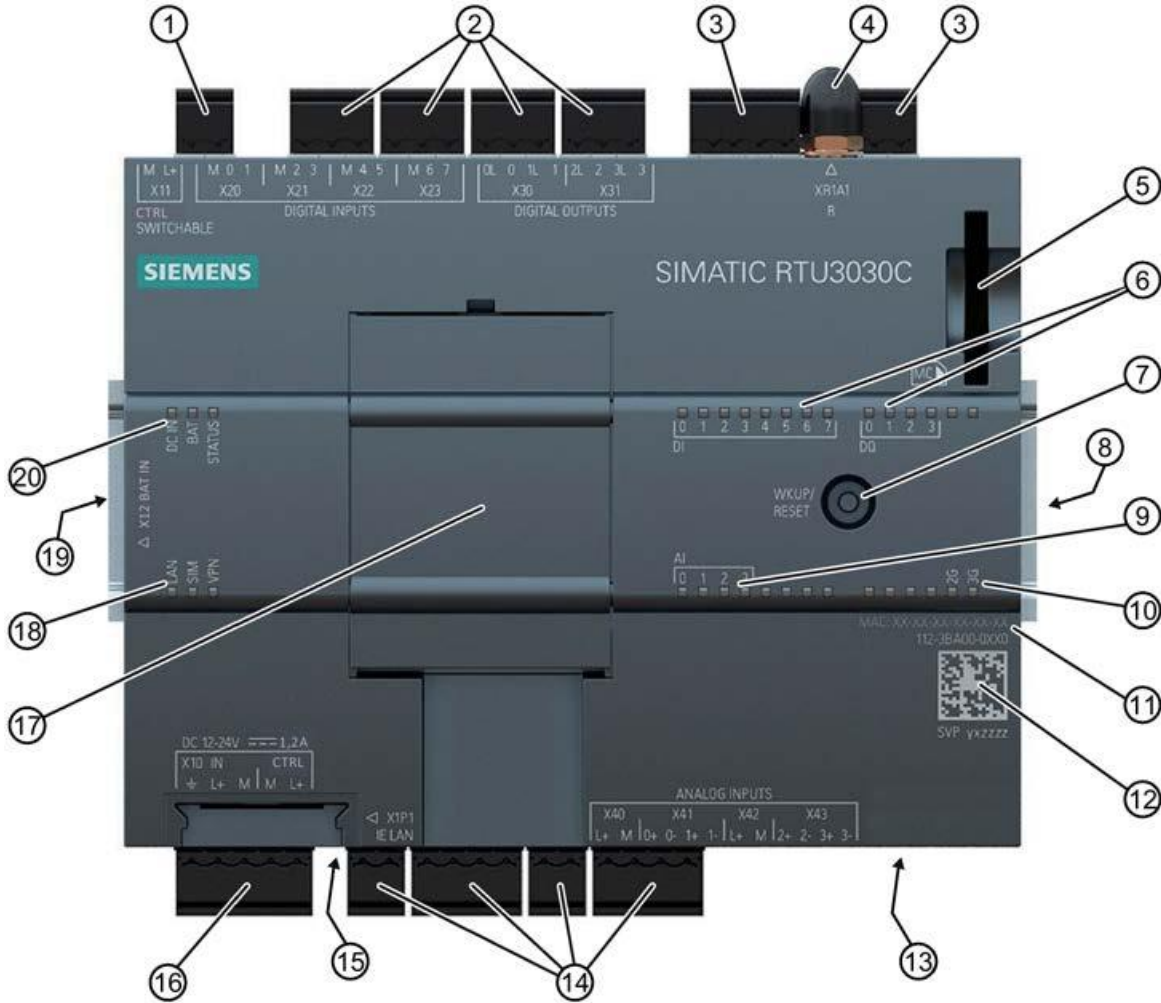
Readily available interfaces	SMA Antenna Socket (4)
	RJ-45 Socket (15)
	Service Interface (8)
	Power ON / Reset Button (7)
	SIM Receptacle (13)
	Slot for signal boards (17)
Power loss protection	Internal Battery
	External Battery (19)
Physical communication interfaces	SMA Antenna Socket (4) | GPRS
(Analyzed in the Logical Security)	RJ-45 Socket (15) | Ethernet
	Service Interface (8) | Proprietary
	Slot for signal boards (17) | Proprietary
Other readily available interfaces	SD card slot (5)
Actuators	4 digital outputs (2)
Inputs	8 digital inputs (2)
	4 analog inputs (14)

