Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)

Feasibility study and initial recommendations for the European Commission and professional users

Paul THERON, Thales

2016

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure

Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)

JRC Science Hub
https://ec.europa.eu/jrc

JRC102550

ISBN 978-92-79-65842-6 - doi:10.2760/717579

Luxembourg: Publications Office of the European Union, 2016

How to cite this report: Paul Theron, Introduction to the European IACS components Cybersecurity Certification Framework (ICCF), doi:10.2760/717579

Contents

Abstract

The principal goal of this report is to propose an initial set of common European requirements and broad guidelines that will help fostering IACS cybersecurity certification in Europe in a manner fully compatible with practices adopted beyond. It describes the IACS component Cybersecurity Certification Framework (ICCF) and its elements and makes suggestions for its governance, adoption and implementation. This report is not intended to be a standard, nor aims at the establishment of new ones, as this effort's focus is to perform and publish a feasibility study that could foster the certification of IACS components in Europe.

1 Executive Summary

Year after year [1], the cybersecurity of IACS is compromised by old and emerging vulnerabilities that may take up to more than 200 days to be fixed once identified. Even if the in-depth cyber-defence of Industrial Automation and Control Systems (IACS) can be fully achieved only at the system level, it starts with fitting - into their basic components - security features that the system level will be able to leverage.

The ERNCIP "IACS cybersecurity certification" Thematic Group's collective decision, made in 2014[1], has been to encourage the provision of certified components as a contribution to improving IACS' in-depth cyber-defence. In 2014, vendors admitted that certification would have a limited impact on products' prices. Hence the view that IACS components' cybersecurity certification is globally viable, while, for the cheapest products, a smart alternative should be found in order to encourage enhancements.

EU-driven policy and strategies will stimulate new demands and offerings. Vendors, traditional and new ones as well, will respond by further innovation in their products so that altogether fostering IACS components cybersecurity certification will lead to enhanced Critical Infrastructure Protection. This last goal clearly bridges actions taken in various areas of competency of the European Commission[2] that, together, aim at transmitting to citizens a greater sense of security.

The principal goal of this report is to propose an initial set of common European requirements and broad guidelines that will help fostering IACS cybersecurity certification in Europe in a manner fully compatible with practices adopted beyond. It describes the IACS component Cybersecurity Certification Framework (ICCF) and its components and makes suggestions for its governance, adoption and implementation. This report is not intended to be a standard, nor aims at the establishment of new ones, as this effort's focus is to perform and publish a feasibility study that could foster the certification of IACS components in Europe.

For relevant bodies of the European Commission, this report shall be considered as an orientation and feasibility study that provides:

- High level support to the implementation of the NIS directive and other ad hoc strategies and policies;
- A framework that will help fostering IACS components cybersecurity certification by proposing an initial set of high level European requirements to that end;
- Four schemes aimed to motivate stakeholders to engage into IACS components cybersecurity certification at their own pace;

[1] On this matter, see the ERNCIP's TG report on "European IACS Components Cyber-security Compliance and Certification Scheme"

[2] On this matter, of particular relevance are the Commission Staff Working Document SWD(2013) 318 final "on a new approach to the European programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure" and Communication COM(2016) 410 final from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of Regions "on strengthening Europe's Cyber Resilience system and Fostering a competitive and innovative cyber security Industry".

- Clear and agnostic concepts and generic rules that do not conflict with European and international standards or schemes, present or future, but embrace them without increasing costs;
- Suggestions for further work to be carried out within and beyond the ERNCIP Project.

For professionals in vendor organisations, industries and certification-related bodies, this report describes the IACS component Cybersecurity Certification Framework (ICCF) with:

- A consistent initial set of high level European requirements;
- Sufficient elements for choosing the certification scheme applicable case by case;
- Freedom of choice as to which compatible standard to use;
- Easy-to-use, broad and flexible implementation guidelines.

The IACS component Cybersecurity Certification Framework (ICCF):

- proposes **four IACS Cybersecurity Certification Schemes** (ICCS):
    - ICCS-C1 (Self-declaration of compliance), section 4.2.4.1;
    - ICCS-C2 (Independent compliance assessment), section 4.2.4.2;
    - ICCS-B (Product cyber resilience certification), section 4.2.4.3 ;
    - ICCS-A (Full cyber resilience certification), section 4.2.4.4;
- … That involve up to three **Evaluation Activities**:
    - Compliance Assessment (in all four ICCS), section 4.2.5.1;
    - Cyber Resilience Testing (ICCS-B & A), section 4.2.5.2;
    - Development Process Evaluation (ICCS-A), section 4.2.5.3;
- … That require the guidelines and resources of **three Pillars**:
    - IACS Common Cybersecurity Assessment Requirements (ICCAR), section 4.2.6.1;
    - IACS Components Cybersecurity Protection Profiles (ICCPRO), section 4.2.6.2;
    - IACS Cybersecurity Certification Process (ICCP), section 4.2.6.3;
- And involves a **fourth pillar** for fostering and disseminating the ICCF:
    - IACS Cybersecurity Certification EU Register (ICCEUR), section 4.2.6.4.

In summary, this framework has been designed to be flexible, agnostic and to foster a fully-fledged approach:

- It shows vendors and buyers that engaging into IACS component Cybersecurity Certification can be easier as its layered schemes range from the least to the most demanding, for applications spanning from the ordinary to the most critical domains;
- It bridges with and embraces the use of existing and recognized IACS cybersecurity certification standards and schemes created or used in Europe and beyond. This feature should also help promoting mutual recognition of certificates across the Globe and to reduce the cost and complexity of duplicate efforts for the benefit of vendors whose market is international.
- It should also be beneficial to buyers and users who will hopefully be able to better see the big picture behind differences between standards and schemes.

The ICCF will be further evaluated and improved through a second phase of this feasibility study due in 2017. The proposed plan of action for 2017 includes governance, pilot projects, feedback studies, awareness raising campaign and a stakeholder consultation.

The present report provides to all interested and involved parties initial, broad guidelines to promote the use of the ICCF.

Feedback and inquiries should be communicated to:

Joint Research Centre

erncip-office@jrc.ec.europa.eu

2 Introduction

During the last six years, in its role of flagship Project - within the European Programme for Critical Infrastructure Protection (EPCIP) - the European Reference Network for Critical Infrastructure Protection (ERNCIP) has been mainly working on the initialization and maintenance of Thematic Groups (TG) with the focus of fostering the development of more advanced security solution for Critical Infrastructures across Europe. Among the nine currently running Thematic Groups, the one on Industrial Automation & Control Systems has been established in order to explore specific issues related to cybersecurity. The Group, established back in 2014, has initially worked on the identification of typical IACS configurations in view to properly scan the horizon and take decision on whether to focus on the cybersecurity of entire systems (as integrated in the industrial environment) or of single components. The analysis of the most recurring configurations, as gathered by the group, has led to the decision to work on the component level.

In this specific field, the Group has identified a huge gap in the European landscape, characterized by a missing framework for certifying and labelling[3] the cybersecurity of the components of IACS systems. Thanks to the mandate and sponsorship of partner Directorate General CNECT, the TG has then started working on a feasibility study for the establishment of a European Framework for the Certification of the Cybersecurity of IACS' components.

The initial steps toward this objective have been: 1) a stakeholder consultation in order to build consensus, recruit experts and fine tune the initial 2014 proposal; 2) a collection and analysis of common cybersecurity requirements from existing standards; 3) the development of the concept of Security Profiles, in order to frame cybersecurity evaluations; 4) the general specification and embryonic design of the IACS Cybersecurity Certification processes.

The need to undertake all of the aforementioned activities has pushed the JRC facilitators in widely promoting such effort in view to expand the Group's network. Participation to events organized by ENISA, ETSI's Cyber Technical Committee and CEN/Cenelec's Cybersecurity Coordination Group (CSCG) has led to the establishment of mutual support through the designation of observers. The observers are taking part in the ERNCIP thematic group with the aim of supporting the future project's activities, the stakeholder consultation and the recruitment of qualified experts in the following areas: standardization, certification process, cybersecurity, cybersecurity testing and the manufacturing of IACS components.

The Group's motivation in carrying out such an initiative stems from an analysis of the current European landscape. EU Member States are actively working on the implementation of Certification Schemes for the Cybersecurity of both IT and OT systems and components, as consolidated experiences show that certified products can contribute to the security of modern infrastructures. Many Governments have asked Information Security Agencies to define minimal requirements for technical standards for IT related equipment and they are already considering methods for widening these requirements and applying them also to Industrial Automation & Control Systems. This particular field requires a granular approach that should take into account the variety of

[3] Labelling is also intended to foster the European market of secured IACS products.

components currently integrated into industrial systems in order to asses which of them require enhanced focus and inclusion in certification schemes.

Another aspect that should also foster the establishment of cybersecurity certification schemes for IACS' components is the possibility that IACS' equipment manufacturers may have an easier access to the wider European market by obtaining a certification that is valid in the entire Union. Such benefit should avoid them to initiate a certification procedure in each Member State in which they'd like to offer their products. On an even wider scale, and in a later stage, the establishment of a European IACS component Cybersecurity Certification framework, based on recognised technical standards, may also lead to international mutual recognitions that should enable European manufacturers to sell their products in non-EU countries without having to re-obtain the certification of their products twice. The work carried on by the ERNCIP TG stands as a clear illustration of this intent to bridge with international practices as its European experts have discussed the feasibility of adopting testing requirements from a standard such as the IEC-ISO 62443 - Part 4-2 (Technical security requirements for IACS components) [2] supporting the ISA secure Conformance certification established in the USA (http://www.isasecure.org/en-US).

2.1 The history of the Thematic Group

When, in 2013, partner DGs and DG JRC gave mandate to this Group and the discussion started around this item, no one really had any set idea of what the IACS Thematic Group (TG) would have come-up with.

Since then, the ERNCIP IACS TG has gone through two successive phases:

- 2014 aimed at taking stock of the context, needs and requirements and to outline the principles of a European IACS cybersecurity certification framework;
- 2015 having been a time of reflection, communication to stakeholders and planning, 2016 saw the second phase of our TG, with a goal to deliver practical recommendations to the industrial systems community at large.

Since 2014, the TG's work has involved:

- National cybersecurity agencies;
- IACS vendors;
- Industrial companies;
- Integrators;
- Professional associations;
- Standardisation bodies;
- Academics and experts.

Together, the Members of the Group have made some determinant choices and have elaborated the propositions laid down in this report.

2.2 Considerations and choices

Three fundamental considerations have driven this work. Such considerations emerged naturally during the Group's work and discussions.

One unanimous view was that cybersecurity can be assured only at the system level, when basic IACS components, such as PLCs, are integrated within an environment where some dispositions may do for the cybersecurity weaknesses of components. On another hand, certifying the cybersecurity of an IACS, or of a subsystem, was deemed too difficult as the configuration of an IACS is complex and varies. Besides, everyone agreed that it would be better for industries to buy cybersecurity-certified components rather than non-certified products, as a manner of introducing a basic brick of in-depth cyber-defence of IACS.

- Hence the choice the TG made collectively to focus on IACS components, not subsystems and even less on systems as a whole. The present report exposes the elements and features of a cybersecurity certification framework (ICCF) the scope of which is only IACS products, and therefore the focus is on the component level.

Another thought the TG had in mind was about how to engage both vendors and buyers into delivering and buying cybersecurity-certified products. A complicated scheme, leading to very few certified products, would be a deterrent, just as a light one would be. And the way a stakeholder may wish to approach IACS components certification may vary according to circumstances (target market, type of products, customer requirements, etc.)

- As a possible solution, this report presents four schemes (ICCS-n) that compose the framework, where ICCS-C (1 & 2) allows vendors to take an easy, low cost step towards proposing cyber-secured products, while ICCS B may be requested for supplying products to critical infrastructure operators, and ICCS-A matches the most demanding needs of vital and sensitive users such as Defence or the nuclear industry for instance. In some cases, these last two schemes may be already reflected into national legislations.

The third consideration at the very root of this work was to make IACS products' certification as cheap and widely recognised as feasible. Easy to say, less so to achieve. During phase 2, the TG worked closely with experts from ISA and NIST (e.g. on the SP800-82 guidebook), and the TG also consulted SOG-IS and experts whose competence lies with Common Criteria (ISO 15408).

- This report's main objective and ambitious goal is to present choices that may maximise the chances of mutual recognition of certificates while simplifying certification itself.

This report proposes:

- Some orientations sought to provide guidance to the European Commission to boost progress in Critical Infrastructure Protection (CIP) by fostering IACS cybersecurity certification;
- Guidelines aimed at helping vendors, buyers and laboratories to engage into IACS cybersecurity certification.

2.3 Contents of the report

Section 4 presents the IACS component Cybersecurity Certification Framework (ICCF). Section 5 presents a proposed ICCF Multilevel Governance Process. Section 6 gives a few suggestions to professional users in order to facilitate their engagement in the use of the ICCF. Section 7 presents the potential plan of action for 2017. Section 8 consists in a series of annexes that may be of interest to readers and constitute the "ground truth" of the Group's debates. A table of illustrations and a list of referenced source documents are also provided at the end of the report.

2.4 Contributions

In alphabetical order, participants of the Thematic Group's plenary meetings have been in 2016:

- William Billotte, NIST, USA
- Sandro Bologna, Italian Association Critical Infrastructure Protection, Italy
- Antonin Briard, Gimelec, France
- Jean-Michel Brun and Laurent Platel, Schneider-Electric, France
- Scott Cadzow, UK
- Carlos Canto, INCIBE, Spain
- Mathieu Feuillet, Thomas Galliano, Eric De Saint-Maurice and Romain Muguet, ANSSI, France
- José Ruiz Gualda, APPLUS, Spain
- Chris Hankin, Imperial College, UK
- Miguel Garcia-Menendez, CCI, Spain
- Georgios Giannopoulos, DG JRC, Ispra
- Philippe Jeannin, RTE-France
- Alessandro Lazari, DG JRC, Ispra
- Jean-Christophe Mathieu and Pierre Kobes, Siemens, Deutschland
- Jos Menting, ENGIE, Belgium
- Nuno Pereira, EDP, Portugal
- Hector Puyosa, SABIC, Spain
- Andre Ristaino, ISA, USA
- Konstantin Rogalas and Sinclair Koelemij, Honeywell
- Stefan Rutten, DEKRA, Deutschland
- Gian-Luigi Ruzzante, DG JRC, Ispra
- Andreas Teuscher, SICK, Deutschland
- Aristotelis Tzafalias and Domenico Ferrara, DG CNECT, European Commission
- Jens Wiesner and Jens Mehrfeld, BSI, Deutschland

In alphabetical order, external liaisons of the Thematic Group have been:

- Sonia Compans and Carmine Rizzo, ETSI (Cyber TC);
- Janusz Górski, GDA Poland (European Workshop on Industrial Computer System Reliability, Safety and Security EWICS);
- Volker Jacumeit, DIN, Deutschland (for CEN/Cenelec's Cybersecurity Coordination Group – CSCG);
- Rossella Mattioli, ENISA (ICS and Euro-SCSIE Groups).

Special thanks go to Antonin BRIARD, Gimelec, France, for his contribution on Protection Profiles.

Special thanks go to Sandro BOLOGNA, Italy, for his contribution on certification processes.

The report has been reviewed by:

- Sandro Bologna;
- Antonin Briard;
- Jean-Michel Brun and Laurent Platel;

- Scott Cadzow;
- Thomas Galliano and Romain Muguet;
- Miguel Garcia-Menendez;
- Philippe Jeannin;
- Alessandro Lazari;
- Jean-Christophe Mathieu and Pierre Kobes;
- Jos Menting;
- José Ruiz Gualda;
- Andre Ristaino;
- Andreas Teuscher;
- Jens Wiesner and Jens Mehrfeld.

3 List of abbreviations

The following acronyms and terms are used in this report:

Entry
CRT = Communication robustness testing
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's DG Joint Research Centre (located in Ispra, Italy)
PLC = Programmable Logic Controller
RTU = Remote Terminal Units
SCADA = Supervisory Control and Data Acquisition
SDSA = Software development security assessment
TOE = Target of Evaluation
VPN = Virtual Private Network

For further details about terms and concepts used in this report, see section 8.4.

4 The IACS component Cybersecurity Certification Framework (ICCF)

4.1 Roles in the ICCF

4.1.1 Buyer

A buyer is an organisation that purchases and uses an IACS product and is impacted by its security. A buyer defines security requirements for the products he intends to buy. He may request that an IACS product holds an ICCF-Label (ICCS-C2) or ICCF-Certificate (ICCS-B & ICCS-A) as a guarantee of security. System Integrators may be the primary buyers of IACS components.

4.1.2 National Cybersecurity Authority

A National Cybersecurity Agency is a governmental body in charge of elaborating and enforcing the legislation, regulation, or rules stemming from international or national standards, which drive the progress and provide guarantees of IACS' cyber resilience.

4.1.3 Vendor (Product supplier)

A supplier is a person or an organization that provides products or services. Suppliers can be either the creators of a product, its distributors, its installers or integrators. In this report the vendor is the company designing and manufacturing the IACS product. System Integrators who create composite products out of several components may also be considered as vendors. Vendors should be responsible for 3rd-party libraries and other components embedded in a product.

4.1.4 Certification Authority (Certifier)

A Certification Authority is an organization either chartered by the ICCF Governance Board and accredited by an Accreditation Body to deliver Labels (ICCS-C2), or operated by a National Cybersecurity Agency that delivers Certificates (ICCS-B & ICCS-A) attesting that an IACS product complies with its Security Profile, the latter stemming from legislation, regulation, standards or contractual requirements for instance. ISO/IEC 17065:2012 (Conformity assessment -- Requirements for bodies certifying products, processes and services) is the standard of reference for certifiers' accreditation.

4.1.5 Laboratory

A laboratory is an independent organisation chartered by the ICCF Governance Board and accredited by an Accreditation Body to perform ICCF evaluation activities according to specified and agreed standards, processes and rules, and to submit their results to a certifier as evidence towards the delivery of a Label (ICCS-C2) or Certificate (ICCS-B & ICCS-A). ISO/IEC 17025:2005 (General requirements for the competence of testing and calibration laboratories) is the standard of reference for laboratories accreditation.

4.1.6 Accreditation Body

An accreditation body is a regulated body allowed to give formal recognition that another Body (Certification Body, Laboratory) is competent to carry out the specific tasks in its remit by controlling that the organisational requirements specified in a reference standard are met by the latter.