3.1.2 PHYSICAL ENCLOSURE PROTECTIONS

The following physical enclosure protections can be found in the device:

- The real measures are unknown. (I.E.:
- TORX screws, lock, glued/sealed screws, ultrasonically sealed plastic enclosure…
- Additional security is provided by a tamper-proof labeling for each of the screw holes)

3.1.3 INTERNAL BOARDS OVERVIEW

[INCLUDE INTERNAL BOARDS PHOTOGRAPHS / DIAGRAMS. These should clearly reflect where the external interfaces meet with the board.]

Internally available interfaces	UNKNOWN (I.E.: UART, JTAG, I2C/TWI, TTL)
Processor	UNKNOWN (IE: NXP MVF51NN152CMK50 BGA)
NV Storage	UNKNOWN (IE: JMICRON NAND512W3A2SNXE TSOP)
RAM	UNKNOWN (IE: JMICRON MT41K128M8DA-107:J BGA – NOTE: Epoxy covered)
GPRS Modem	UNKNOWN (IE: SIMCOM SIM5218 BGA)
Additional security	UNKNOWN (IE: Case open sensor, MEMS magnetic sensor, internal PIR sensor)

3.1.4 PORT PINOUTS

[INCLUDE PORT PINOUTS. For proprietary interfaces, the pinouts should also be provided. This shall allow the evaluator to determine if additional testing is needed for an interface.]

3.1.5 POTENTIAL PHYSICAL VULNERABILITIES

This section will include a list of the detected potential physical vulnerabilities. For a sample vulnerability, please refer to the Potential Logical Vulnerabilities section below.]

No apparent physical vulnerabilities have been found.

3.2 LOGICAL VULNERABILITY ANALYSIS (LOG-VA)

3.2.1 COMMUNICATION PROTOCOLS OVERVIEW

The communication protocols and related cryptography support available in the product are the following:

Control system communication protocols	TeleControl Basic [Proprietary] SINAUT ST7 [Proprietary] OpenVPN 2.3.4 Inside a mandatory OpenVPN tunnel, the following traffic can be found: DNP3 [DNP3 SPECIFICATION Version 2.x (2007/2009)] IEC 60870-5 [IEC 60870-5 Part 104 (2006)] Note: the TeleControl Basic scheme uses its own cryptography and authentication control, and it is not based on OpenVPN.
Internal protocols	HTTP SMS (GPRS)
Cryptography support	Inside OpenVPN: • TLS v1.0 up to v1.2 • AES-256-CBC • DES-168-CBC (DES-EDE3) • BF-CBC (Blowfish) • SHA1, SHA2(224,256) [REVIEW CSPN 3.3 – Specification of cryptographic mechanisms] The cryptography keys are stored in the /etc/ssl/ folder
TOE Operative System	Linux 3.16.50

3.2.2 THIRD PARTY COMPONENTS

The product includes the following third party libraries

Name	Version
OpenVPN	2.3.4
To be Completed	To be Completed

3.2.3 PUBLIC VULNERABILITY ANALYSIS

A PUBLIC VULNERABILITY ANALYSIS SHALL BE CONDUCTED, BY ANALYZING THE THIRD PARTY COMPONENTS USED, AND CHECKING THAT THEY ARE NOT AFFECTED BY PUBLICLY KNOWN VULNERABILITIES.

3.2.3.1 VULN-001 – OpenVPN denial of service (CVE-2014-8104)

The OpenVPN version in use by the developer is vulnerable to the vulnerability identified as CVE-2014-8104

OpenVPN 2.x before 2.0.11, 2.1.x, 2.2.x before 2.2.3, and 2.3.x before 2.3.6 allows remote authenticated users to cause a denial of service (server crash) via a small control channel packet.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8104

3.2.4 SOURCE CODE AUDIT

THE CSPN DEFINES THE FOLLOWING METHODOLOGY:

Give an expert opinion on the readability and structuring of the source code (examples of criteria: existence of comments, division into modules, typing of data, portability, etc.), specifying the modules that were viewed. It is possible to proceed by sampling.

USE OF AUTOMATED STATIC CODE ANALYSIS TOOLS MAY BE USEFUL IN THIS SECTION.

The audit can be limited to only the modules where security functionality has been implemented

TO BE COMPLETED

3.2.5 POTENTIAL LOGICAL VULNERABILITIES

Some potential vulnerabilities have been detected.

The vulnerability description should include information about how the vulnerability will compromise assets of the TOE. It should also clearly state where the vulnerability was identified.

3.2.5.1 VULN-001 – OpenVPN denial of service (CVE-2014-8104)

Origin: Third party components public vulnerability review

OpenVPN 2.x before 2.0.11, 2.1.x, 2.2.x before 2.2.3, and 2.3.x before 2.3.6 allows remote authenticated users to cause a denial of service (server crash) via a small control channel packet.

3.2.5.2 VULN-002 – SS7 impersonation

Origin: Design review

The TOE makes use of an internal phone book to keep track of which phone numbers are authorized to enable the administrative interface.

An attacker connected to the SS7 network of the telco provider would be able to examine the incoming connections to the base station, reading the SMS messages to be delivered to the TOE.

Once the attacker knows one authorized number, an attack can be carried out to force the TOE to constantly be in the "Active" operation mode, draining the system faster than intended, and therefore affecting the availability of the TOE.

Factor	Interval	Value
Elapsed Time	> 6 months	19

Expertise	*Expert*	*6*
Knowledge of TOE	*Public*	*0*
Window of Opportunity	*Unnecessary*	*0*
Equipment	*Specialized*	*4*
	Total Value	*29*
	Attack Potential Required	*Beyond High*
	Vulnerability Type	*Residual*

3.2.5.3   VULN-003 – Communication denial / base station impersonation

Origin: Design review

Tightly related to VULN-002, the attacker could instead of attacking the SS7 network, impersonate a base station, to either block the communications with the TOE, articulate a Man-in-the-Middle attack, or saturate the TOE with SMS's.

An attacker could set up a malicious base station to intercept, forge or block TOE communications

Factor	Interval	Value
Elapsed Time	*> 6 months*	*19*
Expertise	*Expert*	*6*
Knowledge of TOE	*Public*	*0*
Window of Opportunity	*Unnecessary*	*0*
Equipment	*Specialized*	4
	Total Value	29
	Attack Potential Required	Beyond High
	Vulnerability Type	Residual

3.2.5.4   VULN-004 – Log indiscernibility

Origin: Design review

An attacker could connect to the administration panel while this is being accessed by another administrator. The origin of the changes would be undistinguishable between the sessions.

Factor	Interval	Value
Elapsed Time	*> 6 months*	*19*
Expertise	*Layman*	*0*
Knowledge of TOE	*Sensitive*	*7*
Window of Opportunity	*Difficult*	*10*
Equipment	*Standard*	0
	Total Value	36
	Attack Potential Required	Beyond High
	Vulnerability Type	Residual

3.3 ENVIRONMENTAL VULNERABILITY ANALYSIS (ENV-VA)

No environmental analysis is to be executed under the TOE, as it is not dependent on its operating environment.

Therefore, as long as the environmental security assumptions are maintained (in particular, the **Premises** Security Profile assumption), the product should be secure.