Only one accreditation body is established per country. in France, for example, COFRAC is the accreditation body. When it comes to cybersecurity certification, the accreditation assessment may not evaluate precisely the required technical competencies. In France, the National Cybersecurity Agency (ANSSI) therefore evaluates and licenses laboratories from a technical skills perspective on top of COFRAC's accreditation (http://www.ssi.gouv.fr/entreprise/produits-certifies/cc/procedures-et-formulaires).

4.1.7 Licensing bodies

Accreditation bodies should therefore not be confused with Licensing Bodies. The latter may be either national cybersecurity agencies or standard-related licensing bodies (e.g., Common Criteria Recognition Arrangement). Their role is to allow bodies (like laboratories) selected on the basis of a specified evaluation process to perform specified activities (like assessments or tests) on their behalf.

4.1.8 ICCF Governance Board

The ICCF Governance Board (IGB) is the organisation that governs the elaboration, dissemination, use and maintenance of the ICCF and recognises Certification Authorities and Laboratories to perform ICCF related duties.

As of 2016, the ICCF Governance Board is the ERNCIP Thematic Group's plenary meeting as part of the TG's Project 1. Its membership should be further defined in a later stage.

Should the ICCF be adopted on some form of European scale, the IGB should be organised ad hoc. It should set-up all needed liaisons with the European Commission, Standardisation Bodies, international and national Accreditation Bodies, Certification Authorities, Laboratories, Vendors and Industries (buyers) and their respective professional bodies. The IGB should be developed so as to make sure that the framework bridges with and embraces national schemes.

4.1.9 The European Commission

The European Commission, through the Joint Research Centre (Ispra), stimulates and supports the ICCF endeavour, provides or relays European orientations and puts in place or supports the liaisons with partner DG CNECT, with Member States or with European Agencies (ENISA for instance) and European Standardisation Bodies (CEN-CENELEC, ETSI, etc.).

The European Commission, together with other competent bodies may also help disseminating or encouraging the use of the ICCF.

4.1.10 Standardisation Bodies

International and European Standardisation Bodies issue and maintain the standards that the ICCF refers to. In that capacity, the ICCF Governance Board and Standardisation Bodies should liaise when new versions of standards or new ones are scheduled to be developed.

4.2 The ICCF

4.2.1 Introduction

The ICCF aims at providing professionals within vendor, industry, laboratory and certification organisations with guidelines to help IACS components' cybersecurity certification take place in a smoother and easier way, at a controlled cost, and with recognition within and beyond European borders.

Cybersecurity certification may be needed in civil contexts or in the context of Defence and other highly critical domains and systems such as Space or the Nuclear Industry.

The proposed IACS component Cybersecurity Certification Framework (ICCF) implements the *evaluation* activities forming its evaluation pathways presented in section 4.2.2.

4.2.2 Definitions and the ICCF evaluation pathways

In the context of the present report, evaluation activities may be defined as follows:

- EVALUATION
  "Evaluation" is understood as an "*activity meant to judge the security of a product against the requirements of its Security Profile*" (see section 4.2.6.2 for a definition of a Security Profile). Evaluations may take one or either of two forms: assessments and testing.

- ASSESSMENT
  [Compliance] assessment (or compliance evaluation) may be defined by reference to ISO/CEI 17000:2004 - definition 2.1 as the "*demonstration that the requirements specified for a product in its Security Profile have been addressed by appropriate measures*". In the context of the present report, two types of assessments have been identified: compliance assessments, which evaluate the conformance of an IACS product's design to reference requirements; and product development process assessments, which evaluate the conformance of a product's development process to a specified standard or set of requirements.

- TESTING
  In the context of the present report, testing may be defined as checking that an IACS product effectively delivers the cybersecurity and cyber-defence features that its document asserts.

- CERTIFICATION
  Certification can be defined as the delivery by a certification authority of a *certificate* that guarantees that an IACS product has successfully completed the certification process on the basis of the validation (recognition of validity) of an evaluation report. In the context of the present framework, such a report is produced out of the evaluation activities of the ICCS-B and ICCS-A schemes.

- LABELLING
  Labelling can be defined as the delivery by a certification authority of a *label* that attests that an IACS product has successfully completed the labelling process on the basis of the validation (recognition of validity) of an evaluation report. In the context of the present framework, such a report is produced out of the evaluation activities of the ICCS-C2 scheme. A label gives no guarantee but provides an indication of the cybersecurity and cyber-defence features that the vendor claims to have fitted into an IACS product.

- SELF-DECLARATION
  Self-declaration can be defined as the vendors' assertion that one of his IACS products has been submitted by his own teams to an assessment of its compliance against a set of reference requirements.

The following diagram summarises the different pathways within the ICCF:

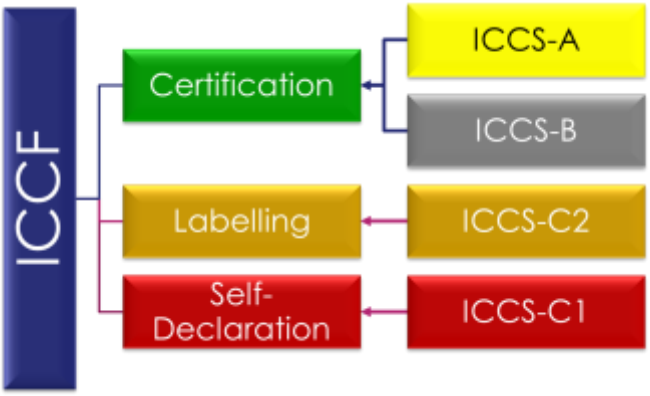

Figure 1 The ICCF evaluation pathways

4.2.2.1 Scope of the ICCF and general rules

Evaluations may be ruled either by guidelines, standards, or regulatory or legislative requirements.

An evaluation relates to a specific product and its associated Security Profile, not a "family of products".

In the present context, the process of any form of cybersecurity evaluation is based upon a product's Security Profile that specifies the security requirements that the product is expected to meet.

The product's Security Profile must specify clearly security requirements specific to a given operating environment. It is mainly the target system's owner's responsibility to specify the product's Security Profile.

The evaluation process complies with established best practices. This process is agreed between all parties involved: vendor, buyer, laboratory, certification authority.

When a product (in the context of this report) has been evaluated successfully by an accredited laboratory, a form of "certificate" or "label" is delivered by a certification authority to the vendor of this product under the condition that the certification authority validates the evaluation report provided by the laboratory.

4.2.2.2 Cyber resilience, cybersecurity and cyber defence

In the context of this report, cyber resilience and associated notions may be defined as follows:

- CYBERSECURITY
  It is the prevision of, prevention of, and protection against illegal, unsolicited, intentional, unintentional adverse events that may affect Industrial Automation & Control Systems or their components, such as penetration, disturbing interferences with or inhibition of their proper and intended operation, inappropriate access to or loss of integrity of information, denials of service, etc.
    - **Prevision** refers to mechanisms seeking to anticipate cyber threats that may target IACS or their components;
    - **Prevention** refers to mechanisms seeking either to reduce cyber threats at their source or at least to deter hostile agents to act;

- **Protection** refers to mechanisms seeking to set-up defence measures allowing to reduce the likelihood of the manifestation of cyber incidents or attacks that may derive from residual threats and that would cause some form of damage or disturbance to the operation of IACS or their components;

- CYBER DEFENCE
  It is the faculty of IACS or of their components to withstand such adverse events if and when they happen despite prevention and protection measures. This implies recognising, responding to and rebounding from them.

  - **Recognition** refers to mechanisms allowing an IACS or one of its components, or a dedicated (external) device or system, or its operators to detect and signal a cyber-incident or attack if and when it occurs;
  - **Response** refers to mechanisms allowing an IACS or one of its components, or else an ad hoc work force or system, to absorb / tolerate, contain, mitigate and stop a cyber-incident or attack and restore the IACS' nominal capacities;
  - **Rebound** refers to mechanisms allowing an IACS or one of its components, or else an ad hoc work force, to learn from experience and improve or adapt the IACS or component's operating capacity.
- CYBER RESILIENCE
  In the context of this report cyber resilience is the combination of cybersecurity and cyber defence [3]:

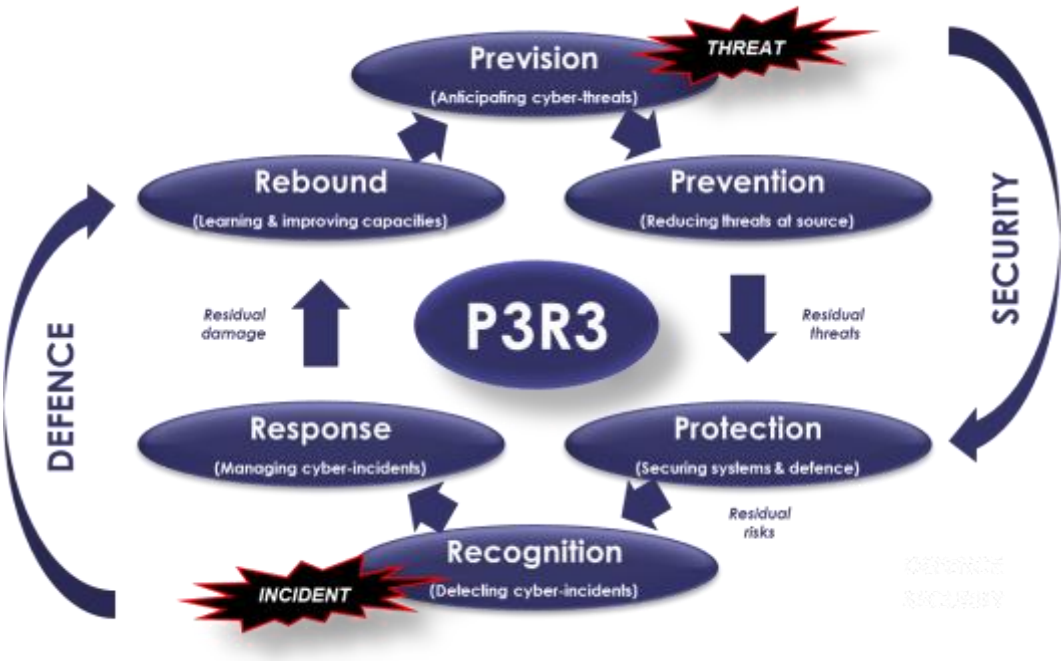

Figure 2 The P3R3 model of cyber resilience mechanisms

4.2.3 Structure of the ICCF

As anticipated in the summary of this report, the IACS component Cybersecurity Certification Framework (ICCF):

- Relies upon **four IACS Cybersecurity Certification Schemes** (ICCS)…

- ICCS-C1, section 4.2.4.1.
- ICCS-C2, section 4.2.4.2.
- ICCS-B, section 4.2.4.3.
- ICCS-A, section 4.2.4.4.

- … That involve up to three **Evaluation Activities**…
  - Compliance Assessment, section 4.2.5.1;
  - Cyber Resilience Testing, section 4.2.5.2;
  - Development Process Evaluation, section 4.2.5.3;
- … That require the guidelines and resources of **three Pillars**:
  - IACS Common Cybersecurity Assessment Requirements (ICCAR), section 4.2.6.1;
  - IACS Components Cybersecurity Protection Profiles (ICCPRO), section 4.2.6.2;
  - IACS Cybersecurity Certification Process (ICCP), section 4.2.6.3;
- And involves a **fourth pillar** for fostering and disseminating the ICCF:
  - IACS Cybersecurity Certification EU Register (ICCEUR), section 4.2.6.4.

The general structure of ICCF components is summarised in the following diagram:

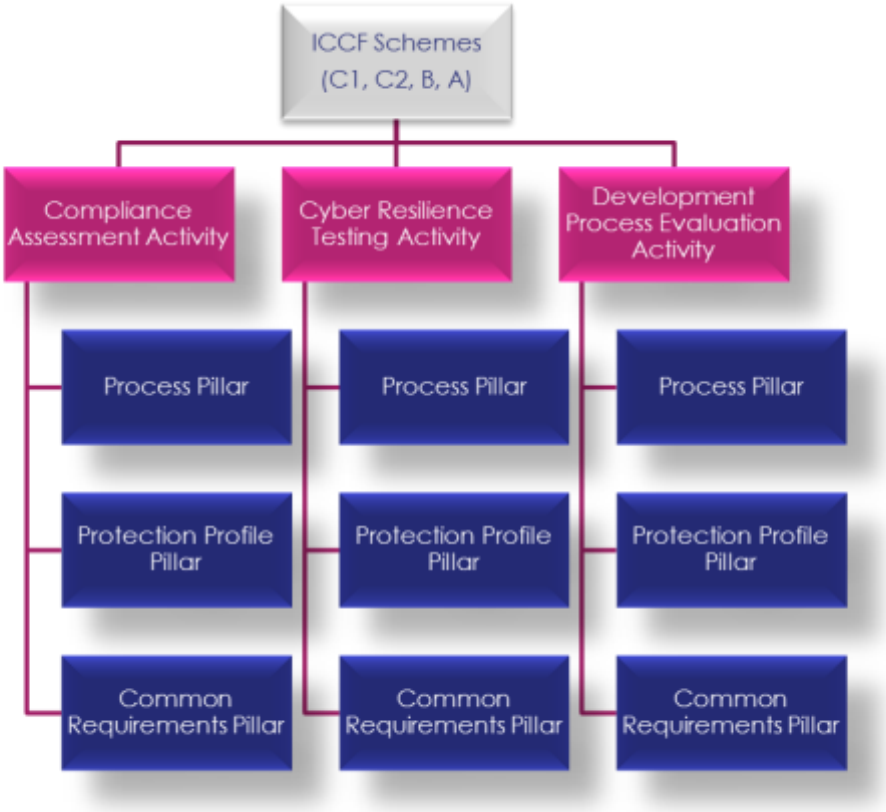

Figure 3 General structure of the ICCF

4.2.4 The IACS Cybersecurity Certification Schemes (ICCS) of the ICCF

The ICCF proposes four possible approaches to certification in the form of four "schemes" named IACS Cybersecurity Certification Schemes (ICCS). The following diagram recapitulates these four

schemes. Definitions follow and the labels proposed[4] for marking certified products, i.e. those that passed the evaluations with success, are presented in regard of each scheme.

Figure 4 The ICCF schemes (ICCS)

4.2.4.1 ICCS-C1: Self-declaration of compliance

ICCS-C1 implies the delivery of no label. It is a mere self-declaration of compliance scheme providing vendors who target non-sensitive markets with an easy, low cost way to declare on paper to their customers that they cared about a product's cybersecurity by fitting into it the cybersecurity mechanisms matching the requirements of its Security Profile. Both the Security Profile of the product and its compliance matrix must be documented. The following mention (suggestion) "ICCF / ICCS-C1 Self-Declaration of Compliance" appears on a carmine-red background (suggestion also):

4.2.4.2 ICCS-C2: Independent compliance assessment

ICCS-C2 is a compliance assessment scheme run by an independent organisation and providing vendors targeting non sensitive markets with an easy, low cost, independent assessment of a product in order to demonstrate on paper that the requirements specified for the product in its Security Profile have all been addressed by appropriate measures. Both the Security Profile of the product and its compliance matrix must be documented. The following label indicates "ICCS-C2 Independent Compliance Assessment" in white on a bronze background (suggestion):

[4] These graphic marks are only indicative and will need to be further validated and elaborated during the second phase of this feasibility study (to take place in 2017).

4.2.4.3 ICCS-B: Product cyber resilience certification

ICCS-B is a product cyber resilience certification scheme run by an independent organisation for vendors targeting critical infrastructure markets and who need to demonstrate, on top of an ICCS-C2 evaluation, the effective ability of a product to satisfy the requirements of its Security Profile. Both the Security Profile of the product, its compliance matrix and its test results must be documented. The following label indicates "ICCS-B Cyber Resilience Certificate" on a label displayed in white on a silver background (suggestion):

4.2.4.4 ICCS-A: Full cyber resilience certification

ICCS-A is a full cyber resilience certification scheme run by an independent organisation for vendors targeting highly critical markets and who need to demonstrate, on top of ICCS-B evaluations, that their product has been developed in a controlled manner to eliminate systematically involuntary and malevolent opportunities to introduce vulnerabilities. The following label indicates "ICCS-A Full Cyber Resilience Certificate" on a label displayed in black on a gold background (suggestion):

4.2.5 Evaluation activities performed in ICCS schemes

Within each ICCF scheme three types of evaluation activities can be performed as indicated in the following diagram. They are described in the next subsections:

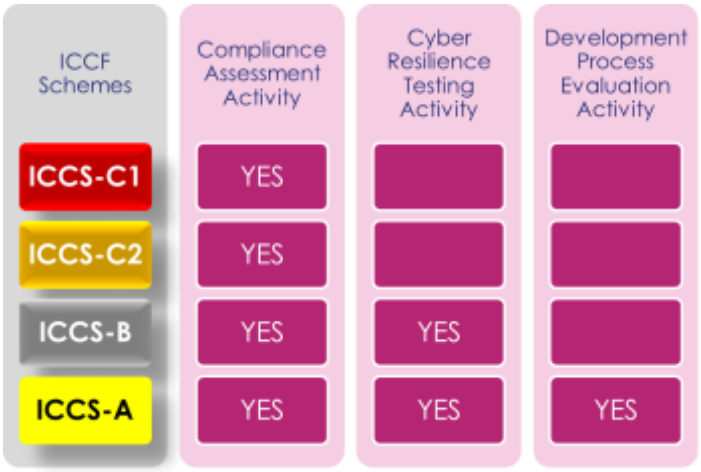

Figure 5 Evaluation activities performed in each ICCF scheme

4.2.5.1 Compliance assessment

Compliance assessment is the evaluation activity consisting in analysing an IACS product's documentation in a systematic manner in order to demonstrate on paper that the requirements specified for this product in its Security Profile have been addressed by appropriate measures (protection measures most of the time, but possibly measures referring also to other P3R3 mechanisms).

In the context of the ICCF, the Security Profile of a product specifies compliance assessment requirements (Figure 22) by proposing a reference to (IEC 62443-4-2, Draft 2, Edit 4, July 2, 2015).

4.2.5.2 Cyber resilience testing

Cyber resilience testing is the evaluation activity consisting in performing all tests required to demonstrate the effectiveness of an IACS product's cybersecurity and cyber defence (Figure 2) mechanisms (Figure 9) evidenced in its compliance assessment in reference to its Security Profile. (ASCI EDSA-100 Version 2, 2011) proposes "Communication robustness testing (CRT)" for instance. Penetration Testing is another kind of tests that allow assessing the resilience to attacks and incidents of IACS components or of their parts targeted either directly or indirectly (through attacks affecting other components or parts). Both hardware and software should be evaluated.

NB: A standard taxonomy of these tests should be elaborated in the future.

4.2.5.3 Development process evaluation

The development process evaluation consists in demonstrating that a product has been developed in a controlled manner to eliminate systematically involuntary and malevolent opportunities to introduce vulnerabilities. For instance, (ASCI EDSA-100 Version 2, 2011) [4] proposes a Software development security assessment (SDSA). Hardware should also be the object of similar evaluations.

4.2.6 The pillars of the ICCF

The ICCF operates on 3 pillars providing the resources that evaluation activities require:

- IACS Common Cybersecurity Assessment Requirements (ICCAR) that provides the set of common requirements needed for compliance assessments across all ICCF schemes;
- The IACS Components Cybersecurity Protection Profiles (ICPRO) that provides the framework needed to elaborate IACS products' Security Profiles;

- The IACS Cybersecurity Certification Process (ICCP) that describes the processes and sub-processes required to run each ICCF scheme and evaluation activity.

Another ICCF pillar was designed to disseminate and foster the implementation of the ICCF:

- The IACS Cybersecurity Certification EU Register (ICCEUR) that exposes on the JRC's website the elements and information regarding the ICCF that are useful to market stakeholders (vendors, buyers, certification authorities, laboratories).

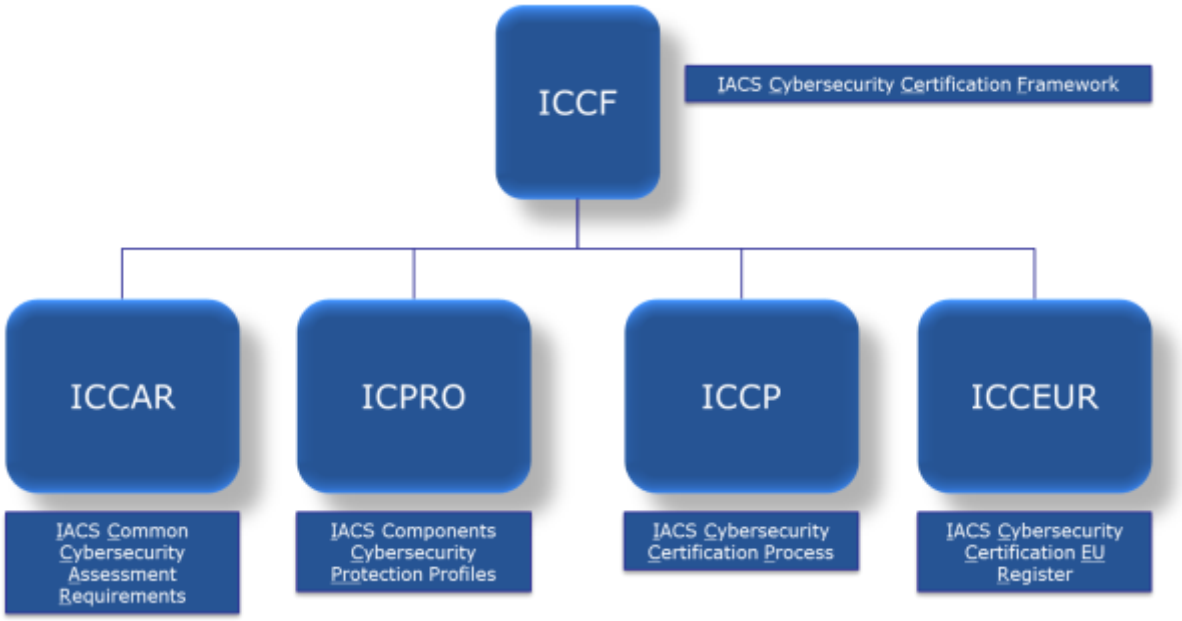

Figure 6 The ICCF's pillars

4.2.6.1 IACS Common Cybersecurity Assessment Requirements (ICCAR)

4.2.6.1.1 Introduction and choice

The IACS Common Cybersecurity Assessment Requirements (ICCAR) pillar provides the basic set of cybersecurity requirements needed for the compliance assessment of an IACS product, whatever the selected ICCF scheme.

As the IEC 62443-4-2 standard was designed to provide such a set of requirements, our ERNCIP Thematic Group (TG), after plenary discussions involving ISA, has suggested that it could be adopted as a source of Common Requirements.

The decision to adopt IEC 62443 standard as our reference for ICCAR constitutes not only a gain in time and effort for the TG but also already a bridge between the ICCF and the IEC 62443 standard.

4.2.6.1.2 Concepts and definitions

A common requirement in the sense of the present report is the conjunction of four concepts found in IEC 62443-4-2:

- FOUNDATIONAL REQUIREMENT (FR):
  Seven types of foundational requirements are identified in IEC 62443-4-2. They are:

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA).

- COMPONENT's CAPABILITY SECURITY LEVEL (SL-C):
  Four security levels are identified in IEC 62443-4-2. They are numbered from 1 to 4.

  NB: This notion is defined in the standard for each Foundational requirement. They need to be explicitly defined in protection profiles and Security Profiles.

- TYPE OF COMPONENTS UNDER EVALUATION (TCE):
  Four types of components are identified in IEC 62443-4-2. They are:

  - Embedded component (E);
  - Network component (N);
  - Host component (H);
  - Application (A).

  NB 1: This taxonomy is very generic. In real-life evaluations, each product will be of a more specific type.

  NB 2: Some requirements apply to all types of components.

- COMPONENT SECURITY REQUIREMENT (CR):
  Component Requirements (CR) in IEC 62443-4-2 are "*derived from system requirements (SRs) in IEC 62443-3-3*".

  Component requirements (CR) come in the form of two types of detailed Component Security requirement are identified in IEC 62443-4-2. They are:

  - System Requirements (SR);
  - Requirement Enhancements (RE).

  At SL-C #1, only System Requirements apply. Requirement Enhancements apply as security levels get higher.

  Component security requirements can be associated with specific types of components, in which case they are named as follows (IEC 62443-4-2, Draft 2, Edit 4, July 2, 2015):

  - ACR: Application Component Requirement
  - ECR: Embedded device Component Requirement
  - HCR: Host device Component Requirement
  - NCR: Network device Component Requirement

  The full list of CRs can be found in section 8.1, Figure 22.

4.2.6.1.3 Conceptual model of component security requirements (CRs)

The following Entity-Relationship (data) model [5] [6] describes the relationship between the concepts that define component security requirements in IEC 62443-4-2 (note that this model differs somehow from the one found in IEC 62443-4-2; this is due to the difference in modelling technique):

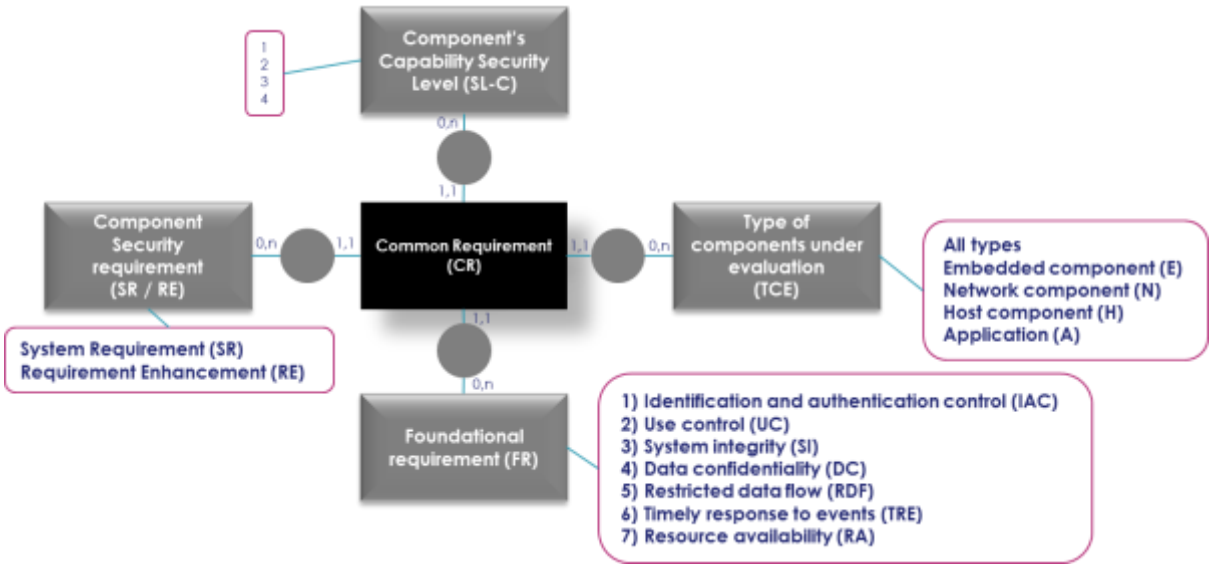

Figure 7 Common component security requirement data model

NB1: Cardinalities set on relationships mean the minimum and maximum number of occurrences of entities that can be associated with a given entity under consideration. For instance, a CR may be of 1 and 1 only type (TCE); or to a component capability security level (SL-C) there can be no (0) associated common requirement (CR) but also there can be "n".

NB2: Entities' properties are listed within rounded rectangles attached to them. They represent the set of values that an entity may take.

NB3: Small circles represent the association between two (or more) entities.

4.2.6.1.4 Basic rules for selecting applicable requirements

The values (within the rounded rectangles attached to entities) of each entity in the above model represent the criteria that can be used to select the set of security requirements applicable to an IACS product.

NB1: Section 4.2.6.2 provides further guidelines for defining requirements applicable to specific IACS products.

NB2: The effective set of requirements applicable to an IACS product / component may also depend on factors such as the *reliance on compensating countermeasures* (see IEC 62443-3-2 for details).

4.2.6.1.5 Validity of compliance assessment results

To be trustworthy, a compliance assessment requires:

- To be performed by a laboratory accredited by an accreditation body, and possibly or as required[5] licensed by a National Cybersecurity Agency or the authority governing the IACS component Cybersecurity Certification Framework (the ICCF Governance Board);
- To be driven by a well-established, documented and agreed (or shared) Security Profile that specifies the security requirements to be evaluated as well as their rationale;
- To be conducted according to a well-established, documented and agreed (or shared) process that specifies who must do what, when and how;
- To be documented both in terms of how and in which conditions the assessment was effectively performed, the difficulties it encountered and the results that it yielded;
- To be verified and approved by independent reviewers and approvers;
- To be attested by an accredited certification authority;
- To be officially communicated to the entity (vendor mainly) who asked for the evaluation.

4.2.6.1.6 Management of the ICCAR

The ICCAR is the basic resource for compliance assessments. The decision was made to make IEC 62443-4-2's component requirements an ICCAR's list of requirements.

As ISA (the standard's authoring body) may revise this standard in the future, and as experience may demonstrate the need to revise the ICCAR list of requirements, or for any other reason that might suggest or imply change, a controlled maintenance process should be defined.

4.2.6.1.7 References and bridges

(IEC 62443-4-2, Draft 2, Edit 4, July 2, 2015) is the main reference for this pillar of the ICCF.

> NB: At the time the present report was written, the IEC 62443-4-2 standard was not yet officially released. Working with this standard was made possible only with the help of ISA representation in our Thematic Group.

See also (ASCI EDSA-100 Version 2, 2011) and annex 8.4.

4.2.6.2 IACS Components Cybersecurity Protection Profiles (ICPRO)

4.2.6.2.1 Introduction

The IACS Components Cybersecurity Protection Profiles (ICPRO) pillar provides the framework for specifying the security requirements associated with a given IACS product / component that is to be evaluated and sold by a vendor.

> Comment: Generally, a given IACS "product" / component has a branding name and a specific vendor reference. It is sold in numbers and each item / occurrence may have a serial number.

There are two levels of definition of a product's security requirements:

- Level 1: the definition of a **Protection Profile** (PP) for the family of products in which specific products to be evaluated belong;

[5] This aspect has not yet been discussed, but for instance (ASCI EDSA-100 Version 2, 2011) specifies the need for test laboratories to be chartered, and this would provide better control over the quality of evaluations and evaluation bodies involved in the ICCF.

- Level 2: the definition of a **Security Profile** (SP) for the specific product under evaluation; a product's SP may be derived from the family's generic PP.

These concepts and their relationship are explained in the next subsections.

Elaborating, validating, publishing and maintaining PPs and SPs require a process, and even the more so as the ICCF is intended for Europe (and beyond) in a multi-stakeholder market.

Creating SPs requires an SP generation process to be used by vendors, buyers, certification authorities and laboratories.

Publishing or protecting PPs and SPs depends on their confidentiality and the kind of markets they are meant for. Sector-specific rules must be defined and implemented in relevant circumstances.

These processes and rules are also explained in the next subsections.

Annex 8.2 provides further details about the rationale of the propositions elaborated by the Thematic Group and presented in the current section.

4.2.6.2.2 Concepts and definitions

In this report the following definitions apply:

- PROTECTION PROFILE (PP)
  A **Protection Profile** (PP) is an implementation-independent set of security requirements associated with a "family of [IACS] products". It specifies, for all products belonging in this family, their generic security requirements.

  NB: A Protection Profile is useful for national cybersecurity authorities or vendors to specify general security requirements expected from a family of IACS products, or for requiring a security upgrade of an existing family. It is also useful for providing buyers with broad indications of the cybersecurity constraints and features of a family of products.

- SECURITY PROFILE (SP)
  Product security evaluations cannot rely directly upon generic Protection Profiles. For instance, *Common Criteria* (CC) evaluations require the definition of a product's *Security Target* (ST) derived, for that product, from the generic Protection Profile of its "family".

  A **Security Profile** (SP) is an implementation-dependent set of security requirements (Figure 22) specific to a given, real IACS product / component (named **Target of Evaluation** - ToE - in Common Criteria).

  NB1: A Security Profile in the ICCF is called a *Security Target* (ST) in the ISO 15408 Common Criteria standard or in the French CSPN certification scheme and in the BSI Baseline Security Certification and in the NLNCSA CSPN Equivalent.

  NB2: A Security Profile is the basis of IACS products evaluations.

4.2.6.2.3 Structure

This subsection presents first the concepts that structure the contents of a PP and of an SP. Then it proposes a typical table of contents for PPs and SPs. Section 8.2 supplies an example of a PP.

4.2.6.2.3.1 Conceptual model of a Protection Profile

The following Entity-Relationship (data) model describes the articulation of the concepts structuring a Protection Profile:

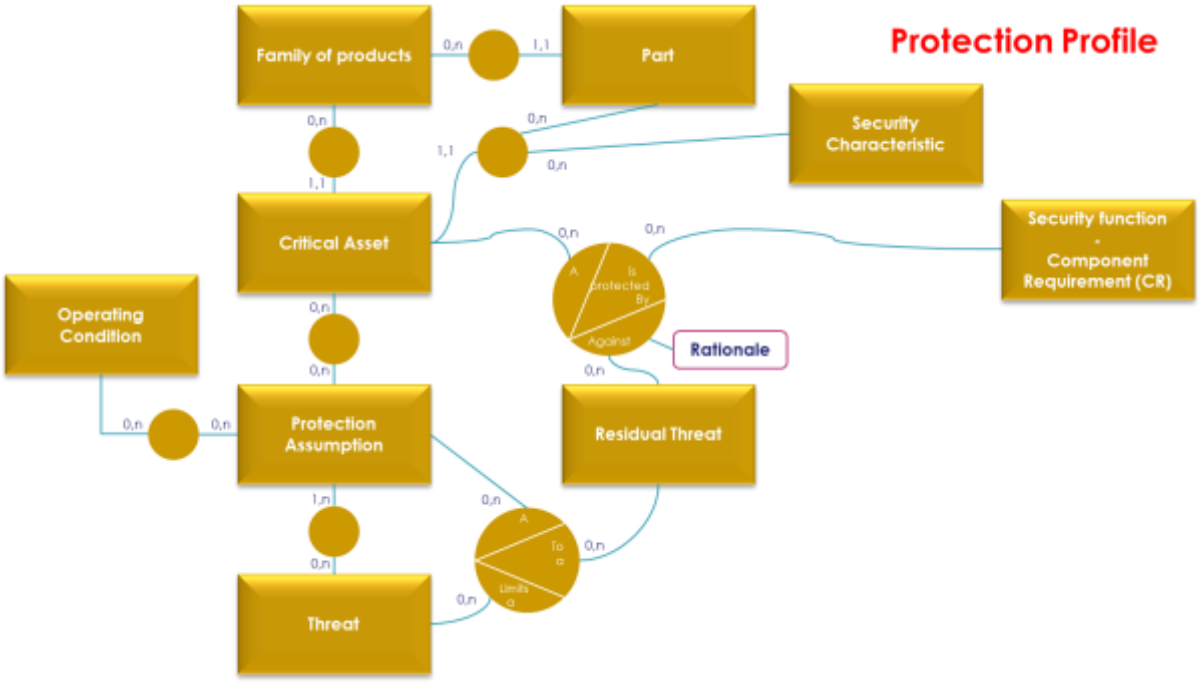

Figure 8 Conceptual model of a Protection Profile

A **Family of Products** can belong in one of the following categories:

- Diode
- Engineering software
- Firewall
- Historian station
- Manufacturing Execution System server
- PLC and RTUs
- SCADA client
- SCADA server
- Switch
- VPN gateway
- WIFI Access Point
- Etc.

NB: http://www.ssi.gouv.fr/entreprise/guide/profils-de-Protection-pour-les-systemes-industriels/ provides a taxonomy of that kind. See also vendors' catalogues, etc.

Comment: The industrial community would benefit from harmonising the taxonomy of IACS families of products.

The family of products is associated with a Protection Profile.

A family of products is made of one or several **Parts**. For instance, a PLC includes a "user program".

Each part may be required to meet one or more **Security Characteristics** such as:

- Availability: Aptitude to ensure a timely and reliable access to and use of control system information and functionality
- Confidentiality: Aptitude to preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity: Aptitude to protect the accuracy and completeness of assets
- Authenticity: Aptitude to assure that an entity is what it claims to be
- Non repudiation: Aptitude to prove the occurrence of a claimed event or action and its originating entities

  Comment: Various definitions of security characteristics coexist today and to prevent any misunderstanding a definition of reference should be included in a Protection Profile or Security Profile. A standard definition should be adopted in the ICCF.

A **Critical Asset** is the conjunction of a Part and a Security characteristic assigned to that part.

NB1: A critical asset is an assertion of the security of a product's part.

NB2: 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 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.

NB1: Operating conditions may refer to the physical layout of buildings (e.g., peripheral security) or of devices (e.g., no USB port on an Engineering Workstation or PLC), or to people working in the environment of the product (e.g., technicians are trustworthy), etc.

NB2: Risk analyses should include the identification of P3R3 measures (section 4.2.2.2) that reduce security risks faced by a critical asset.

NB3: Compensating countermeasures (section 4.2.6.1.4) are part of operating conditions.

The set of protection assumptions associated with a critical asset should leave only **Residual Threats**, in other words the threats that could not be reduced by P3R3 measures formulated in the protection assumptions.

NB: A risk analysis may conclude to the management of only a subset of all residual threats depending on factors such as their likelihood or potential impacts if materialised into incidents, for instance. Unaddressed residual threats constitute accepted known risks.

Given a proper **Rationale**, residual threats on a critical asset require appropriate specific reduction measures, i.e. one or several **Security Functions** to be put in place.

NB: Security Functions correspond to Component Security Requirements (CR). They may be grouped under a more generic security objective (see Figure 27 for details).

4.2.6.2.3.2 Example Protection Profile

The following example provides some illustration of the terms of a protection profile:

Programmable Logic Computer (PLC)

Family of products
Programmable Logic Controller.
This kind of devices allows to monitor and/or to actuate a field instrument, an automation device.
Part
A 'user program' ran by the PLC is a (digital) part of this kind of products.
Critical asset
'The integrity of the user program' is a critical asset of the ToE (combination of the part 'user program' and the security criterion 'integrity').
Threat
User program alteration: The attacker manages to modify, temporarily or permanently, the user program
Operating Conditions (Users)
An administrator is a user of the product who has maximum privileges (modification of the user program, firmware updates, etc.).
Assumption(s)
'The PLC stands in an open area fully accessible to users. Not only administrators have access to PLC's user programs. Administrators are competent and trustworthy. But other users such as hired, external staff are competent but may be untrustworthy'.
Residual Threat(s)
Hired staff may be a threat to the integrity of a PLC.
Security function
Integrity and authenticity of the user program. Only authorized users can modify it. To do so, the product shall at least implement the following CRs:
- CR 1-1 Human user identification and authentication
- CR 1-2 Software process and device identification and authentication
- CR 3-4 Software and information integrity
- CR 4-3 Cryptography

Rationale of the security function
Concept of security objective as in table Figure 26 Threats vs. Security Functions Rationale in annex 8.2.

4.2.6.2.3.3 Generic table of contents of a PP

A Protection Profile's table of contents should include the following sections:

- Description of the family of products;
- Parts;
- Operating conditions;

- Critical assets;
- Threats;
- Protection assumptions;
- Residual threats;
- Security functions requirements;
- Security functions rationale.

4.2.6.2.4 Conceptual model of a Security Profile

The following Entity-Relationship (data) model describes the articulation of the concepts structuring a Security Profile:

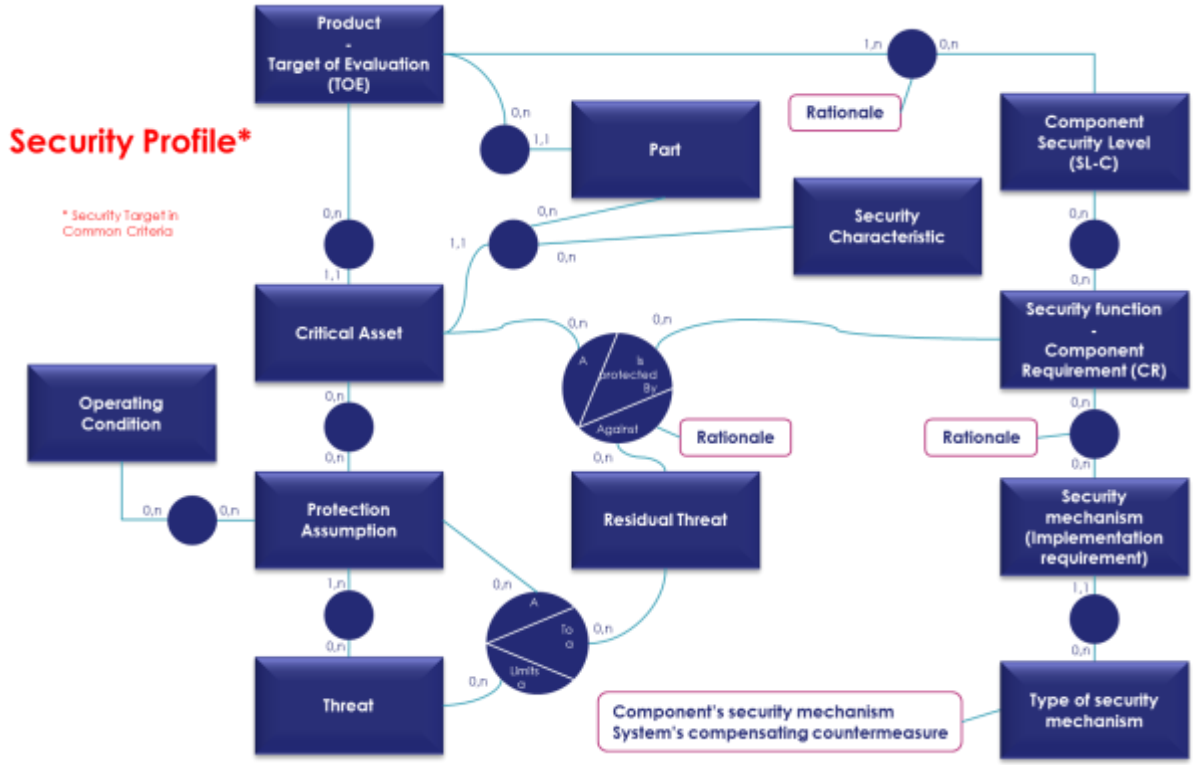

Figure 9 Conceptual model of a Security Profile

This conceptual model is in part similar to a PP's model. Its specific elements are detailed below.

A **Product** is a device or piece of software that belongs in a vendor's range, that has a reference and / or branding name, and the occurrences of which may be assigned a serial number identifying each item of the product built by the vendor.

Examples from the marketplace:

For instance, Siemens' *SICAM RTUs - I/O Modules* brochure of 11/04/2014 (ref: SICRTUs-HBIOMODULE-ENG_V2.06) presents their *SICAM RTU* product range: *SICAM TM*, *SICAM MIC*, *SICAM EMIC*. The *SICAM EMIC* range itself includes the "*TM 1703*" EMIC system.

For instance, also, Honeywell's SO-09-32-ENG leaflet of May 2010 describes the *RC500 Remote Terminal Unit for Oil and Gas Applications* RTU product.

Another example is Computer Process Controls' *MultiFlex Rooftop Unit* for activating and deactivating fans, heat and cool stages, economizers, and other systems or devices.

Products are the **Target of Evaluation** (TOE) in an evaluation process (assessment or certification).

Products are made of different **Parts**.

Example: Siemens' "*TM 1703*" EMIC system is made of a power supply module, a peripheral control module and up to 8 Input/Output modules. The modules are mounted on a TS35 rail (DIN rail).

Given a **Rationale**, the **Security Functions** needed to reduce residual threats are selected according to the **Component's Security Level** (SL-C), itself assigned on the basis of a clearly explicated **Security Level Rationale**. Security functions are implemented through **Security Mechanisms** that, in a Security Profile, are Implementation Requirements that must be met by the vendor, whether he himself decides on which mechanisms to implement or it is the buyer who requires them or else a national security authority.

Example: For instance, a Siemens PLC is required to have communications' integrity and authentication and may implement the S7 protocol. Schneider Electric, for a similar PLC may implement the IPsec protocol. Such choices are based on a **Security Mechanism Rationale**.

The security mechanisms implemented in specific products may alternatively be replaced or complemented by compensating countermeasures implemented in the system the product will be fitted in. A given security mechanism may therefore be of two **Types**: either one embedded in the product itself, or one fitted in the operating environment of the product.

Security functions correspond to Components Security Requirements (see example in annex 8.2.4).

4.2.6.2.5 Generic table of contents of an SP

A Security Profile's table of contents should include the following sections:

- Definitions;
- Description of the product (Target of Evaluation);
- Parts;
- Operating conditions;
- Critical assets;
- Threats;
- Protection assumptions;
- Residual threats;
- Component security level and Security Level Rationale;
- Security functions requirements;
- Security functions rationale;
- Security mechanisms implementation requirements and Security Mechanisms Rationale;
- Evaluations' roles and processes.

4.2.6.2.6 Usage rules and processes

This section provides broad guidelines for managing and using Protection Profiles and Security Profiles. Suggestions for the future made in section 6.1 include some related elements.

4.2.6.2.6.1 General PP and SP management processes

PPs are managed according to the following process:

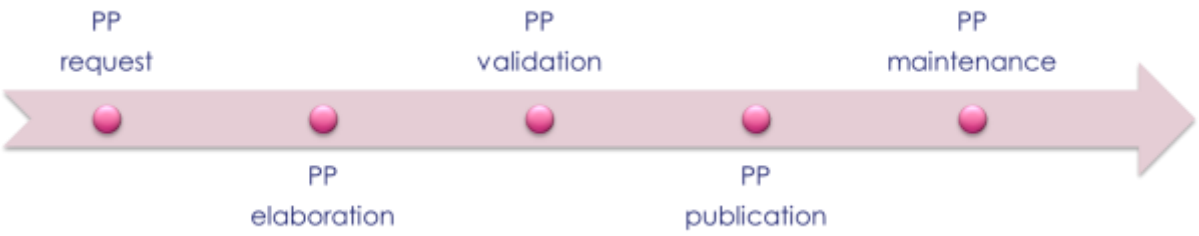

Figure 10 General PP management process

SPs are managed according to the following process (it can be triggered at the SP elaboration step of Figure 11):

Figure 11 General SP management process

4.2.6.2.6.2 Requesting PPs and SPs

When PPs do not yet exist, one of the market's stakeholders may request their elaboration. The leading author invites the appropriate stakeholders to participate in their elaboration and collects their initial views and elements of interest.

When an IACS product needs to be evaluated according to one of the four ICCS, the stakeholder leading the process is responsible for the elaboration of the SP.

4.2.6.2.6.3 Elaborating PPs and SPs

The elaboration of PPs falls under the responsibility mainly of vendors or buyers (user industries), preferably in collaboration with national cybersecurity agencies.

When a product needs to be evaluated, its SP may be elaborated by buyers or vendors, possibly in collaboration with national cybersecurity agencies.

The list of IACS cybersecurity common requirements detailed in section 8.1 may:

- Be incomplete in specific cases as the IEC 62443.4.2 standard may not be exhaustive;
- Be therefore complemented by requirements specific to the product to evaluate.

4.2.6.2.6.4 Validating PPs and SPs

PPs are validated by a certification authority.

SPs must be jointly approved between all parties who took part in their definition.

4.2.6.2.6.5 Using PPs and SPs

PPs are used by vendors in support of their internal product engineering activities, by buyers to select IACS products or to help specifying their requirements for new products.

SPs are used by laboratories to frame evaluation activities required by the chosen ICCS. They are used by certification authorities to verify that ICCS evaluation activities have been conducted in conformance with the contents of the SP.

4.2.6.2.6.6 Publishing PPs and SPs

Unless falling under specific regulations or restrictions, PPs should be made public.

Unless falling under specific regulations or restrictions, SPs should be made public.

4.2.6.2.6.7 Maintaining PPs and SPs

Unless otherwise impossible, PPs should be maintained collectively by the same stakeholders as those who elaborate them.

SPs are updated on request, for instance of vendors when new versions of products involve updates to their cybersecurity specifications or from national cybersecurity agencies.

4.2.6.2.7 References & bridges

Protection Profiles and Security Profiles are not part of the IEC 62443 suite of standards.

The ISO 15408 (Common Criteria) standard and national IACS certification schemes such as the French or German ones define or use similar notions. Refer to these documents for further details.

4.2.6.3 IACS Cybersecurity Certification Process (ICCP)

The IACS Cybersecurity Certification Process (ICCP) pillar provides the processes needed for conducting ICCS and their evaluation activities.

4.2.6.3.1 Introduction

The ICCP organises the conduct of:

- Each ICCS (➔ processes);
- Each evaluation activity (➔ sub-processes).

The following subsections provide guidelines for elaborating and running these processes and sub-processes.

4.2.6.3.2 Concepts and definitions

In this report, the following definitions apply:

- PROCESS

  A process is defined in this report as the sequence of steps required to achieve a given task. Each step has a goal and requires a method that specifies how to reach its goal. A method may require facilitating tools and support guidelines or forms.

4.2.6.3.3 Structure

In this report, processes and sub-processes are articulated as shown in the following diagram:

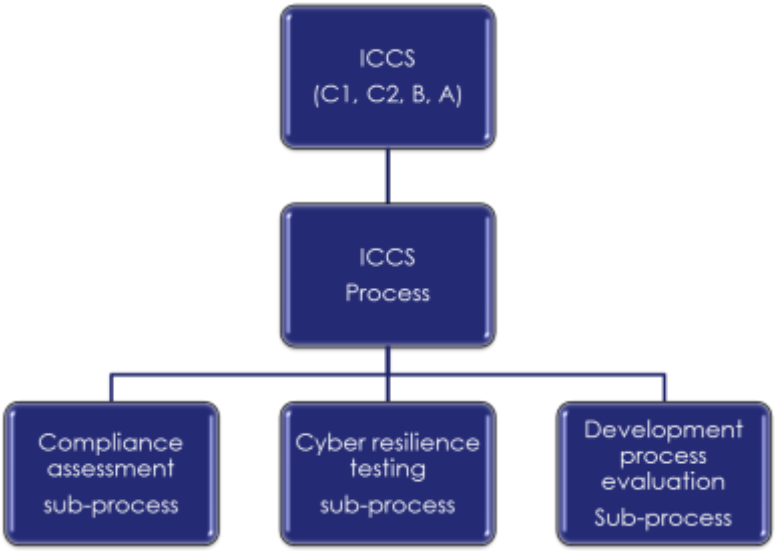

Figure 12 ICCS process hierarchy

All ICCS achieve their goals through a generic process described in section 4.2.6.3.4.

Evaluation activities run in ICCS schemes (Figure 5) require sub-processes described in section 4.2.6.3.6.

4.2.6.3.4 ICCS generic process and rules

The following diagram depicts the general process for the conduct and delivery of ICC Schemes:

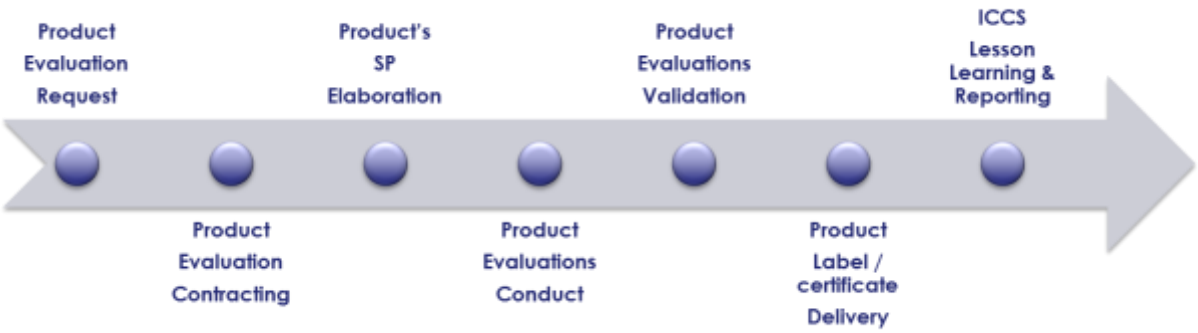

Figure 13 ICCS Generic Process

In this initial report of the ICCF guidelines, the steps of this ICCS Generic Process are not detailed and are therefore left to an agreement between the parties involved in the performance of an ICCS.

> Comment: In the context of given Evaluation Requests, each step may involve differently the roles mentioned in section 4.1; or difficulties may appear; or contractual clauses may be elaborated to regulate the process; or else specific products may involve variations in the ICCS evaluation activities; etc.

Lesson learning is therefore a crucial step of the process and its feedback should be provided to the ICCF Governance Board. It will serve as an input to the elaboration of future versions or releases of the ICCF.

4.2.6.3.5 A consolidated view of PP, SP and ICCS generic processes

The following diagram show how the PP management process (Figure 10), the SP management process (Figure 11) and ICCS generic process (Figure 13) combine together:

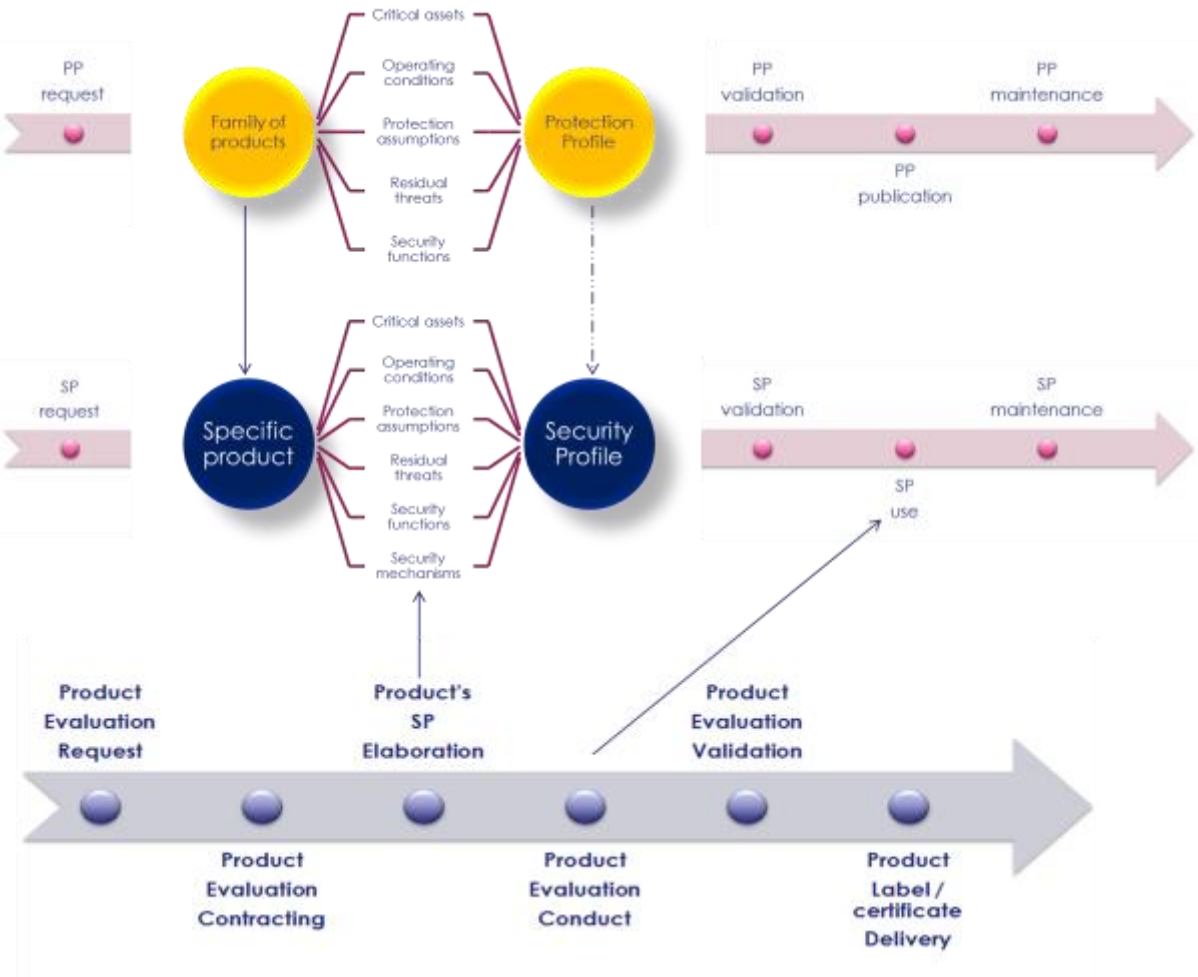

Figure 14 Combination of PP, SP and ICCS processes

4.2.6.3.5.1 Product Evaluation Request

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.5.2 Product Evaluation Contracting

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.5.3 Product's Security Profile Elaboration

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.5.4 Product Evaluation Conduct

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.5.5 Product Evaluation Validation

With ICCS-C1, the vendor who performs a self-assessment of compliance does not communicate its report to a certifier but should publish it (Security Profile + Compliance Matrix) on the IACS Cybersecurity Certification EU Register.

4.2.6.3.5.6 Product Label / Certificate Delivery

Only a certification authority delivers labels and certificates. Once delivered, a label or certificate is recorded in the IACS Cybersecurity Certification EU Register (section 4.2.6.4).

4.2.6.3.5.7 ICCS Lesson Learning & Reporting

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.6 Evaluation activities and their sub-processes

Evaluation activities are run at the "Product Evaluation Conduct" step of the ICCS Generic Process:

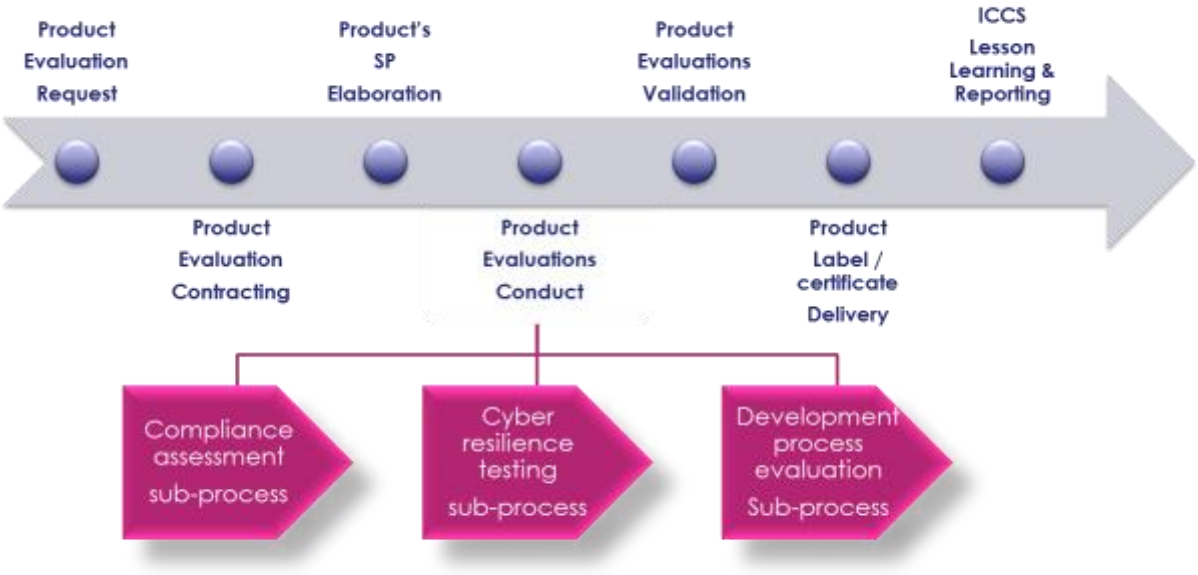

Figure 15 ICCS sub-processes

Each sub-process follows the Generic Evaluation Activity Sub-Process shown on the next diagram:

Figure 16 Generic Evaluation Activity Sub-Process

Specific adaptations and refinements of the Generic Evaluation Activity Sub-Process may be made in the future either at the request of the ICCF Governance Board or in the context of specific Evaluation Requests (meaning for evaluating specific IACS products).

> Example: For instance, specific toolsets may be used to perform specific evaluations and they may be chosen because of their specific advantages or features (rationale of choice).

In this latter case, these adaptations or refinements and their rationale must be documented at the Lesson Learning & Reporting step. This feedback should be provided to the ICCF Governance Board. It will serve as an input to the elaboration of future versions or releases of the ICCF.

4.2.6.3.6.1 Product Evaluation Results Reporting step: generic guidelines

As a general rule, the results of evaluations should consist of:

- The product's reference;
- The ICCS (A, B, C2, C1);
- The product's Security Profile;
- The evaluation results:
  - For a compliance assessment: a compliance matrix;
  - For tests: a test report;
  - For a development process assessment: a development process assessment report.

4.2.6.3.6.2 Compliance assessment sub-process

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.6.3 Cyber resilience testing sub-process

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.6.4 Development process evaluation sub-process

This item will be detailed in the next phase of the feasibility study of the ICCF.

4.2.6.3.7 Management and maintenance of the ICCP

With the experience gained from the practice of ICCSs and of evaluation activities, the specification of processes and sub-processes will improve.

Lesson learning is therefore a crucial and ICCF practitioners must comply with the request to perform Lesson Learning & Reporting steps mentioned in earlier subsections. Lesson learning reports must include the details of the practices effectively adopted as well as changes, adaptations, refinements and innovations made to the definitions and pillars previously described.

The ICCF Governance Board will review lesson learning reports and will select the elements that are good candidates for future versions or releases of the ICCF.

4.2.6.3.8 References & bridges

For the short-term, the processes prescribed in the standards taken as a reference in the ICCF or freely agreed between parties at the contracting step of an Evaluation (ICCS' Product Evaluation Contracting step: see subsection 4.2.6.3.4).

4.2.6.4 IACS Cybersecurity Certification EU Register (ICCEUR)

The aim of the IACS Cybersecurity Certification EU Register (ICCEUR) is to provide end users with a portal to get information about the ICCF, its guidelines and a list of ICCF-evaluated IACS products.

In particular, the portal should:

- Provide a database of ICCF- evaluated IACS products;
- Provide ICCF guidelines;
- During the feasibility study, be hosted by the ERNCIP platform website;
- Be available free of charge to all interested parties.

The JRC, in its role of facilitator of this feasibility study, has been actively following the evolution of the TG's internal discussion and orientations toward the potential establishment of the ICCF.

Up to now, the ERNCIP project has already published on its platform (https://erncip-project.jrc.ec.europa.eu) the information regarding the TG's activities, findings and reports. The intention for the future is to enhance web-based ICCF support by developing further information tools/database that can be seen as a complement of the ICCF design and potential model.

The initial high-level functionalities of this web-based platform are presented below and will be implemented in accordance with the upcoming activities carried out by the TG and as soon as the need of their practical implementation will emerge.

4.2.6.4.1 High level functionalities

At the time this report has been drafted, these seem to be the main sections of a dedicated ICCF portal:

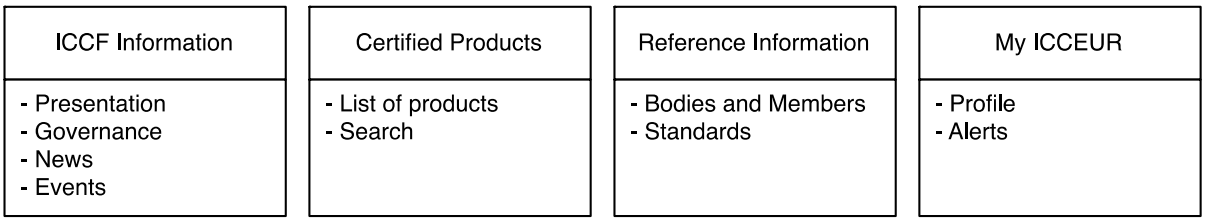

Figure 17 ICCEUR portal's main functions

The portal will incorporate a database of IACS products compliant with or having been certified or labelled according to the ICCF's requirements.

The database will be characterised by a set of functions that will allow users and administrators, according to their privileges, in order to:

- Add new IACS Product;
- Update IACS Product;
- Remove IACS Product;
- Search for Products;
- List IACS Products;

- View Product profile details and their C&C information;
- Request Access Form.

As for the fields associated to an IACS Product, they shall include:

- Product Name;
- Product Version;
- Vendor/Supplier Name;
- Link of Vendor Product Page for additional details;
- Picture;
- Type/Category of the Product;
- ICCF compliance information;
- ICCF certification information.

4.2.6.4.2 Initial ICCEUR mock-ups

The following initial mock-ups suggest how the IACS products database interface might look:

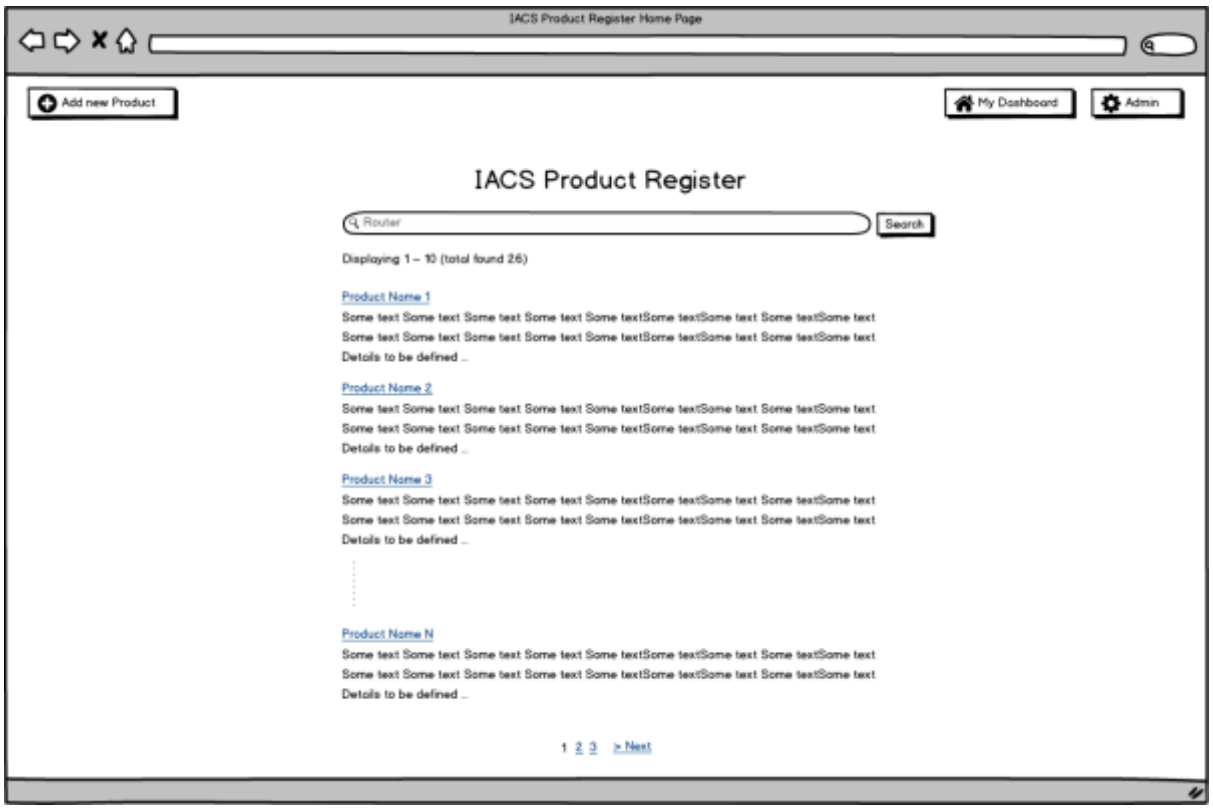

Figure 18 Suggested ICCEUR's products database interface (global)

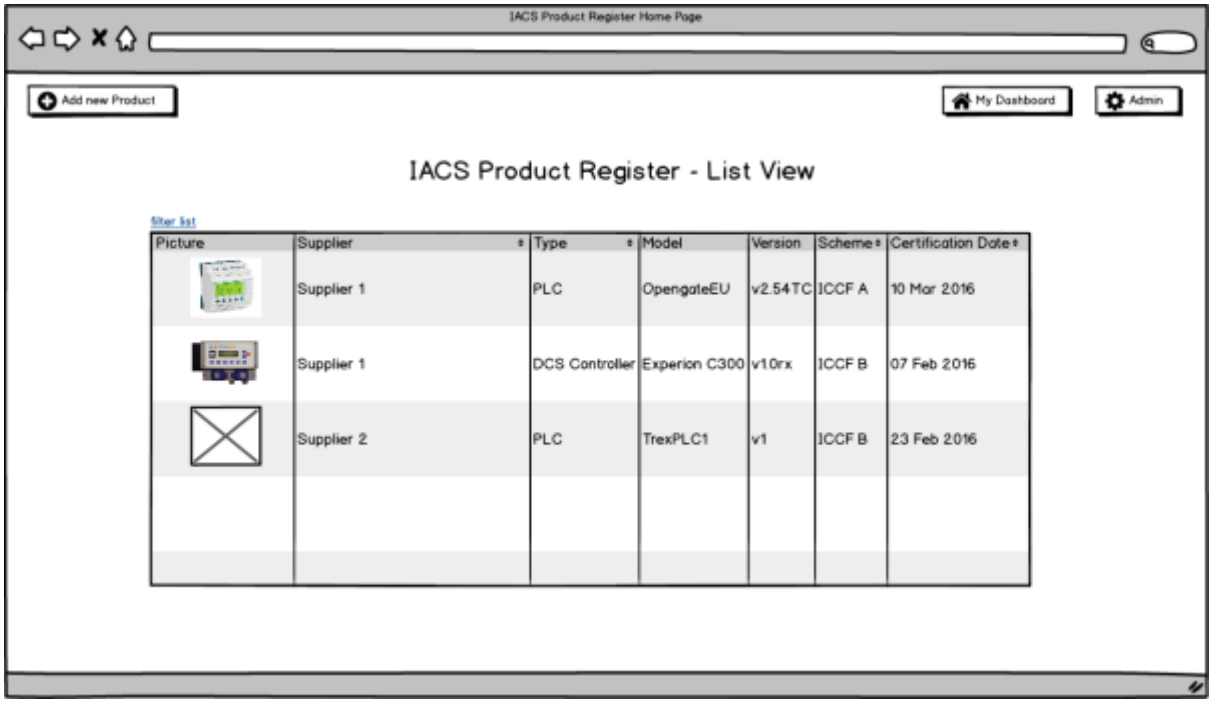

Figure 19 Suggested IACS products database interface (list)

5 The ICCF Multilevel Governance Structure

The activities and schemes described in this report should be supported, managed, promoted and overseen by a global governance structure involving:

- The European Commission and International Standardisation Bodies;
- The JRC's Thematic Group;
- National Cybersecurity Agencies;
- Corporate stakeholders (vendors, buyers, certifiers, laboratories).

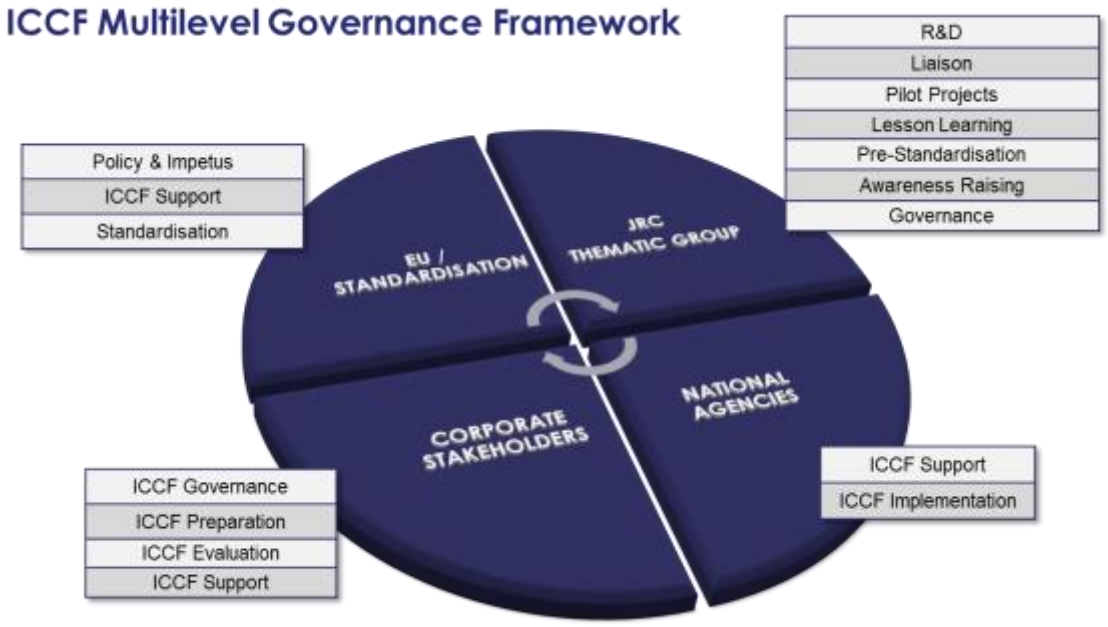

Figure 20 The ICCF Multilevel Governance Structure framework

The European Commission and International Standardisation Bodies (figure above) should play the following roles:

- Setting-up IACS component Cybersecurity Certification policies: this is done under the drive of the EC's Directorate Generals such as the Joint Research Centre (DG JRC), DG CNECT, with the support of their Units and Agencies;
- Supporting the ICCF: this is done under the drive of the JRC and other EC DGs. Support consists in resourcing or financing the ERNCIP IACS Cybersecurity Certification Thematic Group, finding new supporters of the TG's project, publishing and disseminating the TG's results;
- Elaborating and publishing standards in relation to IACS cybersecurity & certification, and liaising with the ICCF governance board.

The JRC and the IACS cybersecurity certification Thematic Group should play the following roles:

- Researching, developing and maintaining the ICCF with the collaboration of stakeholders;

- Liaising with stakeholders, including the EC, standardisation bodies, national cybersecurity authorities, vendors, buyers, laboratories, certifiers, etc.;
- Running pilot projects that help to test and fine tune the ICCF;
- Drawing the lessons from pilot projects to improve the ICCF;
- Promoting a pre-standardisation activity in liaison with standardisation bodies, European and national cybersecurity authorities;
- Raising stakeholders' awareness through training sessions, conferences, publications.

National Cybersecurity Agencies should play the following roles:

- Supporting the ICCF either by taking part in the TG's activities or by fostering their outcomes;
- Implementing the ICCF or fostering its implementation nationally, for instance by contributing to the elaboration of Protection Profiles.

Corporate stakeholders should play the following roles:

- Putting in place an internal ICCF governance process giving directions for its implementation;
- Preparing for the ICCF: this may mean that vendors assess and engineer their IACS products from the point of view of cybersecurity; it may mean for buyers to evaluate their needs and to prepare for requesting certified IACS products; it means for certification authorities to prepare to deliver certificates according to ICCF processes and for laboratories to prepare for getting accredited and to perform evaluations according to ICCF prescribed processes and guidelines; for accreditation bodies, it means preparing to assess laboratories and to deliver them accreditation;
- Evaluating IACS products: this means that laboratories, under the control of a certification authority and in collaboration with vendors and buyers, should proceed to running ICCF Schemes and delivering labels and certificates according to prescribed processes;
- Supporting the ICCF: this may mean taking part in the TG's activities, publicising the ICCF, training stakeholders, etc.

How this structure will live will be documented in a later report once discussions with stakeholders, pilot projects and further work will have been carried out.

6 Implementing the ICCF: Initial guidelines

This section tells future ICCF users where and how to start using the ICCF.

6.1 How the ICCF could work: an initial proposition

The first aspect of the implementation of the ICCF is the way it could possibly work.

The following diagram intends to elaborate on the different roles described in section 4.1 and on how they should collaborate in the future:

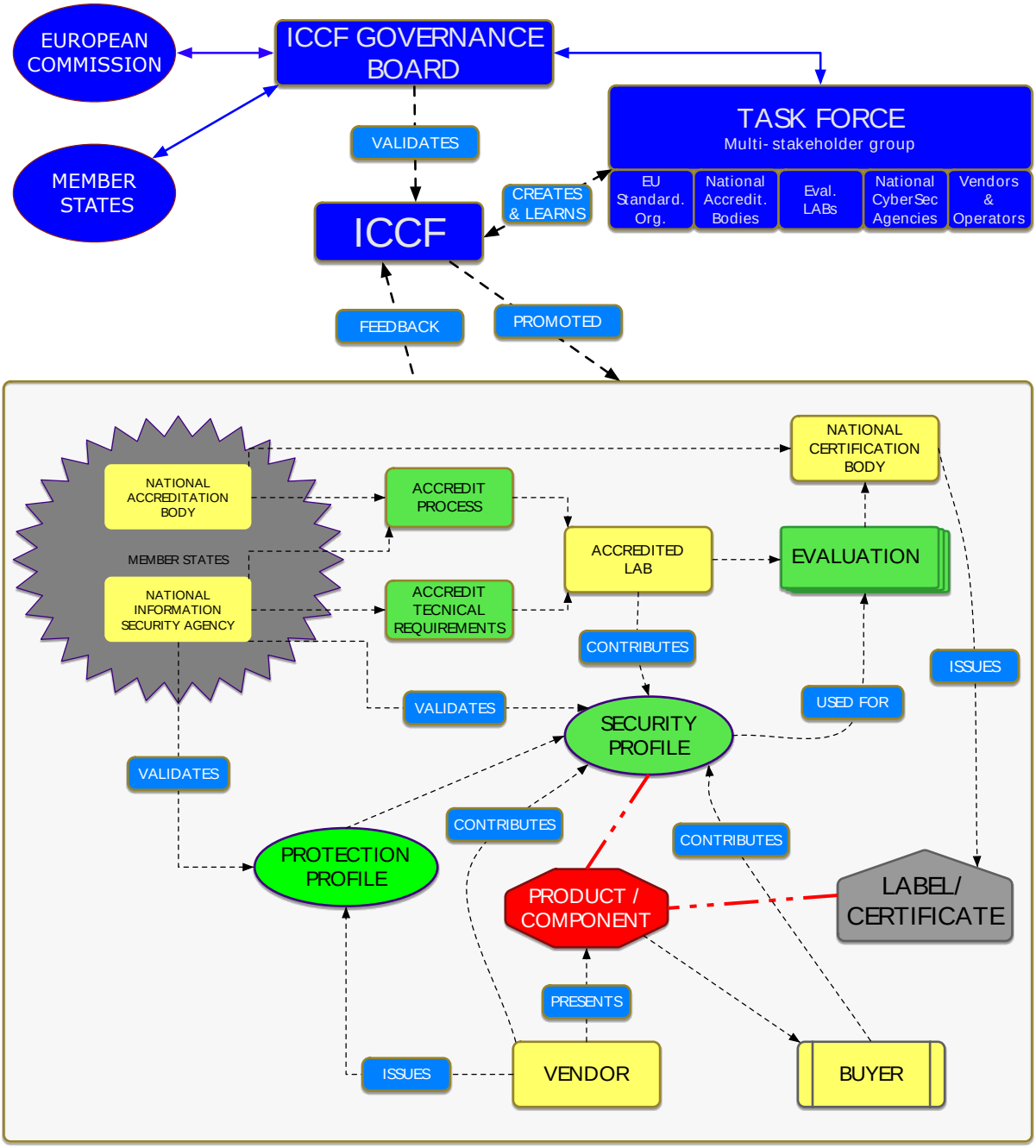

Figure 21 How the ICCF could work

The task force mentioned in the diagram could be either the TG as it is today or a specific body, creating work groups for specific purposes and in which ad hoc experts would be invited.

This global process needs to be evaluated in the context of the upcoming pilot projects and discussions with stakeholders.

6.2 Recommendations for vendors

Vendors should, at their own pace or in function of market demands:

1. Assess their needs for IACS products certification: this can be done based on market analyses as well as security analyses, in conjunction with National Cybersecurity Agencies where required;
2. Select the ICCS best suited to each family of products or possibly to each product within that scope;
3. Review the associated necessities and ways (such as creating PPs and SPs, working with specific standards, laboratories, certifiers, preparing for the processes to be undertaken and the time schedule, communication of certificates or labels to clients, etc.);
4. Budget and schedule their engagement into IACS certification;
5. Launch easy-to-run pilot projects and draw organizational lessons from them.

6.3 Recommendations for buyers

Buyers should, at their own pace or in function of security or procurement requirements:

1. Assess their needs, priorities and constraints (security, budget, systems, premises, project management, technology, etc.) in terms of procurement and use of cybersecurity certified IACS components;
2. Determine the processes and partners (certifiers, laboratories, national cybersecurity authorities…) they need or want to work with;
3. Define and enforce an ad hoc procurement process;
4. Work with their partners to make things happen;
5. Budget and schedule their engagement into the procurement of certified IACS components;
6. Launch easy-to-run pilot projects and draw organizational lessons from them.

6.4 Recommendations for the European Commission

EC should, at its own pace or in function of security policy, strategies and priorities:

1. Evaluate the ICCF against current European needs both in terms of 2017 planned consultation and impact assessment[6];
2. Disseminate the ICCF vision in all 28 Member States;
3. Promote full ICCF certification pilot from the beginning of 2018 and bridge it with the wider ICT certification initiative of DG CNECT;

[6] COM(2016) 410 final from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of Regions "on strengthening Europe's Cyber Resilience system and Fostering a competitive and innovative cyber security Industry".

4. Validate the ICCF in the light of the experiments carried out in 2017/2018;
5. Evaluate whether this effort should be enforced through dedicated legislation or fostered through voluntary adoption;
6. Liaise with international stakeholders in order to facilitate mutual recognition of certificates and labels across the world, based on the successful outcome of the previous 5 recommendations.

7 Conclusions

7.1 The ICCF as a contribution to DG CNECT's strategy

This report entails an "introduction to the ICCF" the aspects, pillars and governance model of which may be used in support of DG CNECT's "*Roadmap toward a European ICT security certification framework for product and services*". As the Roadmap will be defined in the upcoming months, through the formulation of a Proposal[7], this activity, carried on by the JRC, together with the stakeholders operating in the European domain of IACS, can explore in advance constraints, limits, success factors and enablers that can influence the implementation of a European certification framework in the next future.

The ERNCIP Thematic group, by taking into consideration the recommendations formulated above and the need to deepen further the feasibility study of the ICCF, proposes to keep working on this item in 2017. The main goal for 2017 is to "challenge" the current stage of development of the ICCF with the work streams described below and also to organise exercises that will simulate "the behaviouristic and governance model" of the Framework, in cooperation with national stakeholders operating in "National Exercise Groups" (ERNICP IACS NEGs).

The conclusion of the following activities will contribute to further enhance the ICCF's feasibility study as potential "*sectorial response*" to the "*Roadmap toward a European ICT security certification framework for product and services*".

7.2 Proposed plan of action for the ERNCIP IACS TG in 2017

The proposed 2017 plan of action may include:

1. Focused pilot-projects ("National Exercise Groups") in relation to:
   - The usability of the component requirements (product assessment criteria);
   - The assessment & test of protection & security profiles elaboration and usability;
   - The simulation or test of ICCF processes;
2. A feedback study for the improvement of the ICCF based on the results of the aforementioned pilots;
3. A study of the development process assessment aspect that answers the following questions: which requirements? Which reference process model? Which process to do the assessment? How to include this into Security Profiles?
4. A study of the ICCF governance structure;
5. A final report including the outcome of 2017's projects in a fine-tuned version of the ICCF and a potential work programme for 2018.

The Work programme describing the activities to be carried on by the ERNCIP TG in 2017 could be made of the following 7 streams:

[7] See DG CNECT's Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry".

1. Global project management and stakeholder engagement (leading to creating the required "National Exercise Groups" and establishing the exercises' plan and protocol);
2. Stakeholders recruitment and liaison (including national cybersecurity agencies, vendors, user industries, certifiers, accreditation body and labs);
3. A one day of ICCF training (perhaps during the 2017 kick off meeting) for recruited pilot-participants, to introduce everyone to the ICCF mind-set, concepts, upcoming challenges and vocabulary, as well as to the protocol of the "National Exercises" (pilot projects);
4. Focused pilot projects (exercises run by "National Exercise Groups") performed by relevant stakeholders to test the components of the ICCF;
5. ICCS-A development process assessment (this could be also a "National Exercise");
6. ICCF governance body and processes (this could be also a "National Exercise");
7. Feedback and improvement of the ICCF (2017 report writing and validation).

As for the "National Exercises" (i.e. the tests of ICCF elements), four types of exercises can be identified - at the time this report is published - along with two execution options:

4 types of exercises (E1 to E4)

E1 - Elaborate a protection profile and a security profile and report on the easiness/difficulty of this activity.

- Standardize the contents and define the elaboration process of (protection) security profiles.

E2 - Simulate a product compliance assessment, document and report on easiness and difficulty.

- Review product requirements of IEC 62443-4-2 (Industrial communication networks – Technical security requirements for IACS components) against ISO/IEC 15408 and NIST SP800-82 (Guide to Industrial Control Systems Security);
- Validate the data model of requirements and justify its constituents.

E3 - Simulate a product cyber resilience test, document and report on easiness and difficulty.

- Review product cyber resilience testing methods, techniques, processes, outcomes, actors.

E4 - Simulate a product development process evaluation, document and report on easiness and difficulty.

- Review product development process assessment processes and schemes and precise contexts/limits.

2 options to perform the exercises

O1 - Unique shared exercise

- All teams work on only one exercise (then E1 might be the priority);
- Advantage: comparison of results would yield sound improvements;
- Disadvantage: only one test in 2017 means limited improvement of the ICCF;
- Implications for protocol: focus on benchmarking results.

O2 - Paralleled four exercises

- Each team performs a different test (each national teams runs one of the 4 exercises)
- Advantage: all types of tests are performed, ICCF improvement may be equal on all aspects
- Disadvantage: each test being performed once only, results may be insufficient.
- Implications for protocol: focus on quality standards to guarantee usable results.

When launching the IACS TG work plan, the TG will have to decide, in conjunction with the European Commission, the most appropriate exercise scheme.

8 Annexes

8.1 Annex 1: The ICCAR pillar's requirements

The following table lists the component security requirements (CR) supplied by (IEC 62443-4-2, Draft 2, Edit 4, July 2, 2015). It shows also the association between CRs and security levels (shaded boxes) and the requirements associated with specific types of components (TCE):

- ACR: Application Component Requirement;
- ECR: Embedded device Component Requirement;
- HCR: Host device Component Requirement;
- NCR: Network device Component Requirement.

FR, CRs and REs				
FR 1 – Identification and authentication control (IAC)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 1.1 – Human user identification and authentication				
CR 1.1 RE 1 – Unique identification and authentication				
CR 1.1 RE 2 – Multifactor authentication for untrusted interface				
CR 1.1 RE 3 – Multifactor authentication for all interfaces				
CR 1.2 – Software process and device identification and authentication				
CR 1.2 RE 1 – Unique identification and authentication				
CR 1.3 – Account management				
CR 1.4 – Identifier management				
CR 1.5 – Authenticator management				
CR 1.5 RE 1 – Hardware security for authenticators				
NCR 1.6 – Wireless access management				
NCR 1.6 RE 1 – Unique identification and authentication				
CR 1.7 – Strength of password-based authentication				
CR 1.7 RE 1 – Password generation and lifetime restrictions for human users				
CR 1.7 RE 2 – Password lifetime restrictions for all users				
CR 1.8 – Public key infrastructure certificates				
CR 1.9 – Strength of public key authentication				
CR 1.9 RE 1 – ISO/IEC 19790 Level 3 security for public key authentication				
CR 1.9 RE 2 – ISO/IEC 19790 Level 4 security for public key authentication				
CR 1.10 – Authenticator feedback				
CR 1.11 – Unsuccessful login attempts				
CR 1.12 – System use notification				
NCR 1.13 – Access via untrusted networks				
NCR 1.13 RE 1 – Explicit access request approval				
CR 1.14 – Strength of symmetric key authentication				
CR 1.14 RE 1 – ISO/IEC 19790 Level 3 security for symmetric keys				
CR 1.14 RE 2 – ISO/IEC 19790 Level 4 security for symmetric keys				
FR 2 – Use control (UC)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 2.1 – Authorization enforcement				
CR 2.1 RE 1 – Authorization enforcement for all users				
CR 2.1 RE 2 – Permission mapping to roles				
CR 2.1 RE 3 – Supervisor override				
CR 2.1 RE 4 – Dual approval				
CR 2.2 – Wireless use control				
CR 2.3 – Use control for portable and mobile devices				
ACR / ECR / HCR / NCR 2.4 – Mobile code				
ACR / ECR / HCR 2.4 RE 1 – Mobile code integrity check				
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 2.9 RE 1 – Warn when audit record storage capacity threshold reached				
CR 2.10 – Response to audit processing failures				

CR 2.11 – Timestamps				
CR 2.11 RE 1 – ~~[Internal]~~ time synchronization				
CR 2.11 RE 2 – Protection of time source integrity				
CR 2.12 – Non-repudiation				
CR 2.12 RE 1 – Non-repudiation for all users				
FR 3 – System integrity (SI)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 3.1 – Communication integrity				
CR 3.1 RE 1 – Cryptographic integrity protection				
ACR / ECR / HCR / NCR 3.2 – Malicious code protection				
HCR 3.2 RE 1 – Report version of code protection		HCR	HCR	HCR
CR 3.3 – Security functionality verification				
CR 3.3 RE 1 – Automated mechanisms for security functionality verification				
CR 3.3 RE 2 – Security functionality verification during normal operation				
CR 3.4 – Software and information integrity				
CR 3.4 RE 1 – Automated notification of integrity violations				
CR 3.5 – Input validation				
CR 3.6 – Deterministic output				
CR 3.7 – Error handling				
CR 3.8 – Session integrity				
CR 3.8 RE 1 – Invalidation of session IDs after session termination				
CR 3.8 RE 2 – Unique session ID generation				
CR 3.8 RE 3 – Randomness of session IDs				
CR 3.9 – Protection of audit information				
CR 3.9 RE 1 – Audit records on write-once media				
ECR / HCR / NCR 3.10 – Originality	H/NCR	H/NCR	H/E/NCR	H/E/NCR
HCR / NCR 3.10 RE 1 – Unalterable proof of originality		H/NCR	H/NCR	H/NCR
FR 4 – Data confidentiality (DC)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 4.1 – Information confidentiality				
CR 4.2 – Information persistence				
CR 4.2 RE 1 – Purging of shared memory resources				
CR 4.3 – Use of cryptography				
FR 5 – Restricted data flow (RDF)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 5.1 – Network segmentation				
NCR 5.2 – Zone boundary protection				
NCR 5.2 RE 1 – Deny all, permit by exception				
NCR 5.2 RE 2 – Island mode				
NCR 5.2 RE 3 – Fail close				
NCR 5.3 – General purpose person-to-person communication restrictions				
CR 5.4 – Application partitioning				
FR 6 – Timely response to events (TRE)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 6.1 – Audit log accessibility				
CR 6.1 RE 1 – Programmatic access to audit logs				
CR 6.2 – Continuous monitoring				
FR 7 – Resource availability (RA)	**SL-C 1**	**SL-C 2**	**SL-C 3**	**SL-C 4**
CR 7.1 – Denial of service protection				
CR 7.1 RE 1 – Manage communication load from application or device				
CR 7.2 – Resource management				
CR 7.3 – Control system backup				
CR 7.3 RE 1 – Backup verification				
CR 7.3 RE 2 – Backup automation				
CR 7.4 – Control system recovery and reconstitution				
CR 7.5 – Emergency power				
CR 7.6 – Network and security configuration settings				
CR 7.6 RE 1 – Machine-readable reporting of current security settings				
CR 7.7 – Least functionality				
CR 7.8 – Control system component inventory				
Reliance on compensating countermeasures: see IEC 62443-3-2				

Figure 22 List of components security requirements

8.2 Annex 2: The ICPRO pillar; example of the French CSPN scheme

This section provides an illustration of ICCF's concepts of Protection Profile and Security Profile.

8.2.1 Example of a Security rationale

8.2.1.1 Critical assets versus threats

Threats **Critical assets**	Firmware alteration	Authentication violation	Credential theft
Integrity of configuration			
Integrity of user authentication mechanism		x	
Confidentiality of user secrets			x

8.2.1.2 Threats versus security functions

Security functions Threats	Secure connection with the authentication server	Firmware signature	Secure storage of secrets
Firmware alteration		x	
Authentication violation	x		
Credential theft			x

8.2.2 Usage rules

8.2.2.1 Protection Profile and Security Profile (Security Target)

In the French CSPN (Certification de Sécurité de Premier Niveau) certification scheme, a Protection Profile sets minimum security requirements for a family of products. It gives the list of security functions that must be implemented in the products belonging to that family.

The Protection Profile serves as a template to write a Security Target for a given product of that family. The Security Target can extend the security functions of the Protection Profile it is based on.

From a purchaser's perspective, a Protection Profile serves as a comparison tool: if certified against the same PP, different products can be better compared.

A **Security Target** is an instantiation of a Protection Profile.

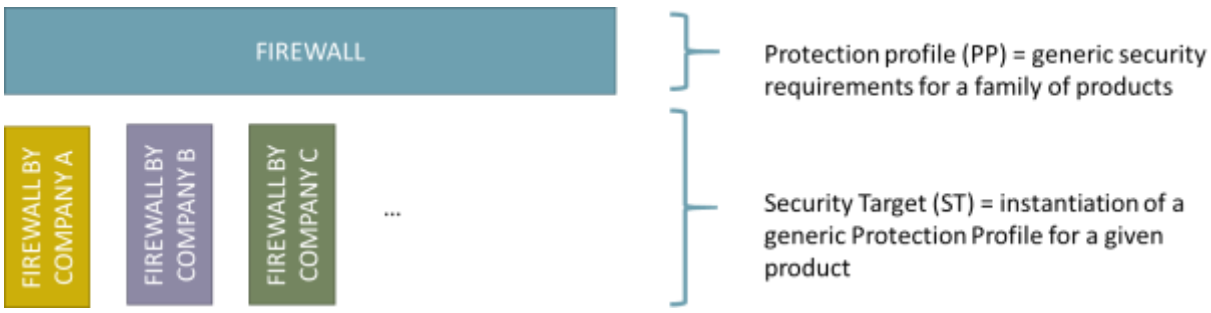

Figure 23 Security profiles may be derived from protection profiles

8.2.2.2 Usage rules for evaluation

When a vendor wants its product to be evaluated against a certain Protection Profile, it must explicit the instantiation of the security functions implemented in the product to be evaluated. The instantiation is described in a document called Security Target, that is to say that the Security Target addresses each security requirements of the Protection Profile by specifying which mechanisms are implemented in the vendor's product. For instance, a security objective such as authentication may be implemented with a password-based mechanism, or a certificate. The Security Target specifies how the security functions contained in the Protection Profile are instantiated in the vendor's product. The Security Target is technology-dependent.

The Protection Profile does not specify the test methodology to be applied by laboratories.

8.2.2.3 Usage rules for updating

Protection Profiles may need to be updated in case of major evolution in assumptions or threats.

8.2.3 Example of contents of a Protection Profile for a PLC

This example is provided as an illustration of the concept of Protection Profile and may be subject to caution or questions. It is based on ANSSI's Protection Profile of an industrial programmable logic controller, as of July 13th 2015.

8.2.3.1 Preface

In the whole document, the acronym FoP (Family of Products) designates the type of components that may be evaluated.

8.2.3.2 Description of the Family of Products

8.2.3.2.1 General description

A programmable logic controller (PLC) is a device designed for controlling and commanding an industrial automation device in a continuous way, without human intervention. A PLC processes input data received from sensors and sends output commands to actuators.

In addition to standard references, there are two types of PLCs:

- redundant PLCs, used for higher availability of ICS;
- safety PLCs, used for ensuring safety of people and assets.

The PLC must be able to run in a hostile environment. In particular, it must run despite humidity, dust or unusual temperatures for IT systems.

8.2.3.2.2 Parts

A PLC typically includes the following parts:

- User program execution: The FoP runs a user program. This program processes the inputs and updates the outputs.
- Input/output management: The FoP is able to read local or remote inputs and to write local or remote outputs. These I/O can be digital or analog. These I/O allows the FoP controlling and commanding the industrial process.
- Communication with the supervision: The FoP can communicate with the SCADA for receiving commands and transmitting process data.

- Administration functions: The FoP includes administration functions in order to configure, or program the other functionalities of the FoP. 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 FoP (Family of Products) supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events.
- Remote logging: The FoP supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

8.2.3.3 Operating conditions

8.2.3.3.1 Product usage

A PLC can be used in diverse architectures but a general framework can be characterized. The PLC is connected to inputs and outputs and to its local HMI through the same communication interface on the field network. Exchanges with the supervision (HMI, SCADA) are performed through a dedicated interface on the supervision network.

The PLC is managed with an engineering workstation. Firmware updates and user programs can, in general, be loaded on the PLC through the network, thanks to a serial bus or a removable device (SD memory cards, USB keys for instance).

Setting-up a dedicated network is recommended for network maintenance. 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.

This basic architecture is depicted on the following diagram:

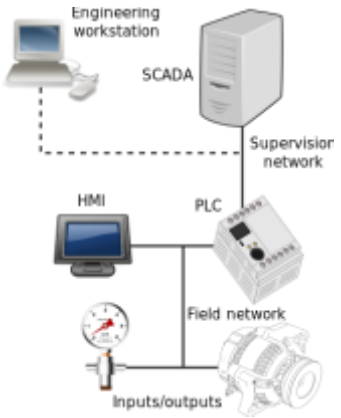

Figure 24 Typical network architecture for a PLC (Open ClipArt, Creative Commons)

8.2.3.3.2 Users

The users that may interact with the FoP (Family of Products) are the following:

- Operator: This user can access the FoP data with read-only privileges.
- Technician: This user has the same privileges as the previous one and he can also modify some variables in the FoP.

- Automation Engineer/administrator: This user has maximal privileges. He can, in particular modify the user program and update the firmware of the FoP. In some cases, this type of user is called “developer”.

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.

8.2.3.4 Assumptions

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

- Logs checking: We assume that administrators check regularly the local and remote logs produced by the FoP.
- Administrators: FoP administrators are competent, trained and trustworthy.
- Premises: The FoP is not necessarily in secured premises and the attacker can have access to all physical interfaces of the FoP. Similarly, the attacker can plug a trapped device (for instance, a USB drive or a SD card) on any physical port of the FoP. Conversely, the attacker cannot disassemble the FoP or perform physical attacks on it. Since similar products in a FoP may be purchased freely, the attacker may purchase one in order to search for vulnerabilities.
- Unevaluated services disabled by default: Services of the FoP which are not covered by the security target are disabled in the default configuration (also named factory default configuration).
- Security documentation: The FoP 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.

8.2.3.5 Critical assets

8.2.3.5.1 Critical assets of the environment

The critical assets of the environment are the following:

- Availability and integrity of control-command of the industrial process: The FoP controls and commands an industrial process by reading inputs and sending commands to actuators.
- Integrity and authenticity of data exchanges between the FoP and the supervision
- Integrity, confidentiality and authenticity of engineering workstation flows
- Integrity and authenticity of data exchanges between the FoP and another PLC: For the communication between the FoP and another PLC, the use of dedicated I/O should be preferred. In the case where these exchanges should transit on a mutualized infrastructure, they must be protected in integrity and authenticity.

8.2.3.5.2 FoP’s critical assets

The critical assets of the FoP are the following:

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

- Integrity, confidentiality[8] and authenticity of the user program: The FoP runs a program written and loaded by the users. Its integrity, confidentiality[9] and authenticity must be protected.
- Confidentiality and integrity of the configuration: The configuration of the FoP must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the FoP by other means than the FoP activity.
- Integrity and authenticity of the execution mode: The integrity and authenticity of the execution mode of the FoP must be protected.
- Integrity and authenticity of the user authentication mechanism: This mechanism can be based on a local database or on a remote authentication server. In both cases, the FoP must ensure the integrity and authenticity of the mechanism[10].
- Integrity and confidentiality of user secrets: The user secrets can be passwords, certificates…They can be stored in the FoP or stored in a remote authentication server. In all cases, the FoP must ensure the integrity and confidentiality of these credentials.
- Integrity of access control policy: The policy can be stored locally or remotely on a authentication server. In both cases, the FoP must ensure the integrity of the access control policy.
- Availability of local logging: Once configured, the local logging must remain operational.
- Availability of remote logging: The FoP is capable of remote logging. Once configured, the logging must remain operational.
- Integrity of local logs: The integrity of the local logs must be ensured by the FoP.
- Integrity and authenticity of remote logs: The remote logs generated by the FoP 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.

8.2.3.6 Threats

8.2.3.6.1 Attackers

The following attackers are considered:

- Attacker on the supervision network: The attacker controls a device plugged on the supervision network of the FoP.
- Attacker on the process network: The attacker controls a device plugged on the field network.
- Evil user: The attacker has compromised an unprivileged account and tries to bypass the access control policy of the FoP.

8.2.3.6.2 Threats

The following threats are considered:

---

8 Confidentiality is not a primary measure for protecting industrial control systems; it is an in-depth defence measure. This security property can also be required for industrial secrecy purposes.

9 Confidentiality is not a primary measure for protecting industrial control systems; it is an in-depth defence measure. This security property can also be required for industrial secrecy purposes.

10 All authentication mechanisms offered by the FoP may not necessarily be part of a security profile. However, those not included in the security profile must be disabled by default.

- Denial of service: The attacker manages to generate a denial of service on the FoP 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 FoP or only some of its functions.
- Firmware alteration: The attacker manages to inject and run a corrupted firmware on the FoP. 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 FoP by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the FoP without having the privilege to do so.
- Execution mode alteration: The attacker manages to modify the execution mode of the FoP without being authorized (a stop command for instance).
- User program compromise: The attacker manages to obtain some parts of the configuration of the FoP by other means than the observation of the activity of the FoP11.
- User program alteration: The attacker manages to modify, temporarily or permanently, the user program.
- Configuration alteration: The attacker manages to modify, temporary or permanently, the FoP configuration.
- Configuration compromise: The attacker manages to illegally obtain some parts of the FoP 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 FoP.
- 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 FoP or to transmit commands without being authorized.
- Flows alteration: The attacker manages to corrupt exchanges between the FoP 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 FoP and an external component.

8.2.3.6.3 Critical assets vs. Threats Rationale

The following table is provided as an example. It allows checking the completeness of the analysis of threats against critical assets:

11 This threat is considered only when the confidentiality of the user program has been identified as critical.

A Critical assets vs threats

	Control-command of the industrial process	Data exchanges between the ToE and the supervision	Engineering workstation flows	Data exchanges between the ToE and another PLC	Firmware	User program	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		
Firmware alteration					I Au										
Execution mode alteration								I							
User program compromise						(C)									
User program alteration	I					I Au									
Configuation alteration							I								
Configuration compromise							(C)								
Credentials theft										C I C					
Authentication violation									I Au						
Access control violation											I				
Local logs alteration														I Au	
Remote logs alteration															I Au
Parameters or command injection	Av I	I Au													
Flows alteration	Av I	I Au	I Au	I Au											
Flows compromise			(C)												

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

Figure 25 Critical assets vs. Threats Rationale

8.2.3.7 Security functions

8.2.3.7.1 Security Functions

The following security functions are considered:

- Malformed input management: The FoP has been developed in order to handle correctly malformed input, in particular malformed network traffic.
- Secure storage of secrets: User secrets are securely stored in the FoP. 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, 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 FoP.
- Integrity and authenticity of the user program: The FoP ensures the integrity of the user program. Only authorized users can modify it.

- Confidentiality of the user program: The FoP protects the confidentiality of the user program. Only authorized users can access it.
- Integrity and authenticity of commands and PLC mode: The FoP must ensure that the execution mode of the FoP can only be modified by authorized users. This implies, in particular, that they are authenticated.
- Secure communication: The FoP supports secured communication, 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 FoP 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.

8.2.3.7.2 Threats vs. Security Functions Rationale

The following table is given as an example. It allows checking the completeness of the coverage of threats by security functions:

	Denial of service	Firmware alteration	Execution mode alteration	User program compromise	User program alteration	Configuation 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 input 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 program					X										
Confidentiality of the user program				X											
Integrity and authenticity of commands and PLC mode			X												
Secure communication													X	X	X
Logs integrity											X				
Alarms integrity												X			

Figure 26 Threats vs. Security Functions Rationale

8.2.4 Example of security functions and component requirements mapping

The following table links security functions of the proposed Protection Profile for the PLC **Family of Products** (FoP) and the security requirements of IEC 62443-4-2.

The first column of the table presents a series of **security objectives** (and assumptions possibly) proposed as a rationale of choice of security functions in the Protection Profile.

The second column presents associated/equivalent component requirements in IEC 62443-4-2 (NB: “all component requirements are met” does NOT mean that “the associated security objective is met”).

PP PLC Short term v1.1: Security Objectives (Claim)	62443-4-2 Requirements (details of the claim)	
Malformed input management: The FoP has been developped in order to handle correctly malformed input, in particular malformed network traffic.	CR-3.5	Input validation
	CR-7.1	Denial of service protection
	CR-7.1 RE 1	Manage communication loads
	CR-7.2	Resource management
Secure storage of secrets: User secrets are securely stored in the FoP. In particular, the compromise of a file is not sufficient for retrieving them.	CR-4.1	Information confidentiality
	CR-4.3	Use of cryptography
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.	CR-1.1	Human user identification and authentication
	CR-1.1 RE 1	Unique identification and authentication
	CR-1.2	Software process and device identification and authentication
	CR-1.2 RE 1	Unique 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-1.7 RE 1	Password generation and lifetime restrictions for human users
	(CR-1.7 RE 2)?	Password lifetime restrictions for all users
	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-3.8	Session integrity
	CR-3.8 RE 1	Invalidation of session IDs after session termination
	CR-3.8 RE 2	Unique session ID generation
	CR-3.8 RE 3	Randomness of session IDs
	CR 4.3	Use of cryptography
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.	CR-2.1	Authorization enforcement
	CR-2.1 RE 1	Authorization enforcement for all users
	CR-2.1 RE 2	Permission mapping to roles
	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: At each update of the firmware, integrity and authenticity of the new firmware are checked before updating.	CR-3.4	Software and information integrity
	CR-3.4 RE 1	Automated notification about integrity violations
	CR 4.3	Use of cryptography
Configuration confidentiality and integrity: The access control prevents any unauthorized person to read or modify the configuration of the FoP.	CR-3.4	Software and information integrity
	CR-3.4 RE 1	Automated notification about integrity violations
	CR-4.1	Information confidentiality
	CR 4.3	Use of cryptography
Integrity and authenticity of the user program: The FoP ensure the integrity of the user	CR-1.1	Human user identification and authentication

PP PLC Short term v1.1: Security Objectives (Claim)	62443-4-2 Requirements (details of the claim)	
program. Only authorized users can modify it.	CR-1.1 RE 1	Unique identification and authentication
	CR-1.2	Software process and device identification and authentication
	CR-1.2 RE 1	Unique identification and authentication
	CR-3.4	Software and information integrity
	CR-3.4 RE 1	Automated notification about integrity violations
	CR 4.3	Use of cryptography
Confidentiality of the user program: The FoP protects the confidentiality of the user program. Only authorized users can access it.	CR-4.1	Information confidentiality
	CR 4.3	Use of cryptography
Integrity and authenticity of commands and PLC mode: The FoP must ensure that the execution mode of the FoP can only be modified by authorized users. This implies, in particular, that they are authenticated.	CR-1.1	Human user identification and authentication
	CR-1.1 RE 1	Unique identification and authentication
	CR-1.2	Software process and device identification and authentication
	CR-1.2 RE 1	Unique identification and authentication
	CR-3.4	Software and information integrity
	CR-3.4 RE 1	Automated notification about integrity violations
Secure communication: The FoP supports secured communication, protected in integrity and authenticity. If required, confidentiality is enforced with external components.	CR-1.1	Human user identification and authentication
	CR-1.1 RE 1	Unique identification and authentication
	CR-1.2	Software process and device identification and authentication
	CR-1.2 RE 1	Unique identification and authentication
	CR-3.1	Communication integrity
	CR-3.1 RE 1	Cryptographic integrity protection
	CR-3.8	Session integrity
	CR-3.8 RE 1	Invalidation of session IDs after session termination
	CR-3.8 RE 2	Unique session ID generation
	CR-3.8 RE 3	Randomness of session IDs
	CR-4.1	Information confidentiality
	CR 4.3	Use of cryptography
PP PLC Short term v1.1: Assumptions		
Premises: The FoP is located in secure premises with a restricted access limited to trustworthy people. In articular, the attacker does not have access to the physical ports of the FoP. Since identical products to the FoP may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.		
Active logging: We assume that local and remote logging are operational and that local logs are not corrupted.	CR-2.8	Auditable events
	CR-2.9	Audit storage capacity
	CR-2.9 RE 1	Warn when audit record storage capacity threshold reached
	CR-2.10	Response to audit processing failures
	CR-2.11	Timestamps
	CR-2.11 RE 1	Internal time synchronization
	CR-2.12	Non-repudiation

PP PLC Short term v1.1: Security Objectives (Claim)	62443-4-2 Requirements (details of the claim)	
	CR-6.1	Audit log accessibility
	CR-6.2	Continuous monitoring
Unevaluated services disabled by default: Services of the FoP which are not covered by the security target are disabled in the default configuration (also named factory default configuration).	CR-7.7	Least functionality

Figure 27 Security functions Vs. component requirements mapping

8.3 Annex 3: Further views on evaluation, certification and accreditation

8.3.1 Further reflections about evaluations

Security evaluations, as defined in section 4.2.2, are based on a "security assurance case" made of claims, arguments and evidences. A security assurance case is the base of the demonstration of the satisfaction of the requirements mentioned in the Security Profile of a specific IACS product that is presented in the evaluation report to the certification body for validation. And if validated, the certifier delivers the label (ICCS-C2) or certificate (ICCS-A or ICCS-B).

A Security Assurance Case is "*a documented body of pieces of evidence that substantiates a convincing and valid set of arguments that relate to security claims made in a product's Security Profile*". The following diagram shows the link between claims, arguments and evidence:

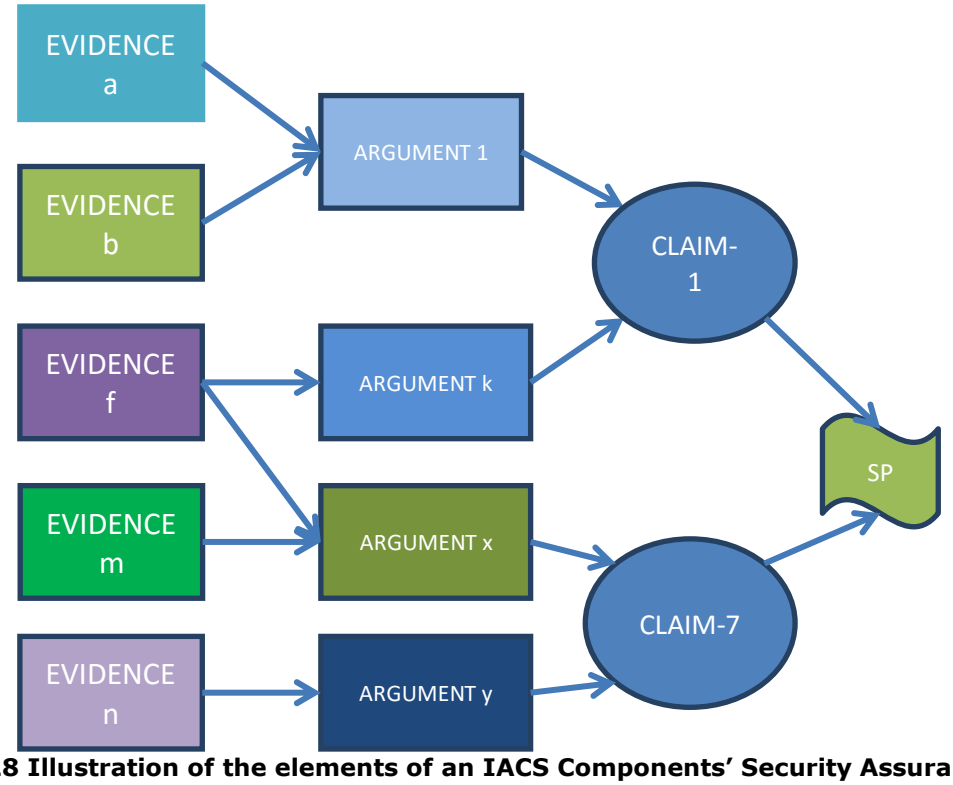

Figure 28 Illustration of the elements of an IACS Components' Security Assurance Case

A claim is the assertion that an IACS product meets a component security requirement (Figure 22 and section 8.2.4). It can be verified to be true or not.

An argument is the way a claimed satisfaction of a requirement is effectively implemented in the product. It provides the link between claims and pieces of evidence. This corresponds roughly to the security functions or mechanisms fitted in the product.

An evidence, or piece of evidence, is the "proof" presented in support of arguments and therefore of claims in a security evaluation. Depending on the chosen ICCS, evaluation activities will vary and pieces of evidence will be of different natures and evidences may be assessment results or test results.

8.3.2 Further precisions about documents for evaluation requests

"Evaluation Request Document" is a generic term for any document that presents the request of a vendor or buyer to have an IACS product evaluated according to one of the four schemes proposed in the ICCF. Such a document should include elements of information such as the reference and description of the product and of its expected characteristics and performance, and also how to configure, implement, operate, maintain, replace and decommission the product. A technical manual is an essential part of this product documentation. Information should be up-to-date, accurate and complete. Its text should be clear and concise. The information should be organized in a hierarchical and consistent manner by use of headings. Technical descriptions should be function-based. Instructions should be procedure-based. Step numbering should be used to support the levels of information. Illustrations (photo, drawings, and graphs) should be provided to support information and text.

8.3.3 Precautions about Compliance Assessments in ICCS-B and ICCS-A

The compliance of a product to its Security Profile (see 4.2.6.2) should be validated and recorded before other evaluation activities take place in the context of ICCS-B & ICCS-A.

8.3.4 Further precisions on accreditation

An accreditation body is an authoritative body allowed to give formal recognition that another Body (e.g. Certification Body, Test Laboratory) is competent to carry out the specific tasks in its remit on the basis of specified standards. Examples of Authoritative Bodies are: American National Standards Institute (ANSI), European Accreditation (EA). At EU national level, each country has its own Accreditation Body. The national accreditation bodies listed at http://www.european-accreditation.org/information/national-accreditation-bodies-having-been-successfully-peer-evaluated-by-ea have been successfully evaluated by EA for accreditation of verifiers as required by Article 64 of the European Commission's Regulation (EU) No 600/2012 and, according to Article 66(1) of the Regulation, Member States shall accept the accreditation certificates of verifiers accredited by these national accreditation bodies and respect the right of the verifiers to carry out verification for their scope of accreditation. National Accreditation Bodies (AB) having government recognition operate to internationally recognized standards and are themselves regularly reviewed by their international peers.

The International Accreditation Forum, Inc. (IAF) is the world association of Conformity Assessment Accreditation Bodies and other bodies interested in conformity assessment in the fields of management systems, products, services, personnel and other similar programs of conformity assessment. Its primary function is to develop a single worldwide program of conformity assessment which reduces risk for business and its customers by assuring them that accredited certificates may be relied upon. Accreditation assures users of the competence and impartiality of the body

accredited. IAF members accredit certification or registration bodies that issue certificates attesting that an organization's management, products or personnel comply with a specified standard (called conformity assessment). More information: http://www.iaf.nu.

8.3.5 The current ERNCIP Inventory Database in the ICCF

The current ERNCIP Inventory is a European central repository with information on European experimental and testing facilities with CIP-related capabilities. The objective of the Inventory is to help all types of critical infrastructure stakeholders to identify and make contact with CIP-related experimental facilities with the competency of their interest. The system is a search tool which stores comprehensive profiles of the European laboratories. The profiles in the Inventory contain basic information about the facility, including contact data; thorough description of competencies; offered services; accreditations and certificates hold; and also the experimental or testing equipment that the facility possesses. The Inventory Database is accessible at https://erncip.jrc.ec.europa.eu.

The following figure provides a screenshot of the Inventory's home page.

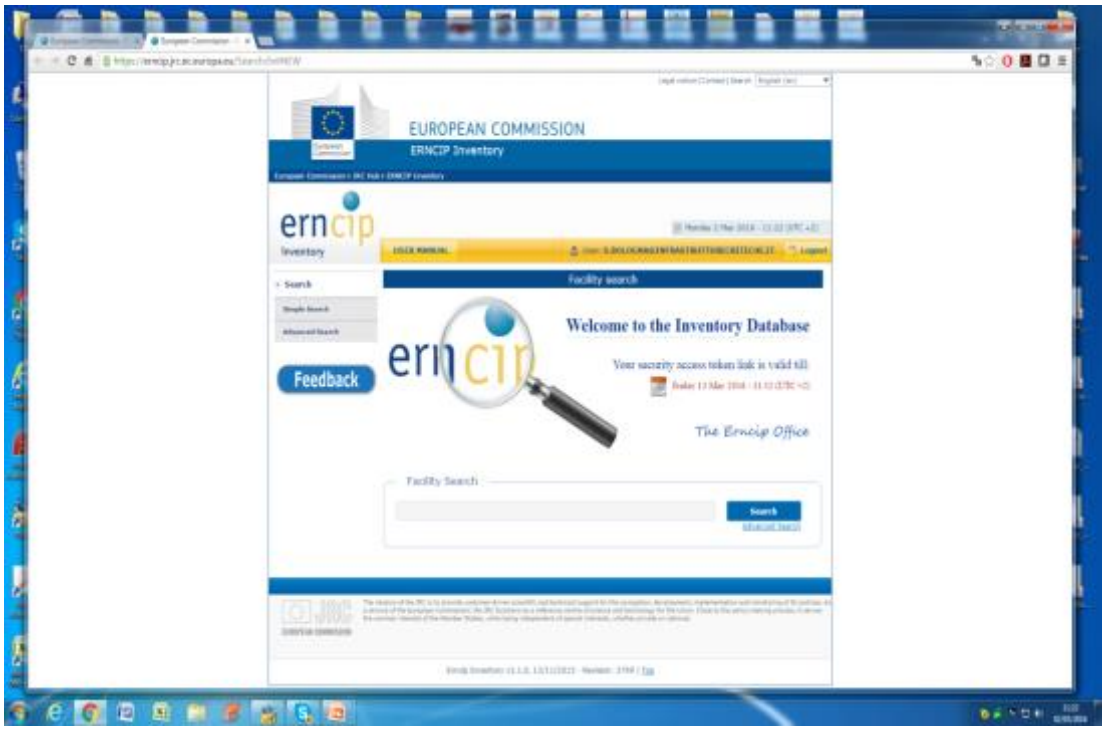

Figure 29 Screenshot of the homepage of the Inventory Database

In June 2016, Google-like searches for the following keywords gave the following results:

- **IACS Testing Laboratory** gave 66 results but only 1 including the word IACS;
- **SCADA Testing Laboratory** gave 77 results but only 18 including the word SCADA;
- **IACS Component Testing Laboratory** gave 88 results but only 1 including the word IACS;
- **SCADA Component Testing Laboratory** gave 78 results but only 12 including the word SCADA;
- **Certification Body** gave 22 results;
- **Accreditation Body** gave 16 results.

8.4 Annex 4: Bridging vocabulary and conventions

This annex provides alternative or complementary definitions useful for the readers of this report to bridge it with other standards they might be familiar with. At the current stage of maturity of the report, this annex may be incomplete and stand as work-in-progress.

8.4.1 Cyber resilience

Many definitions exist and the following ones are quoted only as examples.

(MITRE, 2011) [7] defines a cyber-attack as "*An attack on cyber resources. The attack is typically, but not necessarily, carried out by cyber means. The attack may be intended to adversely affect the cyber resources, or to adversely affect the missions, business functions, organizations, or populations that depend on those resources*."

(MITRE, 2011) [7] also defines cyber resilience as "*The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function*."

And it defines cyber resilience engineering as "*The sub-discipline of mission assurance engineering which considers the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and the trade-offs associated with different strategies for applying those practices*."

8.4.2 ISASecure Embedded Device Security Assurance certification scheme

As an example, the following table compiles some definitions given by the ISA Security Compliance Institute in (ASCI EDSA-100 Version 2, 2011) for Embedded Device Security Assurance / ISASecure certification scheme. This table is not definitive and may be extended in the future.

Word / Concept	Source	Definition / Comments
PRODUCT		
Embedded device	(ASCI EDSA-100 Version 2, 2011)	Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
Version (of embedded device)	(ASCI EDSA-100 Version 2, 2011)	A well-defined release of an embedded device, typically identified by a release number
ROLES		
Automation Standards Compliance Institute (ASCI)	(ASCI EDSA-100 Version 2, 2011)	ASCI, as the legal entity representing ISCI, grants chartered laboratory status or CRT laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI
ISA Security Compliance Institute (ISCI)	(ASCI EDSA-100 Version 2, 2011)	ISCI defines, maintains and manages the overall ISASecure EDSA certification program, grants recognition to qualified CRT tools, interprets the ISASecure EDSA specifications and maintains a web site for publishing program documentation, as well as lists of chartered laboratories, CRT laboratories, recognized CRT tools and certified devices.
Accreditation body	(ASCI EDSA-100 Version 2, 2011)	Third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment
Certifier (see also Chartered laboratory)	(ASCI EDSA-100 Version 2, 2011)	Chartered laboratory, which is an organization that is qualified to certify embedded devices as ISASecure. This term is used when a simpler term that indicates the role of a "chartered laboratory" is clearer in a particular context.

Chartered laboratory	(ASCI EDSA-100 Version 2, 2011)	Organization chartered by ASCI to evaluate devices under the ISASecure EDSA certification program and to grant certifications. A chartered laboratory is the conformity assessment body for the ISASecure EDSA program. Chartered laboratories accept applications from device vendors for device certification, evaluate devices, and grant device certifications to device vendors (conformity assessment body). Note that either a chartered laboratory or a CRT laboratory may perform CRT for a device evaluation. In either case, a chartered laboratory is the entity that grants an ISASecure EDSA certification.
Conformity assessment body	(ASCI EDSA-100 Version 2, 2011)	Body that performs conformity assessment services and that can be the object of accreditation This is an ISO/IEC term and concept. For ISASecure EDSA, the conformity assessment body is a chartered laboratory
Communication robustness (CRT) testing laboratory	(ASCI EDSA-100 Version 2, 2011)	Organization authorized by ASCI to perform *EDSA communication robustness testing* and submit results to a chartered laboratory (certifier) as evidence toward certification. CRT laboratories test devices to the CRT requirements and submit results to chartered laboratories as evidence toward a certification.
Tool supplier	(ASCI EDSA-100 Version 2, 2011)	Provider of a test tool to support communication robustness testing. CRT tool suppliers provide test tools that allow chartered laboratories or CRT laboratories to carry out CRT, and allow device vendors to test their devices in advance of formal evaluation for certification. An organization may perform either one or both of the roles tool supplier and CRT laboratory.
End user	(ASCI EDSA-100 Version 2, 2011)	Organization that purchases, uses or is impacted by the security of embedded devices. End users define procurement criteria for embedded devices, and may request an ISASecure device certified to a particular level
Device vendor	(ASCI EDSA-100 Version 2, 2011)	Organization that is responsible for compliance of an embedded device with ISASecure requirements. Device vendors apply for certification of their embedded devices (supplier).
CERTIFICATION		
Certification	(ASCI EDSA-100 Version 2, 2011)	Third party attestation related to products, processes, or persons, that conveys assurance that specified requirements have been demonstrated. For ISASecure EDSA, this is an authorized evaluation of an embedded device to the ISASecure EDSA criteria, which, when successful, permits the device vendor to advertise this achievement in accordance with certification program guidelines
Certified device	(ASCI EDSA-100 Version 2, 2011)	A well-defined version of an embedded device that has undergone an evaluation by a chartered laboratory, has met the ISASecure EDSA criteria and has been granted certified status by the chartered laboratory
Certificate	(ASCI EDSA-100 Version 2, 2011)	A document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program For ISASecure EDSA, there are certificates for certified devices, recognized CRT tools, chartered laboratories, CRT laboratories.
Symbol	(ASCI EDSA-100 Version 2, 2011)	Graphic affixed or displayed to designate that ISASecure certification has been achieved. An earlier term for symbol is “mark.”
EVALUATIONS		
Conformity assessment	(ASCI EDSA-100 Version 2, 2011)	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

Communication robustness testing (CRT)	(ASCI EDSA-100 Version 2, 2011)	Tests that determine the extent to which an embedded device maintains its essential functions under adverse network traffic conditions CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks.
Functional security assessment (FSA)	(ASCI EDSA-100 Version 2, 2011)	Assessment of a defined list of security features for an embedded device The FSA examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device's overall system environment.
Software development security assessment (SDSA)	(ASCI EDSA-100 Version 2, 2011)	An assessment of the software development process which produced a particular embedded device, from the point of view of the security of a device so produced
PROCESS		
ASCI conformance program	(ASCI EDSA-100 Version 2, 2011)	A program managed by ASCI that offers evaluation of products or processes to a standard or other consensus specification. Several types of documents define the ISASecure EDSA certification program: • Technical specifications that describe the technical criteria applied to determine whether a device will be certified; • Accreditation/recognition that describe how an organization can become a chartered or CRT laboratory, and how a tool supplier can obtain recognition for a CRT tool; • Symbol and certificates that cover the topic of proper usage of the ISASecure symbol and certificates; • Structure, used to describe and operate the overall program; • External references that are documents that exist outside of this particular program that are referenced by ISASecure EDSA program documents.
Certification scheme	(ASCI EDSA-100 Version 2, 2011)	The overall definition of and process for operating a certification program.
Recognized CRT tool	(ASCI EDSA-100 Version 2, 2011)	A test tool that has been evaluated by ISCI and determined to meet applicable requirements for carrying out ISASecure EDSA communication robustness testing
Version (of ISASecure certification)	(ASCI EDSA-100 Version 2, 2011)	The ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a year and release number, such as ISASecure EDSA 2010.2.
Provisional chartered status	(ASCI EDSA-100 Version 2, 2011)	An interim, temporary accreditation status during which a chartered laboratory is authorized to evaluate embedded devices and grant ISASecure EDSA certifications. Provisional accreditation requirements ensure that the laboratory is organized and prepared to carry out ISASecure certifications in a competent, impartial and confidential manner.

Figure 30 ISASecure EDSA definitions

9 Table of illustrations

10 References

[1] DHS, “NCCIC / ICS-CERT FY 2015 Annual Vulnerability Coordination Report,” 2015. [Online]. 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].

[2] IEC 62443-4-2, “Security for industrial automation and control systems. Technical security requirements for IACS components,” , , Draft 2, Edit 4, July 2, 2015.

[3] P. Theron, “ICT Resilience as dynamic process and cumulative aptitude,” in *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, P. Theron and S. Bologna, Eds., PA, Hershey, IGI Global, 2013, pp. 1-35.

[4] ASCI EDSA-100 Version 2, “ISA Security Compliance Institute - Embedded Device Security Assurance - ISASecure certification scheme,” Automation Standards Compliance Institute, , 2011.

[5] H. Tardieu, A. Rochfeld and R. Colletti, La méthode Merise : Principes et outils, Paris: Éditions d'organisation, 1983.

[6] H. Tardieu, A. Rochfeld, R. Colletti, G. Panet and G. Vahée, La méthode Merise, Paris: Éditions d'organisation, 1985.

[7] MITRE, “cyber resiliency engineering framework,” , , 2011.

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (**http://europa.eu**).

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**).

KJ-01-17-099-EN-N

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

Publications Office

doi:10.2760/717579

ISBN 978-92-79-65842-6