3.4 ADDITIONAL SYSTEMS INTERACTION VULNERABILITY ANALYSIS (ASI-VA)

The interaction with other systems and components is only considered for ICCS-A evaluations.

4   PENETRATION TESTING

4.1   ICCAR TESTING

[A TEST BATTERY BASED ON THE IEC- 62443-4-2 SHOULD BE USED. THE SL-C LEVEL 3 IS RECOMMENDED AS A STARTING POINT. HOWEVER; THE TESTS SHOULD BE SPECIFIED BY THE PROTECTION PROFILE

PLEASE REVIEW THE NET DRAFT FOR MORE INFORMATION ON THE E2 TEST, AND THE CONCUSSIONS ON FUNCTIONAL TESTING.

How the TOE was set up should be included here. If special considerations or configurations have been made in a test, it should be included inside the test itself.

4.1.1   IAC – IDENTIFICATION AND AUTHENTICATION CONTROL

4.1.2   CR 1.1 HUMAN USER IDENTIFICATION AND AUTHENTICATION

Operations to be carried out	Expected Results	Observed results
The TOE will be configured with a single user account. An attacker will try to enumerate the registered users, to try to disclose sensitive information	The TOE will not disclose information about the valid users.	The evaluator was unable to enumerate the TOE users by a brute force attack, or information leakage in the error messages.
Conclusions		
The TOE does not disclose unwanted information about the registered users.		
Verdict	Pass	

4.1.3   CR 1.1 RE 1 UNIQUE IDENTIFICATION AND AUTHENTICATION

Test Case to be defined.

4.1.4   CR 1.1 RE 2 MULTIFACTOR AUTHENTICATION FOR UNTRUSTED INTERFACE

Test Case to be defined.

4.2   PHYSICAL PENETRATION TESTING (PHY-PT)

4.2.1   ENCLOSURE SECURITY REVIEW, COMMENTS AND VERDICT

The physical enclosure protections have been found to be sufficient taking into consideration the following operational environments:

- No physical access to the product is to be guaranteed to maintain the security properties. Some kind of external alarm system should be used to ensure this property.

Therefore, the physical enclosure protections verdict is **Pass**.

4.2.2 INTERNAL BOARD SECURITY REVIEW, COMMENTS AND VERDICT

No additional interfaces have been discovered during the TOE inspection

Furthermore, the operational environments and the enclosure security guarantee that no undetected board access will be available to an adversary.

Additional security measures are described, I.E.:

The RAM is protected by an epoxy layer, further increasing the difficulty of a local attack. An open case sensor activates a remote alarm if triggered.

TO BE COMPLETED

Therefore, the internal board security verdict is **Pass**.

4.2.3 EXPLOITED PHYSICAL VULNERABILITIES

No physical exploitation of any interface was achieved during the TOE physical penetration testing.

TO BE COMPLETED

As no outstanding physical vulnerability remains, the physical vulnerabilities verdict is **Pass**.

4.2.4 PHYSICAL SECURITY EVALUATION VERDICT

The following table provides an overview of the results of the physical security evaluation:

Physical enclosure protections	Pass
Internal board security	Pass
Physical vulnerabilities	None (Pass)

The system includes sufficient security to assure physical security, taking into account its operating environment, physical enclosure protections and internal board security.

Therefore, the physical penetration test verdict is **Pass**.

4.3 LOGICAL PENETRATION TESTING (LOG-PT)

4.3.1 NETWORK STRESS TESTING

[AS THE DEVICE IS A NETWORKED APPLIANCE, THE ISA SSA (System Security Assurance) NST (Network Stress Test) SHOULD BE MANDATORY, to try to guarantee operation, even under extraneous loads or messaging]

This tests should include network (OSI levels 3/4 and level 6 protocol) fuzzing, and load testing.

TO BE COMPLETED

4.3.2 PENETRATION TESTING

ADDITIONAL PEN-TESTING ACTIVITIES SHOULD BE CONDUCTED. THE RESULTS SHALL BE RECORDED IN THIS SECTION. This activities should focus on the seemingly most vulnerable protocols and physical interfaces.

TO BE COMPLETED

No exploits were identified during the penetration testing of the TOE.

Therefore, the penetration testing verdict is **Pass**.

4.3.3 POTENTIAL LOGICAL VULNERABILITIES

This section will contain the logical vulnerabilities, identified in the vulnerability analysis.

TO BE COMPLETED

4.3.3.1 VULN-001 – OpenVPN denial of service (CVE-2014-8104)

As the vulnerability known as CVE-2014-8104 only affects the Server portion of the OpenVPN software, and the TOE only makes use of the client portion and does not allow exposing an OpenVPN server, this vulnerability is **Not Exploitable**.

More information is available in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8104

4.3.3.2 VULN-002 – SS7 impersonation

The developer has acknowledged the vulnerability as residual. As such, it will be included in the certification report.

4.3.3.3 VULN-003 – Communication denial / base station impersonation

The developer has acknowledged the vulnerability as residual. As such, it will be included in the certification report.

4.3.3.4 VULN-004 – Log indiscernibility

The developer has acknowledged the vulnerability as residual. As such, it will be included in the certification report.

4.3.4 RESIDUAL LOGICAL VULNERABILITIES VERDICT

No exploitable vulnerabilities exist in the TOE. All of the residual vulnerabilities have been acknowledged by the developer, or have been solved.

Therefore, the residual logical vulnerabilities is **Pass**.

4.3.5 LOGICAL PENETRATION TEST VERDICT

The following table provides an overview of the results of the logical security evaluation:

ICCAR testing	Pass
Network stress testing	Pass
Penetration testing	Pass
Exploited logical vulnerabilities	None (Pass)
Residual logical vulnerabilities	Residual (Pass)

As all the sub steps for the logical security evaluation have passed, the logical security penetration test verdict is **Pass**.

4.4 ENVIRONMENTAL SECURITY PENETRATION TEST (ENV-PT)

As no environmental vulnerability analysis has been done, there is no penetration test for this tier.

Therefore, the environmental security penetration test verdict is **Not tested (Pass)**.

4.5 ADDITIONAL SYSTEMS INTERACTION (ASI-PT)

As no environmental vulnerability analysis has been done, there is no penetration test for this tier.

Therefore, the additional systems interaction security penetration test verdict is **Not tested (Pass)**.

BIBLIOGRAPHY

[CRITERIA] *Evaluation Criteria for the First Level Security Certification*, ANSSI, 2014

[METHODOLOGY] *Methodology for Evaluation for a First Level Security Certification*, ANSSI, 2014

GLOSSARY

Acronym	Description
CSPN	(FR) Certification de Sécurité de Premier Niveau (EN) First Leven Security Certification
ICCF	IACS component Cybersecurity Certification Framework
NIST	National Institute of Standards and Technology
IEC	International Electrotechnical Commission
FIPS	Federal Information Processing Standards
FIDO	Fast IDentity Online
SOG-IS	Senior Officers Group for Information Systems Security
RTU	Remote Terminal Unit
TOE	Target Of Evaluation
DNP3	Distributed Network Protocol
VIT	Vulnerability Identification Test
CRT	Communication Robustness Test
CEM	Common Methodology for Information Technology Security Evaluation
ICCAR	IACS Common Cybersecurity Assessment Requirements
ETR	Evaluation Technical Report
CC	Common Criteria
KRACK	Key Reinstallation Attacks
ASI	Additional Systems Interactions

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (**http://bookshop.europa.eu**);

- more than one copy or posters/maps:
  from the European Union's representations (**http://ec.europa.eu/represent_en.htm**);
  from the delegations in non-EU countries (**http://eeas.europa.eu/delegations/index_en.htm**);
  by contacting the Europe Direct service (**http://europa.eu/europedirect/index_en.htm**) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (**http://bookshop.europa.eu**).

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub