[redacted]

# Thematic Area
# Industrial Control Systems and Smart Grids

[redacted]

[redacted]

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

[redacted]

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 721, 21027 Ispra (VA), Italy
E-mail: erncip-office@jrc.ec.europa.eu
Tel: +39 0332 78 6211
Fax: +39 0332 78 5469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/



JRC94533

EUR 27098 EN

ISBN 978-92-79-45417-2

ISSN 1831-9424

doi:10.2788/21726

Luxembourg: Publications Office of the European Union, 2014



Printed in Italy

| VALIDATION OF THE DOCUMENT | | | |
|---|---|---|---|
| | NAME | FUNCTION | DATE |
| Written by: | Paul THERON<br>Sandro BOLOGNA | Coordinator of the TG<br>Deputy coordinator | 3.11.2014 |
| Verified by: | DG JRC<br>TG members | NA | 3.11.2014 to<br>14.12.2014 |
| Accepted by: | DG JRC | NA | 19.1.2015 |

| TRANSMISSION OF THE DOCUMENT | | |
|---|---|---|
| TRANSMITTED BY | TO | DATE |
| Paul Theron | DG JRC | 3.11.2014 |

| REVISIONS OF THE DOCUMENT | | |
|---|---|---|
| VERSION | DATE | CONTENTS OR MODIFICATIONS |
| 1.0 | 3.11.2014 | Initial version |
| 1.1 | 1.12.2014 | Version reviewed with DG JRC for TG members' comments |
| 1.2 | 19.1.2015 | Version submitted to proof-reader and JRC publication repository (Pubsy) |

This Thematic Group report is the result of the contributions of the Group's members and represents the views of the majority of the participating representatives and their organisations.

# CONTENTS

# 1 Executive summary

All recently published studies agree. Industrial Automation and Control Systems (IACS) increasingly constitute a target for cyber-attacks aimed at disturbing Member States' economies, at disabling our critical infrastructures or at taking advantage of our people. Such hostile acts take place in a context of geostrategic tensions, for the satisfaction of organised crime's purposes, or else in support of possible activist causes.

In this context, the ERNCIP Thematic Group (TG), Case studies for the Cyber-security of Industrial Automation & Control Systems was started in January 2014 to answer the question: 'Do European critical infrastructure operators need to get IACS' components or sub-systems tested and "certified" (T&C) with regard to their cyber-security?' And if the answer was yes, it had to answer a corollary question: 'What are (roughly) the conditions of feasibility for successfully implementing a European IACS T&C scheme ([1])?'

This TG's undertaking was a research project, not a task force seeking to deliver an immediately applicable standard. It mobilised representatives of IACS vendors, industrial operators, European Institutions and national cyber-security authorities.

This report presents:

- The results of 13 short case studies and TG experts' discussions that helped in answering the first question: they concluded that industry operators had an appetite for cyber-security certified IACS products. In addition, they showed that provided a European certification scheme would be in line with the state of the art, supported by mutual recognition agreements ([2]) between Member States (and beyond Europe), and not mandatory, it would be viable for vendors.
- A set of research directions in the form of a possible European IACS Cyber-security Compliance & Certification (C&C) scheme ([3]), as an answer to the corollary question: 2 levels of increasingly trustworthy compliance assessment and 2 levels of increasingly demanding certification were identified and broadly depicted. These four levels were intended to engage vendors progressively into certification and to provide clients and national cyber-security authorities with a flexible tool to specify the level of their requirements for compliance, procurement and other purposes. This C&C scheme relies on a few important assumptions:
    - All existing cyber-security certification standards applicable to IACS products of a designated level of criticality ([4]) verify that products comply with common cyber-security requirements: therefore, given the intense discussions about the choice of a standard finding their common denominator to create a European scheme could be an idea;
    - Product certification is easier to implement than system certification in the first place and, as IACS products are developed by many suppliers from all over the world and as, in comparison, certifying their development process is harder, limiting our ambition initially to product certification sounds like a good, realistic first step towards the benefit of the industrial community.
- A research and action roadmap towards the possible implementation of the proposed European IACS components Cyber-security Compliance & Certification Scheme: it proposes a set of seven actions to be run over the 2015-20 period. This plan should start very soon with Action No 1 aiming at prioritising work, at engaging a wider set of stakeholders and at creating the conditions for an effective implementation of a European IACS components Cyber-security Compliance & Certification Scheme within what appears to be a favourable window of opportunity.

([1]) The term scheme was used in this report by virtue of its original brief. See the proposed scheme in section 5.3.
([2]) This is an issue to be addressed in project #5 of the action plan (see Section 6).
([3]) The report shows that we moved from the concept of Testing & Certification to that of Compliance & Certification.
([4]) A risk analysis, or knowing that the target sector of use could help in determining the criticality of IACS components.

NB: Project No 1 will frame the work to be done in project Nos 2 to 7 and, as needed, its participants will then have an opportunity to refine the proposals and schedule proposed in this report as an input to DG JRC.

# 2 Contributors and acknowledgments

The study was launched under the supervision of DG JRC.

The core team of the project was composed of:

- Mr Paul Théron (Thales Communications & Security), coordinator of the TG;
- Mr Sandro Bologna (AIIC), deputy coordinator;
- Representatives of DG JRC when appropriate:
    - Mrs Naouma Kourti;
    - Mr Georgios Giannopoulos;
    - Mr Peter Gattinesi;
    - Mr Gian Luigi Ruzzante;
    - Mr Alessandro Lazari.

This report is the result of the contribution of the following TG members:

National cyber-security agencies and alike:

- Mr Mathieu Feuillet (ANSSI, France);
- Mr Jonathan L. (MOD, UK);
- Mr Samuel Linares (CCI, Spain);
- Mr Ignacio Paredes (CCI, Spain);
- Mr Enrique Redondo (INCIBE, Spain);
- Mr Jens Wiesner (BSI, Germany).

IACS vendors:

- Mr Jean-Michel Brun (Schneider Electric, France);
- Mr Jean-Christophe Mathieu (Siemens, Germany).

Industrial operators:

- Mr Viorel Ciprian Achim (Transgaz, Romania);
- Mr Julien Didon (ADP, France);
- Mr Philippe Jeannin (RTE, France);
- Mr Gheorghe Stoia (Transgaz, Romania).

Integrators, specialist consultants and universities:

- Mr Thieyacine Fall (Thales, France);
- Mr Alberto Sanna (Istituto San Raffaele, Italy);
- Mr Hector Puyosa, (UPCT, Spain);
- Mr Enzo Maria Tieghi (ServiTecno srl, Italy).

Also, we wish to mention the contribution of ENISA (Mr Adrian Pauna) to the discussions held.

Finally, we wish to thank Mrs Maria-Giovanna Giuliani (DG JRC) for her administrative organisation of the TG's meetings.

# 3 Introduction: background, goals, principles, limits and structure of the study

## 3.1 The ERNCIP

The European Reference Network for Critical Infrastructure Protection (ERNCIP) forms part of the European Programme for Critical Infrastructure Protection (EPCIP), and aims at providing a framework within which experimental installations will share knowledge and expertise throughout Europe leading to improved protection of critical infrastructure against all hazards. ERNCIP objectives are to harmonise test protocols, and to improve the conditions for EU-wide certification and standardisation of security solutions. This will be a step change towards a more trusted, homogeneous and outreaching EU market for security-related equipment and systems, services and applications from which all CIP-related stakeholders will benefit. The mission of ERNCIP is, 'to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities'.

## 3.2 Background

Cyber-attacks targeting industrial automation and control systems (IACS) have been perpetrated for some years already. STUXNET, the piece of malware that affected Iranian nuclear installations, was probably climactic in raising the industrial community's awareness of the risk plants, their neighbourhood and customers might suffer should a significant cyber-attack hit them. The (ENISA, 2013) threat landscape indicates that the various cyber-threats targeting critical infrastructures are increasing. And the question of the potential impacts of cyber-attacks on IACS had been raised even earlier, for instance in (Stamp, Laviolette, Phillips, & Richardson, 2009).

Thus, the (ENISA, 2011) report's recommendation No 5 reflected the industrial community's need to test and certify IACS' cyber-security in those terms:

> 'ICS manufacturers are starting to (or will have to) include security requirements in the design phase of ICS components and applications. However, operators indicate that independent evaluations and tests are missing to effectively guarantee that those devices are in fact secure and that interoperability has also been considered when the new security features/capabilities are included. Furthermore, penetration tests and white box audits in controlled laboratories have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included into the development cycle. In any case, manufacturers, ICS security tools and services providers, as well as operators cannot be completely aware of the implications a modification may have with respect to their own systems or third-party ones. Moreover, it is important to certify that ICS do comply with minimum quality requirements with respect to cyber-security programming bugs.*'* (p. 45).

## 3.3 Questions

The Case studies for the Cyber-security of Industrial Automation & Control Systems thematic group (TG) sought to answer two connected questions:

1. Can we confirm the need of European critical infrastructure (CI) operators to have the cyber-security of IACS components or sub-systems that they buy from vendors tested and 'certified' (T&C) through at least three case studies?
2. If yes, what would be the principal conditions of feasibility to make such a scheme happen?
    - How should it be done?
    - Based on which standard(s)?
    - Who should do it?
    - Where should it be done?
    - Who should bear the costs for its development?

- What is the benefit?

## 3.4 Goals

Started with a kick-off meeting in March 2014 after a pre-meeting held in Paris in January 2014, and to be ended in November 2014, it was to deliver:

- The results of at least three case studies showing how industrial operators' need for cyber-security testing and certification would be expressed:
  - The idea of performing case studies stemmed from (Mahan, et al., 2011) who, based on an IEC 62443 generic IACS architecture, identified data transfers as points of vulnerability in IACS. In the present report, we considered data links as one of the potential points of vulnerability of IACS and extended the principle.
- A research and action roadmap towards a future EU IACS cyber-security certification scheme:
  - The ERNCIP Case studies for the cyber-security of Industrial Automation & Control Systems Thematic Group was conceived as a research project aiming at defining directions about how to tackle the TG's research questions, not as an initiative aimed at delivering a proposal or standard to be immediately applicable.

## 3.5 Methodology

The TG's work was organised in three successive phases:

- Phase 1: Needs identification — 19 March 2014 (Kick-off) to June meeting, seeking to:
  - Set our common work plan for phase 1;
  - Identify case studies understood as points of potential cyber vulnerability within IACS; five case studies were identified; they refer to IACS components that can embed security functions and solutions but are not security products themselves:
    - SCADA ([5]) systems that supervise entire industrial systems;
    - PLCs/IEDs ([6]), i.e. field process automation and control equipment;
    - Engineering/Programming workstations that staff connect to in order to program the field components of an IACS;
    - Databases used for process control (if corrupted may create safety issues, e.g. in luggage handling);
    - Telecommunication links (for instance for remote equipment maintenance).
  - Each case study was to be situated in a sector of activity:
    - Hospital, airport, electricity distribution, car manufacturing, chemicals…
  - Phase 1's method consisted of the following arrangements:
    - A questionnaire was elaborated in order to understand stakeholders' views of the cyber threat and to analyse their background concerns behind the question of IACS cyber-security certification. This questionnaire was dispatched to TG members and other industrial operators. On reception of answers (13 in total) only basic statistics were performed in order to 'profile' the positions expressed by the respondents;
    - Literature review, including: (ENISA, 2011), (ENISA, 2013a), reports from the SCADA LAB project ([7]), (MITRE, 2011), cyber-security certification standards (Common Criteria — ISO 15408, ISA Secure ([8]) and its derived Wurldtech CRT scheme ([9]);

([5]) Supervisory Control And Data Acquisition; See (ENISA, 2011a) for detailed definitions of IACS components.
([6]) PLC: Programmable Logic Controller; IED: Intelligent Electronic Device.
([7]) at https://www.scadalab.eu/index.php/mod.documentos/mem.listado/relmenu.3
([8]) Managed by ISCI; see at www.isasecure.org
([9]) See at www.wurldtech.com

        - A Project's core team meeting to analyse and synthesise results and to elaborate findings before the June meeting;
        - A TG expert group meeting in June (Ispra) to discuss phase 1's findings and to conclude on the need for IACS testing and certification in Europe. This meeting also discussed existing cyber-security schemes (CC, ISA Secure, Wurldtech) and confirmed the need for a European IACS certification scheme. It concluded that the focus of the scheme had to be on IACS components, i.e. individual products rather than sub-systems or systems.
- Phase 2: Conditions of feasibility — 18 June 2014 to September meeting, seeking to:
    - Define the concept of IACS testing & certification if phase 1 answered yes to the question about the need for such a scheme in Europe;
    - Perform the corresponding feasibility study;
    - Define a plan of action towards the possible implementation of the scheme over the next five years.
    - Phase 2's method consisted of the following arrangements:
        - The project's core team first worked to elaborate a basic scheme proposal;
        - Face-to-face meetings with TG members (national cyber-security authority, industrial operators, vendor) were then organised to react to and to amend the proposed scheme; significant modifications were then brought to the original proposal and made it more realistic, helping to finesse the goals and broad characteristics of the scheme;
        - The project's core team then finalised phase 2's findings and elaborated a plan of action for the next five years (2015-20), and prepared the September meeting of the TG experts;
        - The TG expert group met in September (Ispra) to discuss and finalise the proposed European IACS components Cyber-security Compliance & Certification Scheme;
        - The proposed scheme was discussed with ENISA at the September meeting (video conference) and later presented at the ESSENCE Project's meeting of 14 October. This latter presentation did not generate any revision of the scheme.
- Phase 3: Report — 24 September 2014 to 1 November 2014, seeking to:
    - Deliver DG JRC the report of the thematic group's work;
    - Phase 2's method consisted of the following arrangements:
        - TG coordinators worked to write the final report of the study;
        - This report was reviewed by TG members and by DG JRC.

The following diagram summarises the methodological process of the study:

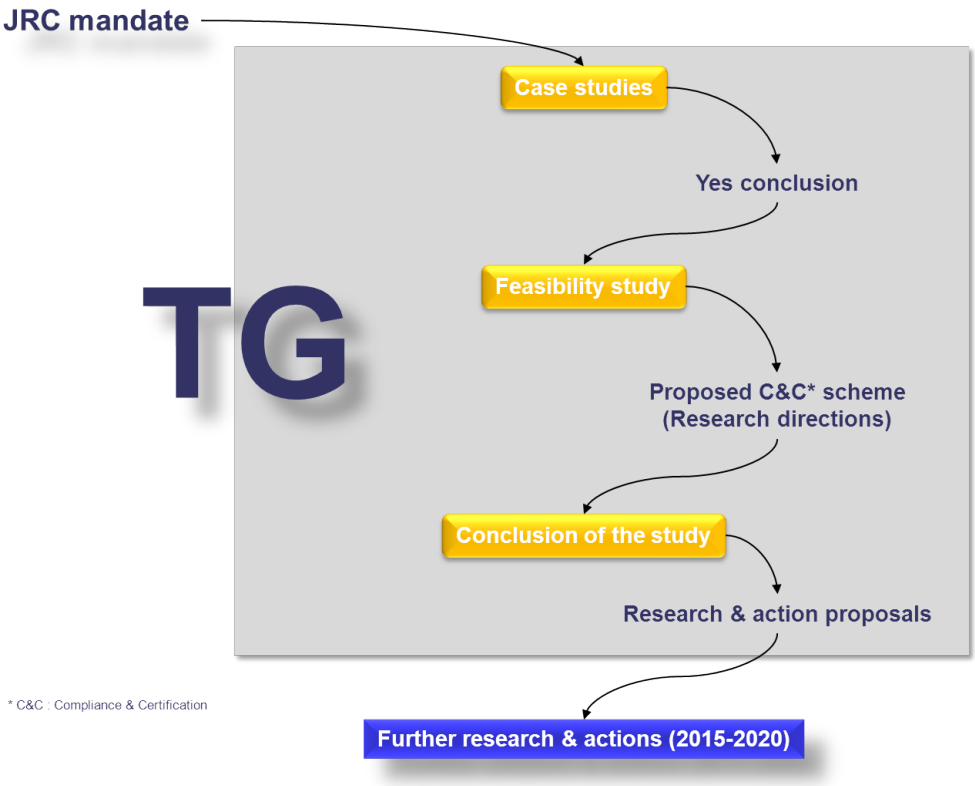



**Figure 1 The TG process**

In addition, three general principles were adopted from the start for the conduct of the study:

- Pragmatism:
  - This TG has gathered a limited number of experts representing industry users/operators, vendors of IACS solutions and national cyber-security authorities;
  - Case studies were used to study essentially industry users' background concerns that would lead to express a need for cyber-security testing and certification;
  - A focus on product certification from the very start, rather than on systems certification, a topic immediately considered as too wide and complicated to address. This view was of particular importance especially if considering that vendors should undergo such certification when they are not always, if not rarely, the integrators and installers of their industrial automation and control products.
- Rapidity
  - Started in January 2014, the TG was to end its work in November 2014. Its work was organised with DG JRC only around the contribution of its limited set of experts and did not include larger meetings, nor dissemination activities.
- Confidentiality
  - Traffic Light Protocol ([10]): all contributions, in phase 1, were made under this protocol and as a result this report only presents the synthesis and conclusions of the TG's work.

## 3.6 Limits of the study

This work had a limited ambition, to propose research directions about IACS cyber-security testing and certification. The present report shows how this research into the two fundamental questions at hand was performed within the short time frame allocated to the TG by a limited set of people selected for their expertise, field practice and representativeness of the different parties in presence. However, it

([10]) See the explanation provided in the ERNCIP Membership Agreement on the website at https://erncip-project.jrc.ec.europa.eu/download-area/finish/24-erncip-office-reports/46-erncip-tgs-membership-agreement

does not pretend to express all views possibly held by the immense number of industries, integrators and vendors who populate the industrial automation and control domain.

## 3.7 Validation

The directions that this report presents have been validated and are endorsed by the members of the TG. The validation process is described along this report as opportunity arises. This report outlines the precautions taken in the conduct of the study and in order to gain feedback from TG members, ENISA and outside audiences. In particular, this report draws the JRC's attention to the rationale behind the collective progressive elaboration of the European IACS components Cyber-security Compliance & Certification Scheme.

## 3.8 Structure of the report

The report is presented as follows:

- Chapter 4 presents the method, findings and conclusions of the case studies (phase 1);
- Chapter 5 presents the European IACS components Cyber-security Compliance & Certification Scheme proposed as a result of phase 2;
- Chapter 6 presents a proposition for a research and action plan for 2015-20;
- Chapter 7 delivers the conclusions of our work;
- Chapter 8 — Annexes — presents complementary elements in support of previous chapters;
- Chapter 9 — Table of illustrations;
- A bibliography is supplied at the end of the document.

# 4 Results and validation of the case studies

Because of the small number of cases studied, the following results do not constitute a statistical analysis. Questionnaires were sent to industrial operators to collect their background perception of the cyber threat against IACS. Other stakeholders' opinions were duly considered in the TG's discussions, and all stakeholders should be involved in the action plan presented in Section 6.

## 4.1 Results from the case studies

This section shows how industrial operators present in the TG see the cyber-threat against IACS.

### 4.1.1 Questionnaires: the background perception of the cyber-threat

13 questionnaires were returned, all but one filled-in by industrial operators, the other being answered by a national cyber-security authority who presented the case of an industrial system:

- 4 SCADA cases;
- 1 process database case;
- 3 engineering workstation cases;
- 4 PLC cases;
- 1 telecom link case.

Respondents belong mainly to the energy sector:

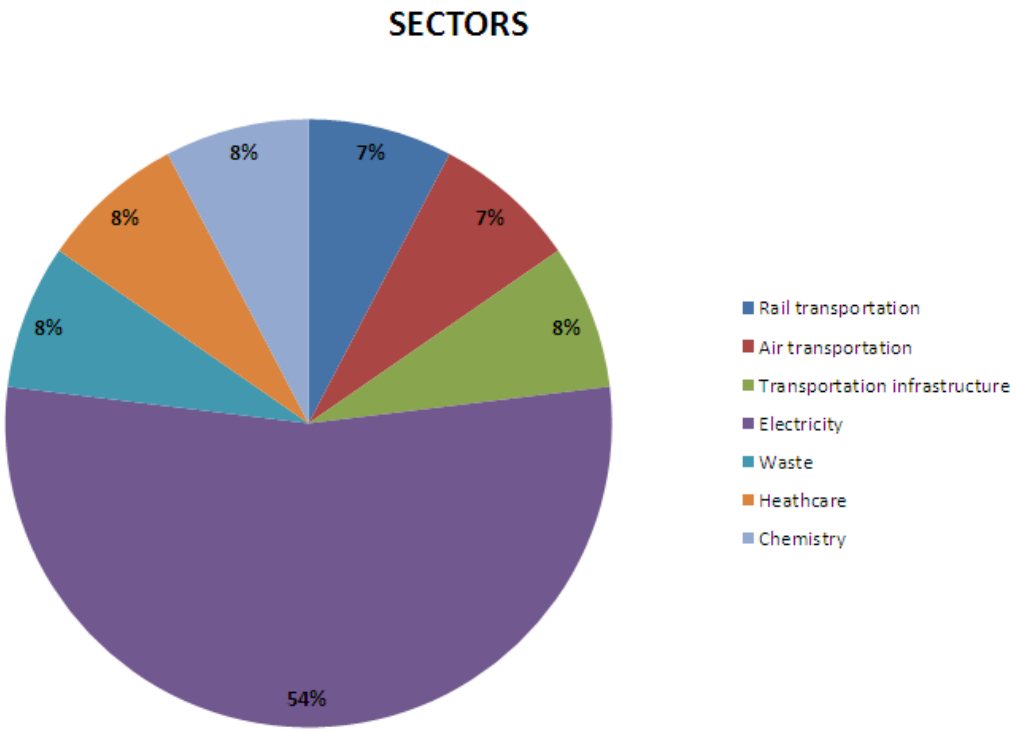



**Figure 2 Respondents to the phase 1 questionnaire**

They belong to the following Member States:

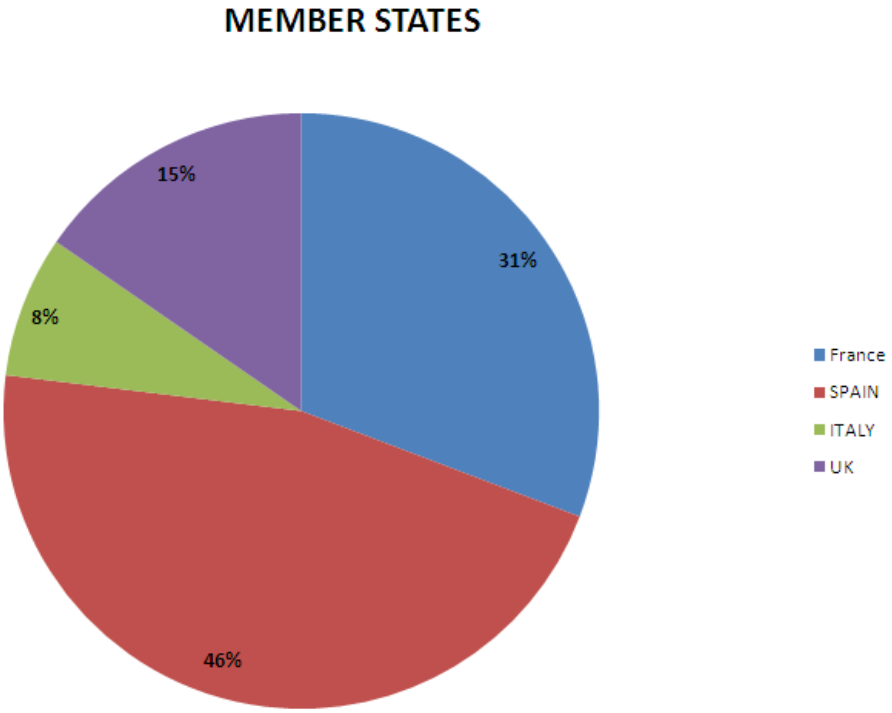



**Figure 3 Member States of origin of the phase 1 questionnaire**

Respondents consider that IACS cyber attackers belong almost equally to four categories:

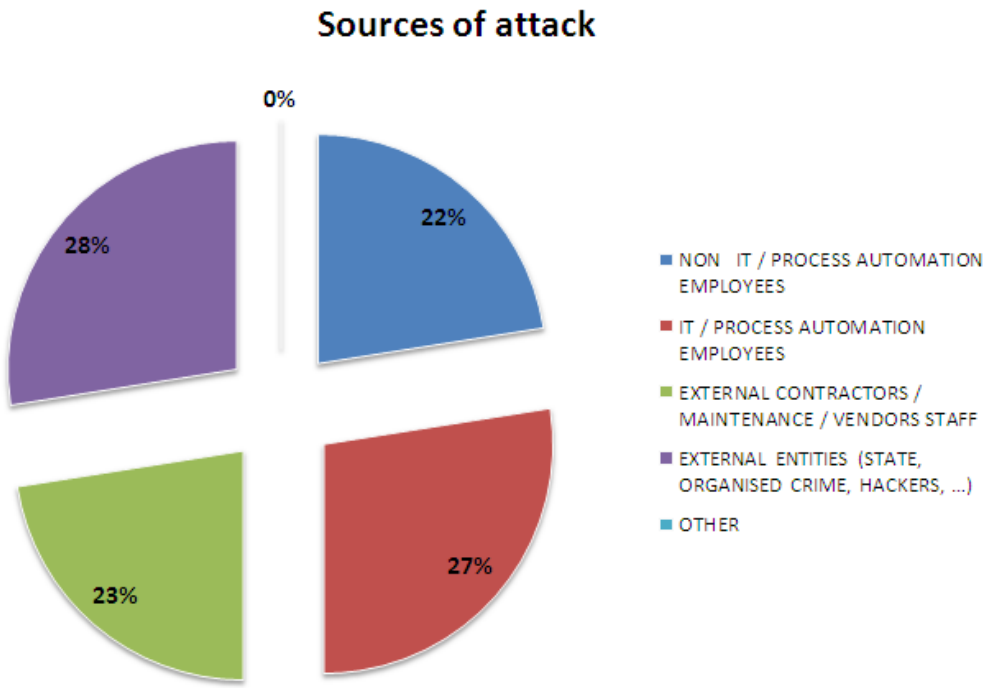



**Figure 4 Sources of attacks (phase 1 questionnaire)**

TG members believe that attackers have motivations that hard to hierarchise:

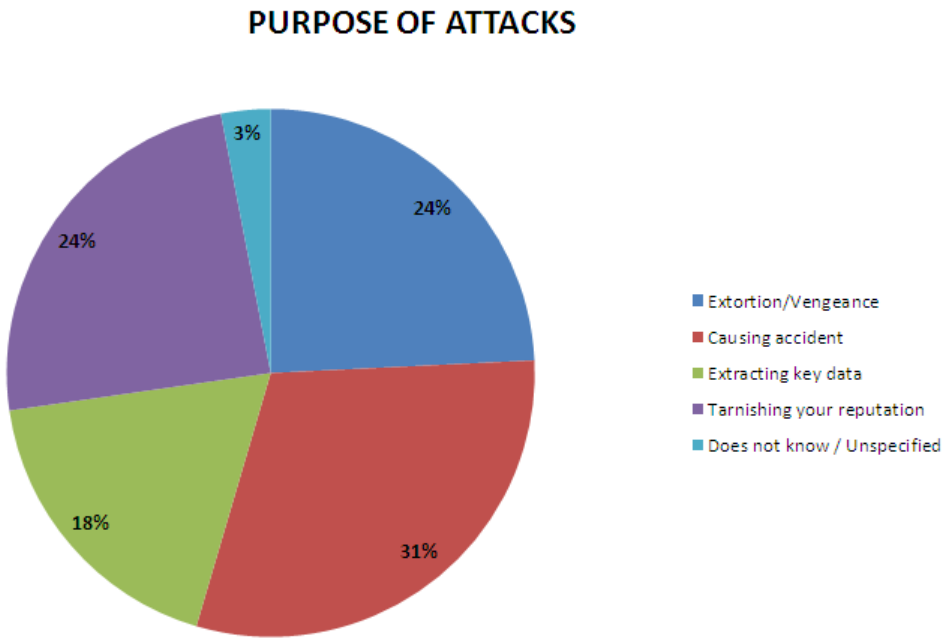



**Figure 5 Purpose of attacks (phase 1 questionnaire)**

They may use a panoply of attack vectors:

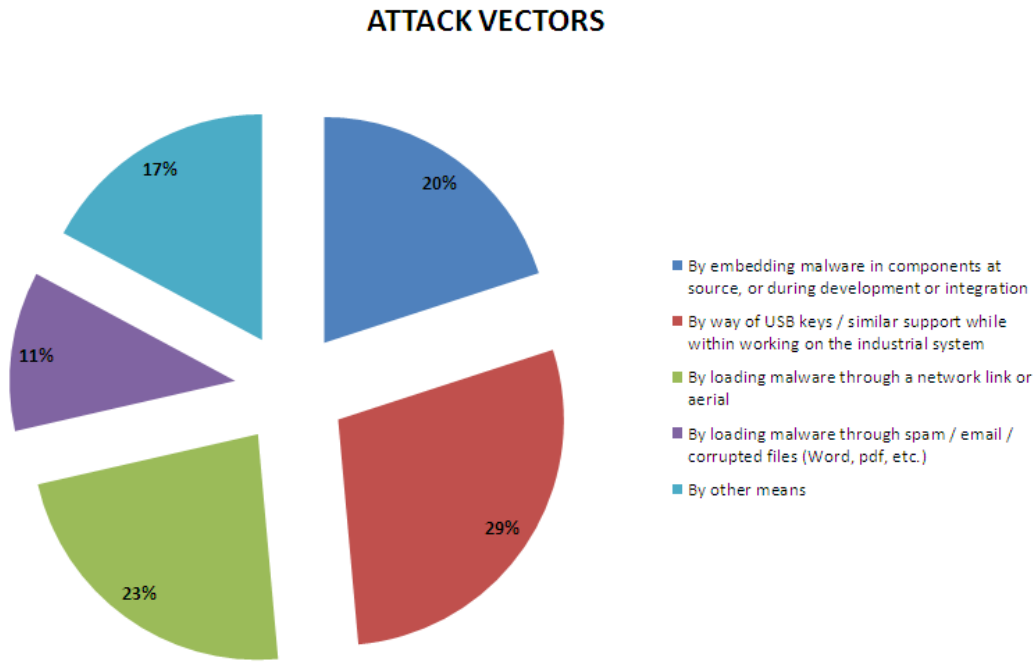



**Figure 6 Attack vectors (phase 1 questionnaire)**

IACS' vulnerabilities can be identified mainly internally, or by suppliers, TG members say:

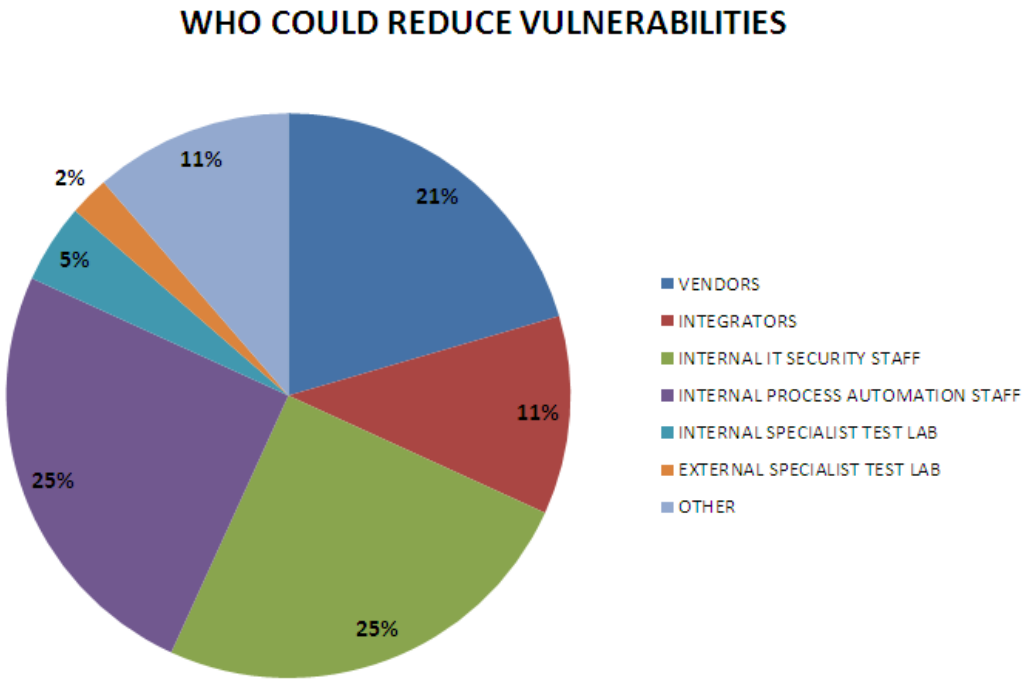



**Figure 7 Who could reduce vulnerabilities (phase 1 questionnaire)**

These vulnerabilities can be identified through specific tests and 'in production' (i.e. during the operation of IACS):

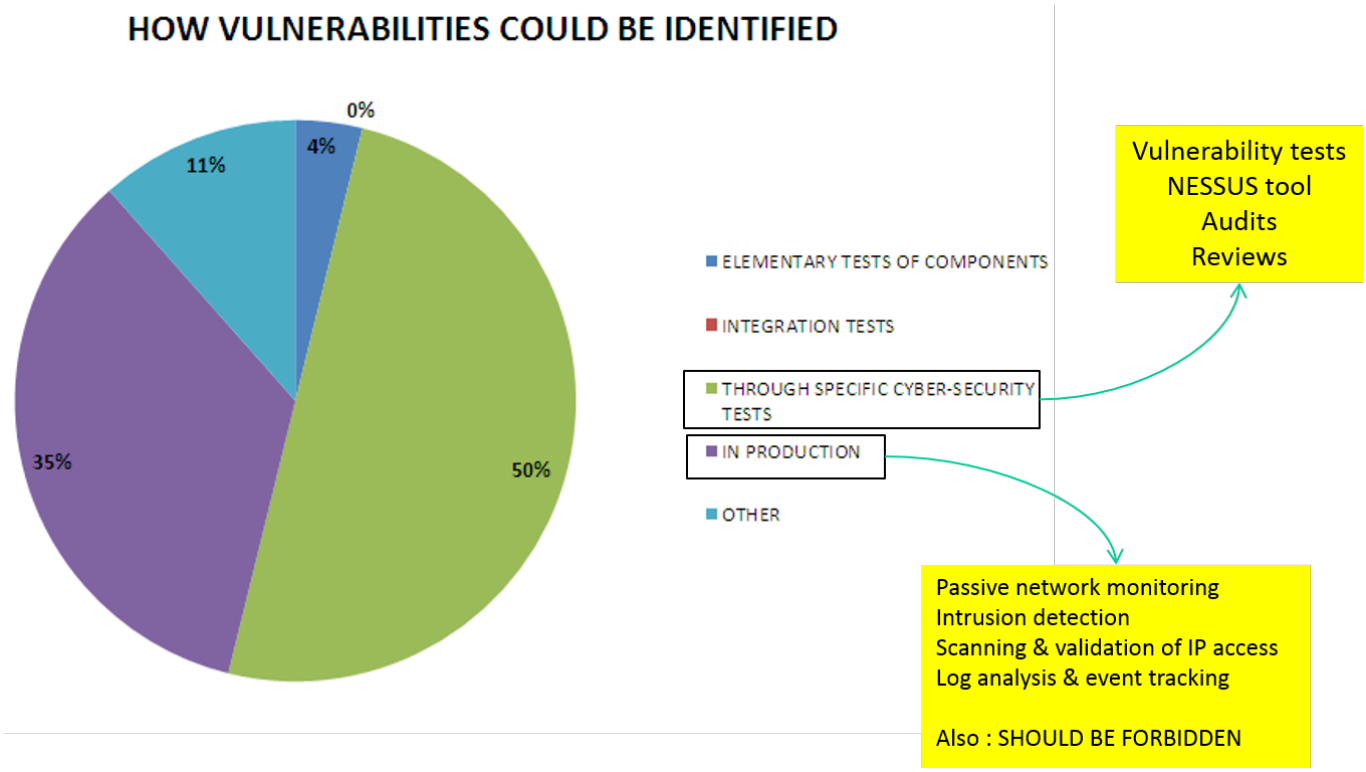



**Figure 8 How vulnerabilities could be identified (phase 1 questionnaire)**

A number of means are suggested to identify cyber vulnerabilities in both contexts. However a voice was raised to say that identifying vulnerabilities in operation should be forbidden for this may create

operational risks. It also has to be noted that the techniques mentioned in this latter context belong in incident detection rather than vulnerability identification in the proper sense.

### 4.1.2 Interpretation of the questionnaires

In conclusion, the questionnaire suggests that:

- TG members are well aware of the cyber threat;
- TG members see the full picture of it but could not prioritise threats, motivations, vectors, etc;
- TG members might currently resort to internal scanning techniques to detect attacks;
- TG members might also wish for suppliers to take their share of the effort to identify vulnerabilities and to reduce them before IACS components are put into operation.

This last point is interesting in the context of this study in the sense that it signifies that should vendors certify their IACS products, clients would welcome the initiative.

### 4.1.3 Discussion of these results: the need for IACS certification

The June meeting of our TG allowed discussion of these results. The main outcome of the debate was that:

- TG experts unanimously agreed on the outcome of phase 1;
- There is currently no European obligation for IACS cyber-security certification;
- Previous ENISA studies have long affirmed the need for IACS cyber-security certification;
- Additionally, in the USA, France, etc., some form of IACS cyber-security certification may have already started;
- Users ([11]) basically want a reassurance that industrial products they buy are cyber secure;
- Users would buy cyber-security certified IACS products rather than non-cyber-security certified ones, provided that this would come at an acceptable cost;
- Compared with plants' set-up and running costs, paying extra to get cyber-secured IACS products was said by participants to be inexpensive, though no clear consensus was reached;
- Vendors added that selling cyber-security certified products would not entail unbearable extra costs for them and was feasible;
- However if IEC 62443 is still a work in progress for some and a good reference for others, Common Criteria appear also as a possible candidate standard for T&C but were deemed too heavy and costly by other TG members who called for a lighter version of Common Criteria.

In conclusion:

- TG experts asserted the need for an IACS cyber-security T&C ([12]) scheme;
- However T&C has limits:
    - It is valid for a given component, in a given version, for specified operating conditions;
    - Cyber-security testing and certification must focus on IACS products/components only (note that even PLCs may be already fairly complicated systems), not on entire systems or sub-systems. Beyond products' T&C, integrators and users will need further efforts to cyber-secure systems and plants (engineering, HR qualification, etc.);
    - A well-shared scheme or standard is required in order to facilitate mutual recognition ([13]) of certificates across Europe (and beyond) and to keep certification costs and complexity down for vendors.

([11]) Process control engineering and procurement services.
([12]) T&C: abbreviation for Testing & Certification.
([13]) For more details on mutual recognition of certificates, refer to the IECEE/CB scheme at http://www.iecee.org/cbscheme/cbfunct.pdf

## 4.2 Literature review

### 4.2.1 ENISA's 2011 report: Protecting Industrial Control Systems

The (ENISA, 2011) report lists 10 recommendations. Among them, recommendation 5, Creation of a common test bed, or alternatively, an ICS security certification framework, states:

> 'The Common ICS security strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership that leverages existing initiatives (e.g. EuroSCSiE). This test bed would make use of realistic environments with the appropriate resources for conducting independent verification and validation tests. These tests should include, at least:
>
> - Check the compliance of applications and systems with specific security profiles;
> - Verify and validate that programming good practices and methodologies are being applied;
> - Certify that ICT security tools and services are compatible with specific ICS systems, applications and specific set-ups.
>
> Product/services certification would not be mandatory but should also be considered as an option.'

### 4.2.2 ENISA's 2013 report: Good Practices for an EU ICS Testing Coordination Capability

Many experts consider necessary the creation or adaptation of existing certification frameworks to IACS environments as a way to ensure a minimum level of cyber-security of IACS infrastructures across the European Union. Some countries like Germany and England are currently working on adaptations of Common Criteria (ISO 15408) to IACS environments ([14]).

Experts also indicated that testing without delivering a certification would convey less attractiveness and market value. Besides, a certification not based on tests would be insufficient.

Several options have been expressed by experts about 'what should be certified':

- Devices: Interesting for stakeholders, but already being done in several test beds and can be too costly for companies with many different products;
- Development process: This could provide more reassurance than device-only certification;
- Security postures: This is a direction some Member States are already working on;
- Whole architecture of the systems;
- Test beds: Many experts consider that in addition to any certification, a European body should accredit those centres that are mature enough to perform appropriate testing.

The diversity of technologies and points of view is expected to be very challenging, especially when taking into account that many legacy components are still in production while others are much more up-to-date. Also, the most current reference standards ([15]) in this field have been fairly well agreed upon though opinions vary about their maturity, but they can be used as a starting point.

### 4.2.3 MITRE 2011 cyber resilience engineering framework

Cyber-attacks come as a surprise, though to a fair extent much can be done to prevent their occurrence. Cyber resilience is an answer to this fact. As illustrated by three examples presented below, cyber resilience engineering frameworks are applied at the 'system' level rather than at the component/device level of testing and certification targets. However, such frameworks suggest that IACS component testing should assess not only their protective capabilities but also their reactive capabilities.

([14]) These projects are performed independently and, according to some experts, the compatibility of their approaches would have to be examined.
([15]) Like ISA-99.

The (MITRE, 2011) cyber resilience engineering framework defines cyber resilience as 'The ability of a nation, organisation, 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.' (p. 8).

This definition accommodates two different views over cyber resilience: the technical perspective of systems able to withstand hazards and malicious acts, and the management perspective of organisations withstanding attacks over the systems on which they depend.

It takes into account the following objectives:

- to understand the threat;
- to prepare for it;
- to prevent it;
- to continue activities despite it;
- to constrain (limit) damages resulting from an attack;
- to reconstitute a functioning system after an attack;
- to transform the way activities are performed to lessen attack possibilities;
- to re-architect systems in order to enhance their cyber-security capabilities.

In order to fully address the cyber-risk, (MITRE, 2013) suggests that cyber resilience should be engineered according to the following logic:

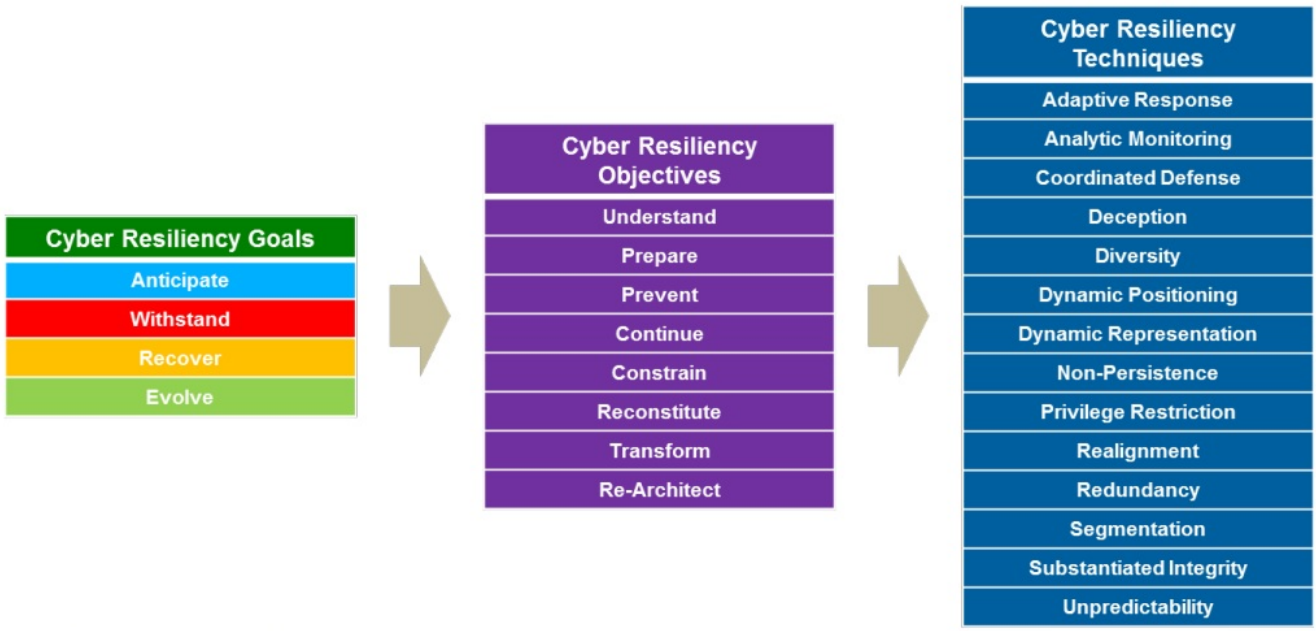



**Figure 9 MITRE's model of cyber-resilience engineering**

The 'resilience umbrella' model presented in (EUROCONTROL, 2012) Manual for National ATM Security Oversight includes pre-incident activities (prevention, preparation) and post-incident activities (emergency response, operational continuity, recovery). The feedback loop of systems and organisations' improvement (transform, re-architect) seen in the MITRE model is not explicitly present.

Another model of resilience engineering can be found in (ENISA, 2011a) and (THERON, 2013). Somehow consistent with (MITRE, 2011), first it is based on the idea that socio-technical systems may collapse under adverse circumstances. It defines target levels of resilience (from 1 — minor incidents — to 6 — extreme shocks) according to the severity of potential cyber-attacks.

Secondly, it articulates the engineering disciplines required to provide each target level of resilience: performance engineering, safety and security engineering, survivability engineering.

Thirdly, these disciplines bring engineers to design and implement proactive pre-incident cyber-security mechanisms: prevision of potential threats (anticipation), prevention (elimination at source) of cyber threats, protection against threats that cannot be prevented, as well as reactive post-incident cyber-security mechanisms: recognition (detection and analysis) of cyber-attacks, response to cyber-attacks (restoration of systems) and recovery (of full business performance and of enhanced daily capacities to thrive).

### 4.2.4 Conclusion of the literature review

Literature has already fairly much advocated cyber-security testing and certification (T&C) for IACS as seen in ENISA reports. Besides, they tend to put some emphasis on the device/component level as one that can be mastered more easily than systems as a whole. And they highlight stakeholders' opposition to mandatory certification schemes (maybe for the time being…). Finally literature recognises that cyber-attacks are unavoidable despite efforts placed on protective measures, and it calls for cyber-resilience.

This suggests the following conclusions:

1. The meaning of IACS components' cyber-security certification is limited to the security objectives (security profile) of a given device in a given context. Beyond those limits, attackers may find ways to cyber-attack a device and certificates constitute no guarantee of results.
2. To go beyond the certification of a device's cyber-protective features, assessments could also address the process by which components are developed and the extent to which cyber-security is taken into account in this context.
3. Cyber-security certification is currently envisaged as being limited to IACS components' proactive pre-incident protection capabilities. But due to the rising need for cyber-resilience the question has to be asked (in a project of the action plan presented in Section 6) if certification should also cover post-incident reactive capabilities that guarantee that despite cyber-attacks a device can continue its mission and recover a nominal level of performance within specified conditions.

## 4.3 Analysis of existing cyber-security certification schemes

### 4.3.1 The Common Criteria scheme (ISO 15408)

The Common Criteria is also known as ISO 15408.

The following quotation describes the background of this cyber-security certification scheme.

***Establishing a Common Criteria***
*Common Criteria Certification provides independent, objective validation of the reliability, quality and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level, and assurance that all goals are met.*

***The history of Common Criteria***
*The Common Criteria is a descendant of the US Department of Defence Trusted Security Evaluation Criteria (TCSEC) originally in the 1970s. TCSEC was informally known as the 'Orange Book'. Several years later Germany issued its own version, the Green Book, as did the British and the Canadians. A consolidated European standard for security evaluations, known as ITSEC, soon followed. The United States joined the Europeans to develop the first version of the international Common Criteria in 1994. The current version of the Common Criteria, 2.1, was issued in August 1999.*

*The Common Criteria is also known as ISO 15408. The international community has embraced the Common Criteria through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The National Information Assurance Partnership (NIAP) was formed to administer a security evaluation programme in the United States that utilises the Common Criteria as the standard for evaluation.*

***Achieving Common Criteria Certification***
*Common Criteria Certification is a rigorous process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluation of products against security requirements. Products are tested against functional security requirements based on predefined Evaluations Assurance Levels (EALs).*

*For healthcare, financial services and other industries, the need for security is no less important. Whether they are protecting their customers' privacy, or intellectual and financial assets, assurance that networks, hard drives and phone lines are safe and secure from hackers, viruses and other malicious activities is critical. Common Criteria Certification, while not a requirement, can provide independent validation.*

***For more information about Common Criteria**, refer to the portal at:*
*http://www.commoncriteriaportal.org/*

The Common Criteria scheme relies upon 11 functionality classes and 8 assurance classes:

| Functionality | Assurance |
|---|---|
| • Security Audit;<br>• Cryptographic Support;<br>• Communication;<br>• User Data Protection;<br>• Identification and Authentication;<br>• Privacy;<br>• Protection of TOE Security Functions;<br>• Resource Utilisation;<br>• Security Management;<br>• TOE Access;<br>• Trusted Path/Channels. | • Protection Profile evaluation;<br>• Security Target evaluation;<br>• Composition;<br>• Development;<br>• Guidance Documents;<br>• Life Cycle Support;<br>• Tests;<br>• Vulnerability Assessment. |

Each of these is broken down into families and then into components.

7 Evaluation Assurance Levels (EAL) are defined:

- Evaluation assurance level 1 (EAL1) — functionally tested;
- Evaluation assurance level 2 (EAL2) — structurally tested;
- Evaluation assurance level 3 (EAL3) — methodically tested and checked;
- Evaluation assurance level 4 (EAL4) — methodically designed, tested and reviewed;
- Evaluation assurance level 5 (EAL5) — semi-formally designed and tested;
- Evaluation assurance level 6 (EAL6) — semi-formally verified design and tested;
- Evaluation assurance level 7 (EAL7) — formally verified design and tested.

Each EAL ([16]) requires a specific set of assessments (of assurance classes) and each number (1, 2, etc.) in the boxes identifies the corresponding assurance components to assess (if applicable):

([16]) NB: The table here is reproduced from ISO 15408:2007, Section 8.1 (Table 1 — Evaluation assurance level summary).

| Assurance class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Development | ADV_ARC | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 |
| | ADV_INT | | | | | **2** | **3** | 3 |
| | ADV_SPM | | | | | | **1** | 1 |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** |
| Guidance documents | AGD_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Life-cycle support | ALC_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 |
| | ALC_DEL | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | **1** | 1 | 1 | 1 | **2** |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 |
| Security Target evaluation | ASE_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| | ASE_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 |
| | ATE_DPT | | | **1** | 1 | **3** | 3 | **4** |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** |
| Vulnerability assessment | AVA_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 |

**Figure 10 Common Criteria Evaluation Assurance Levels**

It was a common opinion among the TG's members that Common Criteria is heavy to apply and too costly to be supported by IACS vendors or their clients. Also, it was agreed at the June meeting that the certification of vendors' development lifecycles would not be a burden for them as already much effort has been thrust into this area.

### 4.3.2 The ISASecure Certification Programme

ISCI (ISA Security Compliance Institute) is a not-for-profit organisation incorporated by ISA in 2006 to provide a home for certification, conformance and compliance assessment activities in the automation arena.

Its governing board is comprised of an ISA 99 committee liaison person and four chairmen from Exxon Mobil, Honeywell, Chevron and Yokogawa. Invensys (now Schneider Electric) is a strategic member.

The ISASecure certification scheme was derived from the framework of the ISA99 Standards Roadmap ([17]):

([17]) http://isa99.isa.org/ISA99 Wiki/Home.aspx

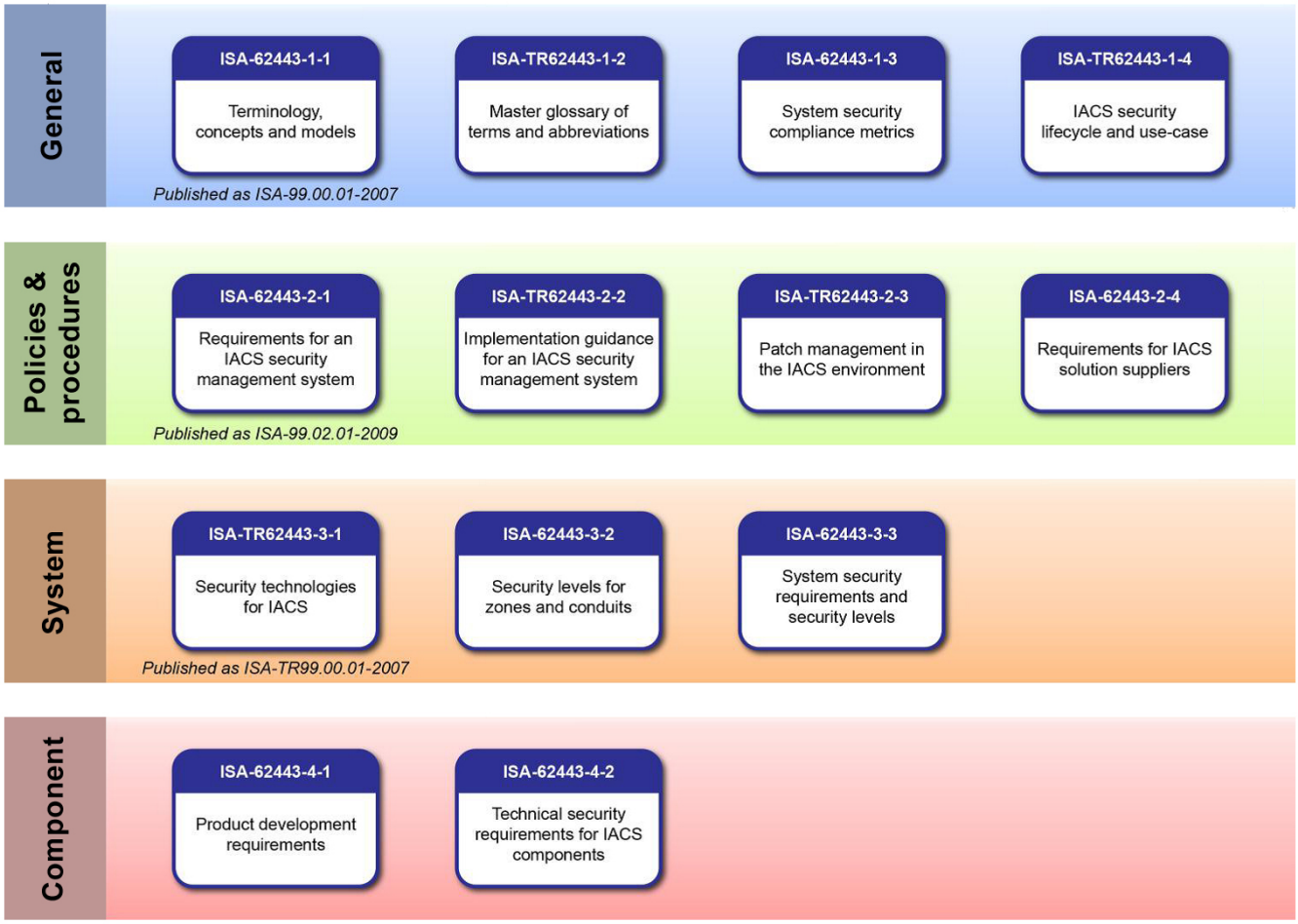



**Figure 11 ISASecure certification scheme**

The ISCI has developed three certifications:

- Functional Security Assessment (FSA);
- Software Development Security Assessment (SDSA);
- Communication Robustness Testing (CRT).

Functional Security Assessment (FSA) is a set of security functions requirements derived from NIST SP 800-53. This includes:

- Access control (access control authorisation, user authentication…);
- Use control (device authentication, audit trail…);
- Data integrity;
- Data confidentiality;
- Restrict data flow (security function isolation…);
- Incident response support;
- Network resource availability (back up, recovery…).

For each requirement a target level (1, 2, 3) is set.

Software Development Security Assessment (SDSA) is a set of requirements in compliance with:

- IEC 61508 (SIL level, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, essentially software requirements);
- ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation);
- Microsoft SDLC;

- CLASP (Comprehensive, Lightweight Application Security Process) from OWASP which addresses applying security to an organisation's application development process.

Requirements are split into 12 chapters:

- PH1 Security Management Process (SMP);
- PH2 Security Requirements Specification (SRS);
- PH3 Security Architecture Design (SAD);
- PH4 Security Risk Assessment and Threat Modelling (SRA);
- PH5 Detailed Software Design (DSD);
- PH6 Document Security Guidelines (DSG);
- PH7 Module Implementation & Verification (MIV);
- PH8 Security Integration Testing (SIT);
- PH9 Security Process Verification (SPV);
- PH10 Security Response Planning (SRP);
- PH11 Security Validation Testing (SVT);
- PH12 Security Response Execution (SRE).

Communication Robustness Testing (CRT) is a set of testing requirements for the following protocols:

- Ethernet, IP v4, ARP, ICMP v4, UDP, TCP.

These tests include resistance to attacks such as SYN flood and invalid packets (fuzzing).

ISCI evaluates cyber-security CRT tools to ensure that the tool's test suites meet the published ISASecure EDSA CRT requirements and are capable of consistently executing ISASecure EDSA CRT certification tests. They recommend the use of such tools. In Japan, under the name, Japanese ISASecure Certification Programme, the Control System Security Centre (CSSC) has been accredited by ISCI and developed a cyber-security test bed in 2012 funded by the Japanese Government (METI, Ministry of Economy, Trade and Industry). Evaluation, certification and incident analysis will be conducted using this test bed. Exida, LLC (a privately held company established in Germany and the US) is another ISCI-accredited test laboratory.

The test platforms currently compliant seem to be:

- Codenomicon (very recent 11.2013) with a product named Defensics X. Codenomicon is privately held by private investment funds (Verdane Capital, Prime Technology Ventures);
- Wurldtech (since 2010) with the Achilles Satellite r3 Level 2. Wurldtech was acquired by GE in May 2014.

The ISA Security Compliance Institute (ISCI) and Wurldtech Security Technologies, Inc. also announced in September 2010 the completion of a collaborative project to make the Wurldtech Achilles Level 1™ certification test specifications converge with the ISASecure™ Embedded Device Security Assurance (EDSA) and communication robustness test (CRT).

However, and with all due precautions, it seems that only a small number of IACS devices have been ISASecure certified:

- 3 from Honeywell Process solutions;
- 1 from Yokogawa;
- 1 from RTP Corporation.

Since February 2014, the ISCI has launched two new certifications:

- System Security Assurance (SSA);
- Software Development Lifecycle Assessment (SDLA).

SSA is a security development process evaluation scheme based on a number of assumptions:

- The control system consists of an integrated set of components and includes more than one device;
- The control system is available from and supported as a whole by a single supplier, although it may include hardware and software components from several manufacturers;
- The supplier has assigned a unique product identifier to the control system which the supplier uses in the marketplace to refer to the integrated set of components as a whole;
- The system product is under configuration control and version management.

SDLA is a certification scheme that assesses a supplier's product development lifecycle processes for industrial automation control systems. An SDLA certification is granted for:

- A named development organisation or organisations;
- A specific version of a named, documented development lifecycle process under version control that is used by that organisation(s);
- A certification level of 1, 2, 3 or 4 designed to match SAL in IEC 62443.

The full picture of this in-development ISASecure scheme will then be as indicated in this diagram:

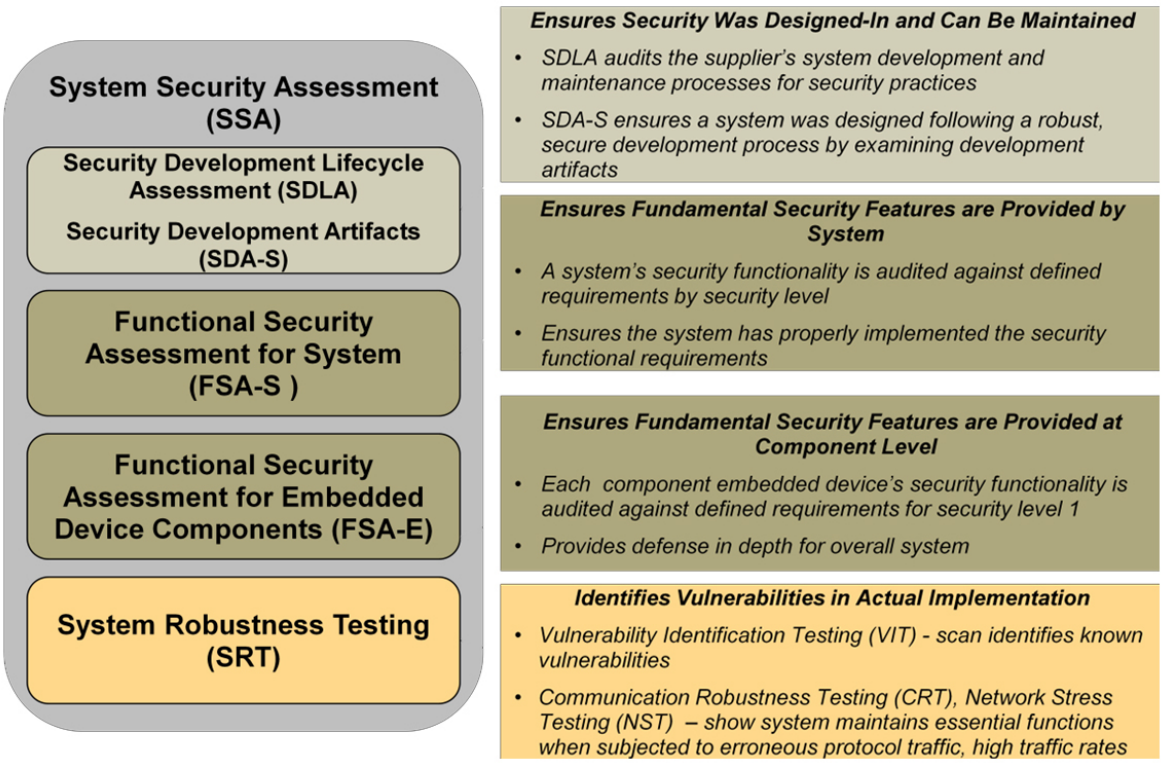



**Figure 12 Development in the ISASecure scheme**

## 4.4 In conclusion: The need for a European IACS components Cyber-security Compliance & Certification Scheme

It was the common opinion of the TG Members that Europe should have and implement its own IACS components Cyber-security Compliance & Certification Scheme:

- ⇨ The idea expressed here was not to create yet another certification standard;
- ⇨ Rather, it was to look for what is common to existing standards and to exploit those commonalities to create a European IACS certification scheme.

Testing and certifying the cyber-security of IACS components/devices seemed to TG members a useful step to take as it would bring a higher level of cyber-confidence to industry buyers and users. However they know that certified components do not entail that sub-systems and entire industrial systems would be cyber-threat free. Engineering cyber-security into those more global levels of IACS architectures requires efforts on the part of integrators and industries themselves, which is why the idea of certifying sub-systems or systems was discarded by our thematic group. The cyber-security of an entire system can hardly be globally certified because it is very much dependent of the environment in which it is embedded, each implementation being different.

Vendors agree that today they cannot afford to release products that would not embed a level of cyber-security sufficient to prevent cyber-attacks, and that this does not generate unbearable extra costs. However such testing and certification activities should be performed according to a widely accepted and practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. In addition, the existence of different domains of industry and of many types of systems should not lead to a variety of T&C ([18]) schemes. And intellectual property over industrial devices' code should not be breached in case of T&C, this being non-negotiable. Should such a scheme fail to provide these characteristics, it would engender costs and difficulties that would immediately undermine its market value.

Besides, the level of cyber-security maturity of IACS stakeholders varies. For instance, industrial operators may not know what to focus on when it comes to making ad hoc decisions or may conversely disperse their efforts by attempting to address every single cyber-security issue. Legal responsibilities ultimately fall onto industrial operators' shoulders in case of industrial accidents, whatever the chain of contracts binding them to integrators and vendors. National cyber-security authorities should foster the adoption of cyber-security dispositions by providing the best possible guidance. Should a testing and certification scheme be proposed, it should accommodate vendors who need to put a foot on the first step of the certification ladder. It should engage them into progressive improvements of their practices towards a capacity to present the market with fully certifiable IACS products.

What this TG recommends is the test and certification of devices, i.e. components found in IACS. Staff certification is out of the scope of this TG. And the adoption of IACS cyber-security T&C will be as quick as solutions/schemes will be available.

Finally, there were two options for proposing the European Commission an IACS cyber-security testing and certification scheme:

1. Promoting one of the existing standards (ISO 15408 or IEC 62443) as the way forward,
   or
2. Studying further the question of how T&C could be achieved.

The market is filled with discussions about which standard should become the reference for market players with regards to cyber-security T&C and it was hard to decide in favour of option 1.

Besides, option 2 was suggesting a research into what a 'European' scheme could look like. This is the way chosen for works carried out in phase 2 of our thematic group. As explained before, the driving principle is *a priori* not to reinvent the wheel and create another standard but to reuse the good principles present in existing standards and to seek a documented bridge and compatibility between a European IACS certification scheme and existing standards.

([18]) In phase 1, TG members were still referring to T&C (Testing & Certification) rather than to C&C (Compliance & Certification) that emerged from work carried out in phase 2.

# 5 Research directions: a proposed EU C&C scheme

This chapter shows how TG members moved from the idea of a cyber-security testing and certification (T&C) scheme towards the proposal of a Compliance & Certification scheme (C&C).

## 5.1 A series of initial questions and points

Gaining a 'reasonable assurance' of the cyber security of IACS products seeming to be a good prospect to TG members, it was agreed that any such T&C scheme should answer the following initial set of requirements and questions:

- A European IACS device Testing & Certification scheme should be voluntary, not legally binding:
  - Undertaken by operators, by vendors or by integrators?
  - Performed through self or third-party assessment?
  - According to what process? By what bodies? Accredited by whom and based on which process/standard?
  - What should be the regulatory/legislative conditions?
  - NB: If the idea of a voluntary scheme appeared as a good idea, in certain Member States, due to national security regulation or legislation, some industrial components or systems would be mandatorily certified for certain markets/customers (e.g. Defence).
- A European IACS device Testing & Certification scheme should be affordable and quick:
  - What should be the pricing? How long should the whole process take?
  - Not quick for the sake of quickness, of course…
- A European IACS device Testing & Certification scheme should be based upon an agreed standard (to be defined):
  - To gain recognition across Europe and beyond;
  - Which standard? Existing or to be elaborated?
  - Which should be the assessment/test areas?
    - Development process;
    - Code inspection;
    - Vulnerabilities;
    - Unit & Integration-level pen tests;
  - Which levels and scoring method (s)?
  - Tool-facilitated? But which tools? Should tools be qualified/certified/accredited?
- A European IACS device Testing & Certification scheme should define the conditions of publication of the certificates;
- A European IACS device Testing & Certification scheme should be engaging vendors progressively into certification, towards a full capacity to present the market with duly certified IACS products.

The question was also what would make market players buy into the scheme. The experience already carried out in the UK, where an online self-assessment service is offered to CI operators who wish to assess their governance of cyber-security and gives them anonymous benchmarking facilities, has shown that it works well as a factor of market emulation. Germany is just about to adopt a similar approach.

## 5.2 Assumptions made for the feasibility study

Three assumptions were made about creating a European IACS device cyber-security T&C scheme:

1. Assumption 1: a common logic exists among existing cyber-security certification standards;
2. Assumption 2: a set of common bricks need to be established to create a European T&C scheme;

3. Assumption 3: a multi-level scheme is needed to engage stakeholders toward C&C.

They are presented below and the following section will present the proposed scheme in details.

### 5.2.1 Assumption 1: a common logic exists among existing cyber-security certification standards

Different standards, different formulations and different methodological approaches…

Where such differences exist between IEC 62443 and ISO 15408 standards, for instance the creation of a European IACS product cyber-security T&C scheme would require that these differences be assessed and hopefully resolved. But why and how could they be resolved?

A most fundamental need of European stakeholders of the IACS domain is to level down the amount of effort and to assure the mutual recognition of certification. National cyber-security authorities and IACS vendors may have already certified some products based on one of these standards and it is hardly conceivable to upset past investments. Besides, certifications based on one standard are not equivalent to certificates based on the other. And at the present stage of these standards' development, it becomes useful to provide points of comparison to industrial operators, vendors, integrators and national cyber-security authorities.

The following diagram presents the elements underlying the first assumption:

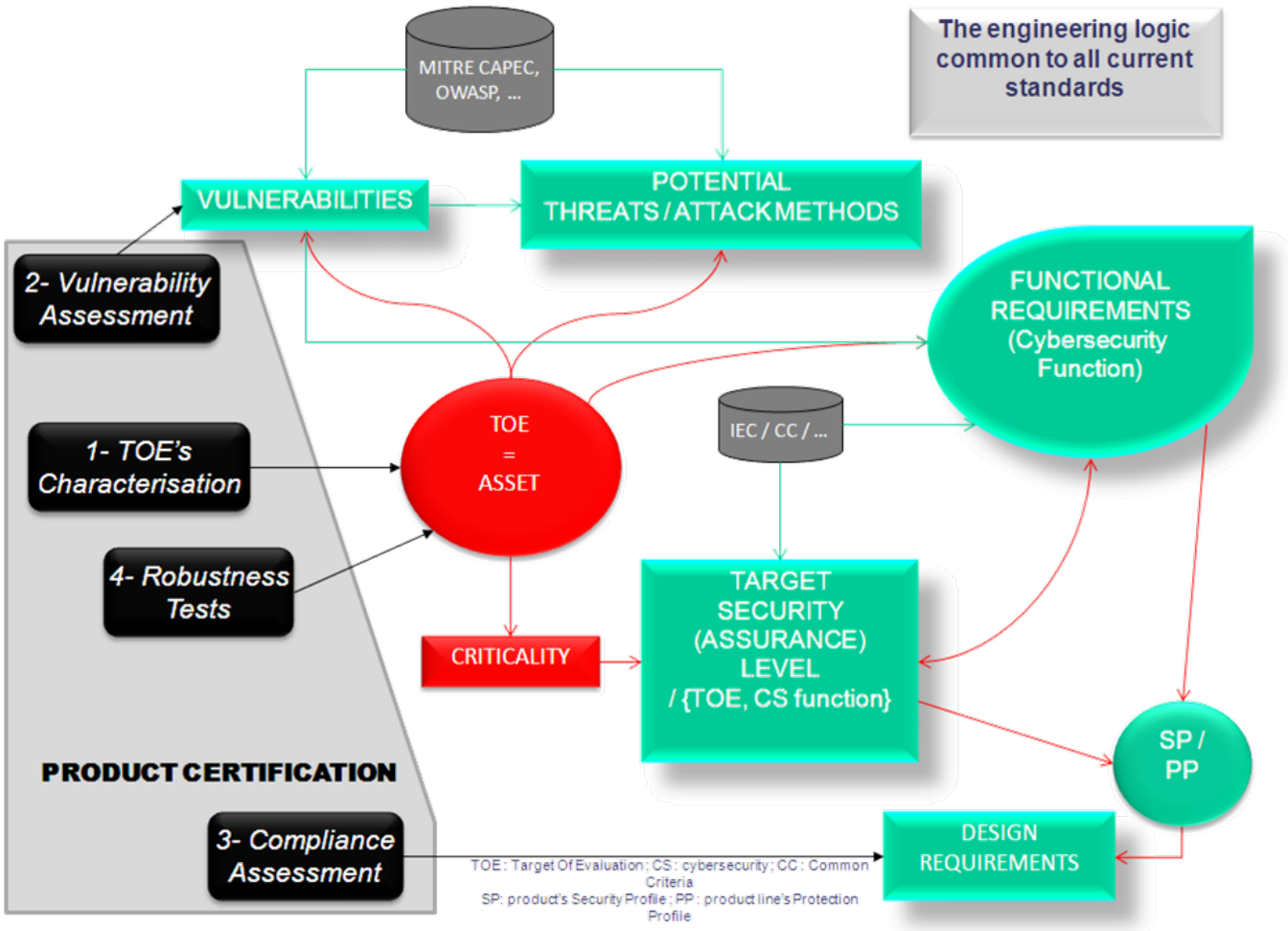



**Figure 13 Assumption 1**

#### 5.2.1.1 There is a common logic of cyber-security engineering in standards

A target IACS asset (an IACS component/device to be assessed) that needs to be cyber-secured may present vulnerabilities that allow potential cyber-attack methods to be used against it. Such vulnerabilities must therefore be reduced. The current state of the art has identified:

- A number of cyber-attack methods, or threats, that exploit known vulnerabilities, and these are well documented in at least two classifications available online, the MITRE's CAPEC and the OWASP.
- A number of cyber-security functional and more technical requirements that, if complied with during the development and operation of the component, allow to make the latter cyber-secure. They are well described in the IEC 62443 and ISO 15408 standards.

##### 5.2.1.1.1 Classifications of cyber vulnerabilities and attack methods

As of June 2014, MITRE's CAPEC (Common Attack Pattern Enumeration and Classification) classification ([19]) identifies 463 cyber-attack patterns. CAPEC is co-sponsored by the US office of Cyber-security and Communications ([20]) at the US Department of Homeland Security ([21]). The website is sponsored and managed by the MITRE Corporation ([22]), a not-for-profit company that operates multiple Federally Funded Research and Development Centres (FFRDCs), to enable stakeholder collaboration. Cyber threats are classified according to three different criteria and described in minute detail:

- Domains of attack ([23]);
- Mechanisms of attack ([24]);
- Attack techniques ([25]).

Domains of Attack are:

- Social Engineering — (403 categories);
- Supply Chain — (437 categories);
- Communications — (512 categories);
- Software — (513 categories);
- Physical Security — (514 categories);
- Hardware — (515 categories).

Mechanisms of Attack are:

- Gather Information — (118 categories);
- Deplete Resources — (119 categories);
- Injection — (152 categories);
- Deceptive Interactions — (156 categories);
- Manipulate Timing and State — (172 categories);
- Abuse of Functionality — (210 categories);
- Probabilistic Techniques — (223 categories);
- Exploitation of Authentication — (225 categories);
- Exploitation of Authorisation — (232 categories);
- Manipulate Data Structures — (255 categories);
- Manipulate Resources — (262 categories);
- Analyze Target — (281 categories);
- Gain Physical Access — (436 categories);
- Malicious Code Execution — (525 categories);
- Alter System Components — (526 categories);
- Manipulate System Users — (527 categories).

Attack techniques are:

- WASC-03 — Integer Overflows;

([19]) http://capec.mitre.org/
([20]) http://www.dhs.gov/office-cyber-security-and-communications/
([21]) http://www.dhs.gov/
([22]) http://www.mitre.org/
([23]) http://capec.mitre.org/data/graphs/3000.html
([24]) http://capec.mitre.org/data/graphs/1000.html
([25]) http://capec.mitre.org/data/definitions/333.html

- WASC-05 — Remote File Inclusion;
- WASC-06 — Format String;
- WASC-07 — Buffer Overflow;
- WASC-08 — Cross-Site Scripting;
- WASC-09 — Cross-Site Request Forgery;
- WASC-10 — Denial of Service;
- WASC-11 — Brute Force;
- WASC-12 — Content Spoofing;
- WASC-18 — Credential/Session Prediction;
- WASC-19 — SQL Injection;
- WASC-23 — XML Injection;
- WASC-24 — HTTP Request Splitting;
- WASC-25 — HTTP Response Splitting;
- WASC-26 — HTTP Request Smuggling;
- WASC-27 — HTTP Response Smuggling;
- WASC-28 — Null Byte Injection;
- WASC-29 — LDAP Injection;
- WASC-30 — Mail Command Injection;
- WASC-31 — OS Commanding;
- WASC-32 — Routing Detour;
- WASC-33 — Path Traversal;
- WASC-34 — Predictable Resource Location;
- WASC-35 — SOAP Array Abuse;
- WASC-36 — SSI Injection;
- WASC-37 — Session Fixation;
- WASC-38 — URL Redirector Abuse;
- WASC-39 — XPath Injection;
- WASC-41 — XML Attribute Blowup;
- WASC-42 — Abuse of Functionality;
- WASC-43 — XML External Entities;
- WASC-44 — XML Entity Expansion;
- WASC-45 — Fingerprinting;
- WASC-46 — XQuery Injection.

The OWASP ([26]) (Open Web Application Security Project) is a worldwide not-for-profit charitable organisation focused on improving the security of software. Their website is an open wiki. The OWASP community offers, among other things:

- A cyber-attack techniques wiki ([27]) somehow similar to CAPEC attack techniques;
- A cyber-security testing guide applicable in development projects ([28]);
- A set of generic attack detection rules that provide a base level of protection for any web application ([29]);
- The OWASP Application Security Verification Standard (ASVS) Project that provides a basis for testing web application technical security controls ([30]);
- Etc.

#### *5.2.1.1.2 Classifications of cyber-security functional requirements*

The IEC 62443 standard identifies the following functional and associated technical requirements:

| Functional Requirements | Associated System Requirements |
|---|---|
| FR 1 — Access control | SR 1.1 — IACS user identification and authentication<br>SR 1.2 — Account management<br>SR 1.3 — Access enforcement<br>SR 1.4 — Identifier management<br>SR 1.5 — Authenticator management |

([26]) https://www.owasp.org/index.php/Main_Page
([27]) https://www.owasp.org/index.php/Category:Attack
([28]) https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf
([29]) https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
([30]) https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

| | |
|---|---|
| | SR 1.6 — Authenticator feedback<br>SR 1.7 — Unsuccessful login attempts<br>SR 1.8 — System use notification<br>SR 1.9 — Previous logon notification<br>SR 1.10 — Session lock<br>SR 1.11 — Remote session termination<br>SR 1.12 — Remote access<br>SR 1.13 — Device identification and authentication |
| FR 2 — Use control | SR 2.1 — Wireless access restrictions<br>SR 2.2 — Use control for portable and mobile devices<br>SR 2.3 — Mobile code<br>SR 2.4 — Concurrent session control<br>SR 2.5 — Auditable events<br>SR 2.6 — Audit storage capacity<br>SR 2.7 — Response to audit processing failures<br>SR 2.8 — Time stamps<br>SR 2.9 — Protection of audit information<br>SR 2.10 — Non-repudiation |
| FR 3 — Data integrity | SR 3.1 — Communication integrity<br>SR 3.2 — Malicious code protection<br>SR 3.3 — Security functionality verification<br>SR 3.4 — Software and information integrity<br>SR 3.5 — E-mail use in the control system<br>SR 3.6 — Information input restrictions<br>SR 3.7 — Information integrity and authenticity<br>SR 3.8 — Error handling<br>SR 3.9 — Session authenticity |
| FR 4 — Data confidentiality | SR 4.1 — Information persistence<br>SR 4.2 — Communication confidentiality<br>SR 4.3 — Cryptographic key establishment and management<br>SR 4.4 — Use of cryptography<br>SR 4.5 — Public key infrastructure certificates |
| FR 5 — Restrict data flow | SR 5.1 — Information flow enforcement<br>SR 5.2 — Application partitioning<br>SR 5.3 — Security function isolation<br>SR 5.4 — Boundary protection |
| FR 6 — Timely response to an event | SR 6.1 — Audit reduction and report generation<br>SR 6.2 — IACS monitoring tools and techniques |
| FR 7 — Resource availability | SR 7.1 — Denial of service protection<br>SR 7.2 — Management of network resources<br>SR 7.3 — IACS backup<br>SR 7.4 — IACS recovery and reconstitution<br>SR 7.5 — Emergency power<br>SR 7.6 — Network and security configuration settings<br>SR 7.7 — Least functionality<br>SR 7.8 — IACS component inventory |

This is to be compared to ISO 15408:2005/Common Criteria — Part 2: Security Functional Components that defines the following security functional requirements in relation to target systems under evaluation:

| Security Classes | Security Functional Components |
|---|---|
| 1 CLASS FAU: SECURITY AUDIT | 1.1 Security audit automatic response (FAU_ARP)<br>1.2 Security audit data generation (FAU_GEN)<br>1.3 Security audit analysis (FAU_SAA)<br>1.4 Security audit review (FAU_SAR)<br>1.5 Security audit event selection (FAU_SEL)<br>1.6 Security audit event storage (FAU_STG) |
| 2 CLASS FCO: COMMUNICATION | 2.1 Non-repudiation of origin (FCO_NRO) |

| | |
|---|---|
| | 2.2 Non-repudiation of receipt (FCO_NRR) |
| 3 CLASS FCS: CRYPTOGRAPHIC SUPPORT | 3.1 Cryptographic key management (FCS_CKM)<br>3.2 Cryptographic operation (FCS_COP) |
| 4 CLASS FDP: USER DATA PROTECTION | 4.1 Access control policy (FDP_ACC)<br>4.2 Access control functions (FDP_ACF)<br>4.3 Data authentication (FDP_DAU)<br>4.4 Export from the TOE (FDP_ETC)<br>4.5 Information flow control policy (FDP_IFC)<br>4.6 Information flow control functions (FDP_IFF)<br>4.7 Import from outside of the TOE (FDP_ITC)<br>4.8 Internal TOE transfer (FDP_ITT)<br>4.9 Residual information protection (FDP_RIP)<br>4.10 Rollback (FDP_ROL)<br>4.11 Stored data integrity (FDP_SDI)<br>4.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT)<br>4.13 Inter-TSF user data integrity transfer protection (FDP_UIT) |
| 5 CLASS FIA: IDENTIFICATION AND AUTHENTICATION | 5.1 Authentication failures (FIA_AFL)<br>5.2 User attribute definition (FIA_ATD)<br>5.3 Specification of secrets (FIA_SOS)<br>5.4 User authentication (FIA_UAU)<br>5.5 User identification (FIA_UID)<br>5.6 User-subject binding (FIA_USB) |
| 6 CLASS FMT: SECURITY MANAGEMENT | 6.1 Management of functions in TSF (FMT_MOF)<br>6.2 Management of security attributes (FMT_MSA)<br>6.3 Management of TSF data (FMT_MTD)<br>6.4 Revocation (FMT_REV)<br>6.5 Security attribute expiration (FMT_SAE)<br>6.6 Specification of Management Functions (FMT_SMF)<br>6.7 Security management roles (FMT_SMR) |
| 7 CLASS FPR: PRIVACY | 7.1 Anonymity (FPR_ANO)<br>7.2 Pseudonymity (FPR_PSE)<br>7.3 Unlinkability (FPR_UNL)<br>7.4 Unobservability (FPR_UNO) |
| 8 CLASS FPT: PROTECTION OF THE TSF | 8.1 Fail secure (FPT_FLS)<br>8.2 Availability of exported TSF data (FPT_ITA)<br>8.3 Confidentiality of exported TSF data (FPT_ITC)<br>8.4 Integrity of exported TSF data (FPT_ITI)<br>8.5 Internal TOE TSF data transfer (FPT_ITT)<br>8.6 TSF physical protection (FPT_PHP)<br>8.7 Trusted recovery (FPT_RCV)<br>8.8 Replay detection (FPT_RPL)<br>8.9 State synchrony protocol (FPT_SSP)<br>8.10 Time stamps (FPT_STM)<br>8.11 Inter-TSF TSF data consistency (FPT_TDC)<br>8.12 Testing of external entities (FPT_TEE)<br>8.13 Internal TOE TSF data replication consistency (FPT_TRC)<br>8.14 TSF self-test (FPT_TST) |
| 9 CLASS FRU: RESOURCE UTILISATION | 9.1 Fault tolerance (FRU_FLT)<br>9.2 Priority of service (FRU_PRS)<br>9.3 Resource allocation (FRU_RSA) |
| 10 CLASS FTA: TOE ACCESS | 10.1 Limitation on scope of selectable attributes (FTA_LSA)<br>10.2 Limitation on multiple concurrent sessions (FTA_MCS)<br>10.3 Session locking and termination (FTA_SSL)<br>10.4 TOE access banners (FTA_TAB)<br>10.5 TOE access history (FTA_TAH)<br>10.6 TOE session establishment (FTA_TSE) |
| 11 CLASS FTP: TRUSTED PATH/CHANNELS | 11.1 Inter-TSF trusted channel (FTP_ITC)<br>11.2 Trusted path (FTP_TRP) |

These methods also define, though differently, security targets for specific devices and protection profiles for generic families of devices, i.e. for product lines. Such profiles determine which types of security requirements must be provided to a device or family of devices to reach a target level of cyber-security.

#### *5.2.1.2 There is a common logic of cyber-security testing and certification*

In the same two standards, cyber-security evaluations rely also on similar concepts:

- The identification/characterisation of the target of evaluation (TOE) ([31]), including its context of operation;
- The assessment of the TOE's vulnerabilities;
- The definition of a target level of cyber-security for the TOE ([32]);
- The assessment of how the TOE responds to the cyber-security requirements that need to be complied with at the target level of cyber-security of the TOE;
- Complementary robustness tests, like penetration tests;
- This may also include the assessment of the development and operating process, this involving an assessment of the product's architecture, its documentation, lifecycle support and maintenance.

The following picture shows some of these potential correspondences between security requirements promoted by the two standards:

([31]) TOE: this terminology is proposed by ISO 15408 / Common Criteria. This reference to Common Criteria does not express a prejudice in favour of this standard.

([32]) In ISO 15408 this corresponds to EALs (Evaluation Assurance Levels).

| IEC 62443 | | ISO 15408 | |
|---|---|---|---|
| **Functional Requirements** | **Associated System Requirements** | **Security Classes** | **Security Functional Components** |
| FR 1 – Access control | SR 1.1 – IACS user identification and authentication | 1 CLASS FAU: SECURITY AUDIT | 1.1 Security audit automatic response (FAU_ARP) |
| | SR 1.2 – Account management | | 1.2 Security audit data generation (FAU_GEN) |
| | SR 1.3 – Access enforcement | | 1.3 Security audit analysis (FAU_SAA) |
| | SR 1.4 – Identifier management | | 1.4 Security audit review (FAU_SAR) |
| | SR 1.5 – Authenticator management | | 1.5 Security audit event selection (FAU_SEL) |
| | SR 1.6 – Authenticator feedback | | 1.6 Security audit event storage (FAU_STG) |
| | SR 1.7 – Unsuccessful login attempts | 2 CLASS FCO: COMMUNICATION | 2.1 Non-repudiation of origin (FCO_NRO) |
| | SR 1.8 – System use notification | | 2.2 Non-repudiation of receipt (FCO_NRR) |
| | SR 1.9 – Previous logon notification | 3 CLASS FCS: CRYPTOGRAPHIC SUPPORT | 3.1 Cryptographic key management (FCS_CKM) |
| | SR 1.10 – Session lock | | 3.2 Cryptographic operation (FCS_COP) |
| | SR 1.11 – Remote session termination | 4 CLASS FDP: USER DATA PROTECTION | 4.1 Access control policy (FDP_ACC) |
| | SR 1.12 – Remote access | | 4.2 Access control functions (FDP_ACF) |
| | SR 1.13 – Device identification and authentication | | 4.3 Data authentication (FDP_DAU) |
| FR 2 – Use control | SR 2.1 – Wireless access restrictions | | 4.4 Export from the TOE (FDP_ETC) |
| | SR 2.2 – Use control for portable and mobile devices | | 4.5 Information flow control policy (FDP_IFC) |
| | SR 2.3 – Mobile code | | 4.6 Information flow control functions (FDP_IFF) |
| | SR 2.4 – Concurrent session control | | 4.7 Import from outside of the TOE (FDP_ITC) |
| | SR 2.5 – Auditable events | | 4.8 Internal TOE transfer (FDP_ITT) |
| | SR 2.6 – Audit storage capacity | | 4.9 Residual information protection (FDP_RIP) |
| | SR 2.7 – Response to audit processing failures | | 4.10 Rollback (FDP_ROL) |
| | SR 2.8 – Time stamps | | 4.11 Stored data integrity (FDP_SDI) |
| | SR 2.9 – Protection of audit information | | 4.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) |
| | SR 2.10 – Non-repudiation | | 4.13 Inter-TSF user data integrity transfer protection (FDP_UIT) |
| FR 3 – Data integrity | SR 3.1 – Communication integrity | 5 CLASS FIA: IDENTIFICATION AND AUTHENTICATION | 5.1 Authentication failures (FIA_AFL) |
| | SR 3.2 – Malicious code protection | | 5.2 User attribute definition (FIA_ATD) |
| | SR 3.3 – Security functionality verification | | 5.3 Specification of secrets (FIA_SOS) |
| | SR 3.4 – Software and information integrity | | 5.4 User authentication (FIA_UAU) |
| | SR 3.5 – Email use in the control system | | 5.5 User identification (FIA_UID) |
| | SR 3.6 – Information input restrictions | | 5.6 User-subject binding (FIA_USB) |
| | SR 3.7 – Information integrity and authenticity | 6 CLASS FMT: SECURITY MANAGEMENT | 6.1 Management of functions in TSF (FMT_MOF) |
| | SR 3.8 – Error handling | | 6.2 Management of security attributes (FMT_MSA) |
| | SR 3.9 – Session authenticity | | 6.3 Management of TSF data (FMT_MTD) |
| FR 4 – Data confidentiality | SR 4.1 – Information persistence | | 6.4 Revocation (FMT_REV) |
| | SR 4.2 – Communication confidentiality | | 6.5 Security attribute expiration (FMT_SAE) |
| | SR 4.3 – Cryptographic key establishment and management | | 6.6 Specification of Management Functions (FMT_SMF) |
| | SR 4.4 – Use of cryptography | | 6.7 Security management roles (FMT_SMR) |
| | SR 4.5 – Public key infrastructure certificates | 7 CLASS FPR: PRIVACY | 7.1 Anonymity (FPR_ANO) |
| FR 5 – Restrict data flow | SR 5.1 – Information flow enforcement | | 7.2 Pseudonymity (FPR_PSE) |
| | SR 5.2 – Application partitioning | | 7.3 Unlinkability (FPR_UNL) |
| | SR 5.3 – Security function isolation | | 7.4 Unobservability (FPR_UNO) |
| | SR 5.4 – Boundary protection | 8 CLASS FPT: PROTECTION OF THE TSF | 8.1 Fail secure (FPT_FLS) |
| FR 6 – Timely response to an event | SR 6.1 – Audit reduction and report generation | | 8.2 Availability of exported TSF data (FPT_ITA) |
| | SR 6.2 – IACS monitoring tools and techniques | | 8.3 Confidentiality of exported TSF data (FPT_ITC) |
| FR 7 – Resource availability | SR 7.1 – Denial of service protection | | 8.4 Integrity of exported TSF data (FPT_ITI) |
| | SR 7.2 – Management of network resources | | 8.5 Internal TOE TSF data transfer (FPT_ITT) |
| | SR 7.3 – IACS backup | | 8.6 TSF physical protection (FPT_PHP) |
| | SR 7.4 – IACS recovery and reconstitution | | 8.7 Trusted recovery (FPT_RCV) |
| | SR 7.5 – Emergency power | | 8.8 Replay detection (FPT_RPL) |
| | SR 7.6 – Network and security configuration settings | | 8.9 State synchrony protocol (FPT_SSP) |
| | SR 7.7 – Least functionality | | 8.10 Time stamps (FPT_STM) |
| | SR 7.8 – IACS component inventory | | 8.11 Inter-TSF TSF data consistency (FPT_TDC) |
| | | | 8.12 Testing of external entities (FPT_TEE) |
| | | | 8.13 Internal TOE TSF data replication consistency (FPT_TRC) |
| | | | 8.14 TSF self-test (FPT_TST) |
| | | 9 CLASS FRU: RESOURCE UTILISATION | 9.1 Fault tolerance (FRU_FLT) |
| | | | 9.2 Priority of service (FRU_PRS) |
| | | | 9.3 Resource allocation (FRU_RSA) |
| | | 10 CLASS FTA: TOE ACCESS | 10.1 Limitation on scope of selectable attributes (FTA_LSA) |
| | | | 10.2 Limitation on multiple concurrent sessions (FTA_MCS) |
| | | | 10.3 Session locking and termination (FTA_SSL) |
| | | | 10.4 TOE access banners (FTA_TAB) |
| | | | 10.5 TOE access history (FTA_TAH) |
| | | | 10.6 TOE session establishment (FTA_TSE) |
| | | 11 CLASS FTP: TRUSTED PATH/CHANNELS | 11.1 Inter-TSF trusted channel (FTP_ITC) |
| | | | 11.2 Trusted path (FTP_TRP) |

**Figure 14 Potential correspondences between security requirements promoted by standards**

### 5.2.2 Assumption 2: a set of common bricks must be established to create a European T&C scheme

In order to bring all parties to an agreement on a European IACS cyber-security testing and certification scheme, the second assumption we made was that the industrial community should agree on:

- A common classification of vulnerabilities and attack methods and techniques;
- A common classification of security requirements;
- A common process for testing & certification.

This is summarised in the following diagram:

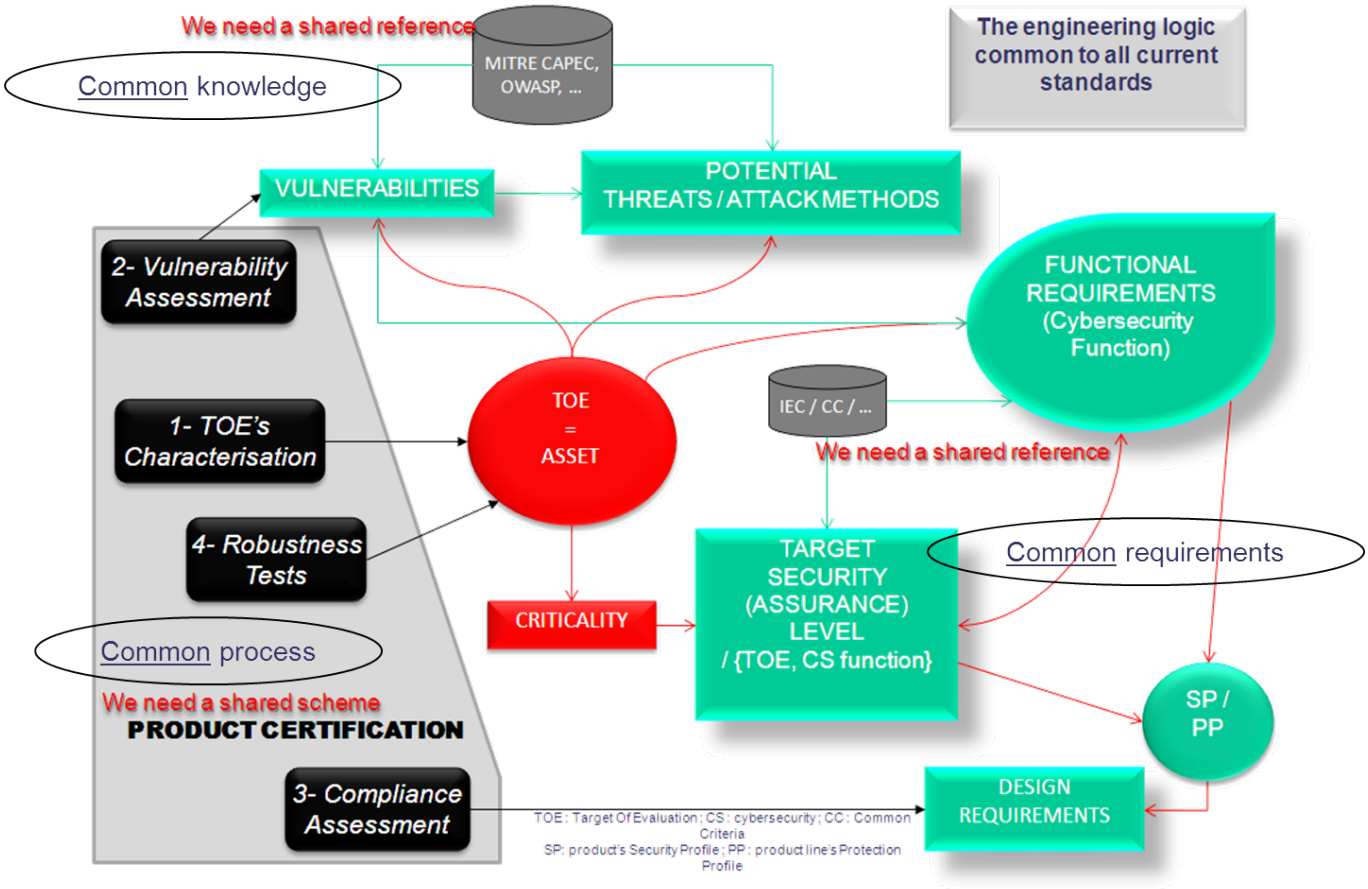



**Figure 15 Assumption 2**

### 5.2.3 Assumption 3: a multi-level scheme is needed to engage stakeholders towards C&C

Our third assumption was derived from the discussions held during the thematic group's meetings. It is the idea that as vendors, integrators and operators altogether have not necessarily reached full maturity with regard to cyber-security, in particular when it comes to certification, it is mandatory to reflect on how to engage them into a virtuous process of improvement in those areas.

Combined with ENISA's findings recalled earlier about the fact that experts thought a mandatory certification scheme was not appropriate, we assumed that if vendors of IACS products/components could in the first place assess their compliance with a set of standard cyber-security requirements that all devices should satisfy, and if such an assessment was in easy reach then they could adhere to the scheme and take their first step towards proper certification.

Besides, the central question in a testing and certification scheme is one of trust:

- A basic self-assessment for instance only tells clients that the vendor has checked the compliance of a product with a shared set of requirements;
- When the same assessment is performed by an independent, accredited third party, clients are certain of the rigour of the assessment process and of the objectivity of the evaluation of the product;
- If, beyond only a formal assessment, 'on paper', a trusted third party tests the cyber-robustness of the product to check if it resists a set of commonly agreed tests, like penetration tests;
- And beyond, assessing the development, operation and maintenance processes associated with the evaluated IACS product gives clients even greater confidence in its cyber-security.

Besides, existing cyber-security certification standards associate requirements to target levels of cyber-security. ISO 15408 standard promotes two approaches to the specification of cyber-security requirements:

- Protection Profiles (PP): describes a type of targets of evaluation (TOE), e.g. 'firewalls' in general;
- Security Target (ST): describes a given TOE, e.g. the MinuteGap v18.5 firewall says ISO 15408:2005 (p. 40).

ANSSI's First level security Certification (CSPN) ([33]) makes certification start from a security target defined in terms of 'the use for which the product was designed and a description of who is meant to use it and in what context; the technical environment in which the product runs (computer model, operating system, etc.); the sensitive assets that the product must protect; the threats against which the product offers protection; the security features implemented by the product to counter the identified threats. These features will be the subject of the evaluation'.

TG members retained the idea of a generic product profile defined in terms of:

- A type of IACS products;
- A standard configuration of the product;
- An operating and access context and protocol;
- A target level of cyber-security requested by a class of buyers;
- A capacity to withstand attacks by adversaries equipped with a certain power of attack.

## 5.3 In conclusion: a four-level Compliance & Certification scheme

Four levels of compliance assessment and certification were defined out of these assumptions:

1. Level 1: self- declaration of compliance;
2. Level 2: third-party compliance assessment;
3. Level 3: third-party product certification;
4. Level 4: third-party full certification.

The following diagram summarises these four levels:


**Figure 16 Four levels of compliance assessment and certification**

This process of progressive improvement of their practices would help vendors to enhance their current quality assurance practices into a proper practice of cyber-security engineering and certification.

([33]) http://www.ssi.gouv.fr/en/certification/first-level-security-certification-cspn/

## 5.4 Detailed description of the proposed C&C scheme

Each level can be described according to the following criteria:

| Elements of the C&C process | Description |
|---|---|
| Product characterisation | The scheme's level includes the definition of the product's cyber-security profile |
| Threats & Vulnerabilities assessment | The scheme's level includes the assessment of the product's vulnerabilities |
| Development process | The scheme's level includes the assessment of the product's development ([34]) process |
| Cyber-security requirements | The scheme's level includes the assessment of the product's cyber-security requirements |
| Cyber-robustness tests | The scheme's level includes the performance of tests aiming at proving that the product effectively delivers the level of cyber-security specified in its profile |
| **Characteristics** | **Description** |
| GENERAL PRINCIPLE | What the scheme's level is intended to deliver |
| DEFINITION | What the scheme's level is |
| POTENTIAL COST | What the scheme's level may cost to a vendor (expressed in broad terms) |
| CONSTRAINTS/LIMITS | What the scheme's level requires and the difficulties potentially associated with it |
| CERTIFICATE VALIDITY | What the scheme's level certificate is valid for |
| MUTUAL RECOGNITION | The conditions of mutual recognition of the scheme's level certificate |
| USEFULNESS | What the scheme's level provides to industry users |
| NORM OF REFERENCE | What standard the scheme's level relies upon |
| PROCESS | Who does the assessment |
| PUBLICATION OF CERTIFICATE | The regime of publication/publicity of the certification |
| LEGAL REGIME | The legal implications of the delivery of the certificate |
| RISKS | The risks associated with the elaboration of the scheme's level |
| OPPORTUNITIES | The opportunities associated with the elaboration of the scheme's level |

The following sections provide the arguments agreed upon by TG members. These arguments must be interpreted as basic, initial elements of description of each level and orientations that must be further studied in the next phase of the ERNCIP programme.

### 5.4.1 Level 1: self-declaration of compliance

| IACS component C&C Scheme (Research directions) | LEVEL 1: SELF-DECLARATION OF COMPLIANCE (based on a generic product profile) |
|---|---|
| Product characterisation | **YES** |
| Threats & Vulnerabilities assessment | |
| Development process | |
| Cyber-security requirements | **YES** |
| Cyber robustness tests | |
| GENERAL PRINCIPLE | Meeting all cyber-security requirements for a given Security Profile |
| DEFINITION | A PRODUCT'S SECURITY PROFILE assessed on paper based on a generic product type's protection profile |
| POTENTIAL COST | Inexpensive (IACS cyber-security assessment management system) |
| CONSTRAINTS/LIMITS | Redo the assessment for each version to assess a product generically (the standard must allow this then)<br>Products have a very long lifecycle => certificates' maintenance to be studied |
| CERTIFICATE VALIDITY | A product version or line (and its upgrades if the standard permits) |
| MUTUAL RECOGNITION | Based on a shared European IACS Cyber-security Certification Standard |
| USEFULNESS | To know which security level the product is engineered for |
| NORM OF REFERENCE | European IACS Cyber-security Certification Standard |
| PROCESS | Self-assessment based on a specified process |
| PUBLICATION | COMPLIANCE DECLARATION could be posted on a European cyber-security IACS Certification Register<br>Visual label showing the level (1 to 4) of the product |

([34]) By development we mean the engineering, production, installation, operation and maintenance processes.

| | |
|---|---|
| LEGAL REGIME | Declarative under professional IACS associations' monitoring |
| RISKS | No short-term agreement on a standard leading to no European mutual recognition<br>Professional IACS associations do not endorse the scheme |
| OPPORTUNITIES | Standards convergence reveals feasibility: cyber-security requirements and measures are fairly homogenously documented across them (ISA/CC ([35])/NIST…) |

### 5.4.2 Level 2: third-party compliance assessment

| IACS component C&C Scheme (Research directions) | LEVEL 2: THIRD-PARTY COMPLIANCE ASSESSMENT (based on a generic product profile) |
|---|---|
| Product characterisation | **YES** |
| Threats & Vulnerabilities assessment | |
| Development process | |
| Cyber-security requirements | **YES** |
| Cyber robustness tests | |
| GENERAL PRINCIPLE | Assurance of meeting all cyber-security requirements for a given Security Profile |
| DEFINITION | A product's security profile assessed on paper, based on a generic product type's protection profile |
| POTENTIAL COST | Low cost (IACS cyber-security assessment management system + audit cost) |
| CONSTRAINTS/LIMITS | Redo assessment for each version to assess a product generically (the standard must allow this then)<br>Products have a very long lifecycle => certificates' maintenance to be studied |
| CERTIFICATE VALIDITY | A product version or line (and its upgrades if standard permits) |
| MUTUAL RECOGNITION | Based on a shared European IACS Cyber-security Certification Standard |
| USEFULNESS | To know which security level the product is engineered for |
| NORM OF REFERENCE | European IACS Cyber-security Certification Standard |
| PROCESS | Assessment by an accredited independent third-party |
| PUBLICATION | Compliance declaration could be posted on a European Cyber-security IACS Certification Register<br>Visual label showing the level (1 to 4) of the product |
| LEGAL REGIME | Declarative under professional IACS associations' monitoring |
| RISKS | No short-term agreement on a standard leading to no European mutual recognition<br>Professional IACS associations do not endorse the scheme<br>Other European activities competing with JRC's projects |
| OPPORTUNITIES | Standards convergence reveals feasibility: cyber-security requirements and measures are fairly homogenously documented across them (ISA/CC/NIST…) |

### 5.4.3 Level 3: third-party product certification

| IACS component C&C Scheme (Research directions) | LEVEL 3: THIRD-PARTY PRODUCT CERTIFICATION (Same as L2 + Robustness tests) |
|---|---|
| Product characterisation | **YES** |
| Threats & Vulnerabilities assessment | **YES** |
| Development process | |
| Cyber-security requirements | **YES** |
| Cyber robustness tests | **YES** |
| GENERAL PRINCIPLE | Verification of TOE's cyber-security robustness |
| DEFINITION | A product's security profile and robustness tests<br>Certifies the product out of the box |
| POTENTIAL COST | Reasonably expensive |

([35]) Common Criteria

| | |
|---|---|
| CONSTRAINTS/LIMITS | Products have a very long lifecycle => certificates' maintenance to be studied<br>An automaton device is not just a box but often a system => difficulty + cost |
| CERTIFICATE VALIDITY | A product version (and its upgrades if the standard permits) |
| MUTUAL RECOGNITION | Based on a shared European IACS Cyber-security Certification Standard and a Robustness Testing standard (TBD) |
| USEFULNESS | To know which security level the product effectively reaches |
| NORM OF REFERENCE | European IACS Cyber-security Certification Standard |
| PROCESS | Third-party accredited by national cyber-security authority |
| PUBLICATION | Certificate could be posted on a European Cyber-security IACS Certification Register + National agency<br>Visual label showing the level (1 to 4) of the product |
| LEGAL REGIME | LEGAL RECOGNITION (possible because of certification + a user's acceptable means of compliance) |
| RISKS | No short-term agreement on L2 certificates European mutual recognition<br>No short-term development of L3 standards and processes |
| OPPORTUNITIES | Standards convergence reveals feasibility: cyber-security requirements and measures are fairly homogenously documented across them (ISA/CC/NIST…) |

### 5.4.4 Level 4: third-party full certification

| **IACS component C&C Scheme (Research directions)** | **LEVEL 4: THIRD-PARTY FULL CERTIFICATION (Same as L3 + Process certification)** |
|---|---|
| Product characterisation | **YES** |
| Threats & Vulnerabilities assessment | **YES** |
| Development process | **YES** |
| Cyber-security requirements | **YES** |
| Cyber robustness tests | **YES** |
| GENERAL PRINCIPLE | Verification of TOE's cyber-security robustness plus evidence of TOE's cyber-security development good practices |
| DEFINITION | Security profile assessment + robustness tests + process certification certifies the product and the process |
| POTENTIAL COST | More expensive |
| CONSTRAINTS/LIMITS | Products have a very long lifecycle => certificate's maintenance is to be studied<br>Also: an automaton device is not just a box but often a system => difficulty + cost |
| CERTIFICATE VALIDITY | A product version (and its upgrades if the standard permits) |
| MUTUAL RECOGNITION | Same as L3 + a Process certification standard |
| USEFULNESS | To know which security level the product effectively reaches in a context for which product and process certification is mandatory |
| NORM OF REFERENCE | Common Criteria? |
| PROCESS | Third-party accredited by national cyber-security authority |
| PUBLICATION | CERTIFICATE on the European Cyber-security IACS Certification Register + National agency<br>Visual label showing the level (1 to 4) of the product |
| LEGAL REGIME | LEGAL RECOGNITION (possible because of product certification + a user's acceptable means of compliance) |
| RISKS | CC too complex and impossibility to define a lighter version of CC<br>Suppliers not ready to disclose their processes |
| OPPORTUNITIES | Demands from protected sectors (defence, etc.)?…<br>Standards convergence reveals feasibility: cyber-security requirements and measures are fairly homogenously documented across them (ISA/CC/NIST…) |

## 5.5 In conclusion

The findings of the TG's phase 2 work are that a four-level European IACS components Cyber-security Compliance & Certification Scheme and its broad characteristics should be developed.

These findings constitute an initial proposal with regards to IACS' cyber-security.

This proposal now requires further work in order to be shared, further defined, developed and fostered across Europe.

The next chapter presents the corresponding research and action plan and its rationale and concepts.

# 6 A research and action plan for 2015-20

## 6.1 Concepts and rationale of the proposed C&C scheme

The proposed European IACS components Cyber-security Compliance & Certification Scheme relies upon a number of concepts and assumptions. They also inform the rationale of the research and action plan proposed for the 2015-20 period:

1. The proposed plan mixes research projects and practical projects and those might be conducted either by the EC, or by other European Institutions, including the CEN and other standardisation bodies. The plan does not make any recommendation about who should do what.
2. The first step to take is to enquire about IACS stakeholders' opinions and, based on the results of this enquiry, to define in detail, organise and schedule further projects suggested in the plan.
3. The creation of a European IACS product register should be further specified and developed.
4. Common cyber-security requirements would be needed for the assessment of IACS products if no agreement was reached about the choice of a standard shared among EU MS and stakeholders. These should be created out of existing standards such as IEC 62443, ISO 15408, etc. this project should cover a common classification of cyber-security vulnerabilities and attack methods (which could be inspired by MITRE CAPEC and OWASP classifications), cyber-security functional and technical requirements, target levels of cyber-security and their contexts of applications, cyber robustness tests, development process characteristics and good practices.
5. IACS product standard cyber-security profiles are needed to further specify target levels of cyber-security and requirements. The French ANSSI's protection profiles ([36]) and similar initiatives should be analysed as a possible reference for this project, as well as the concepts of ISO 15408 protection profiles.
6. A common European process for IACS cyber-security compliance assessment and certification should be defined. IEC 62443/ISASecure and ISO 15408/Common Criteria guidelines should be a primary source of inspiration.
7. A transition and implementation plan is required. Implementation refers to the actions to be taken on a European scale in order to make the C&C scheme become a reality. Transition refers to the assistance to be provided to vendors, integrators and industry operators as to how to implement the C&C scheme and to prepare for it. This includes preparing the launch of the scheme.
8. Once the prior transition and implementation plan established the official launch of the scheme should be done.

The following section summarises the research and action plan proposed for 2015-20.

## 6.2 A research and action plan for 2015-20

The proposed plan is made of seven projects:

1. Stakeholders consultation and project planning
2. Product Register development
3. Cyber-security Common Requirements project
4. Standard Security Profiles project
5. Compliance & Certification Process project
6. Transition & Implementation Plan
7. Launch of the C&C Scheme.

([36]) http://www.ssi.gouv.fr/en/products/protection-profiles/

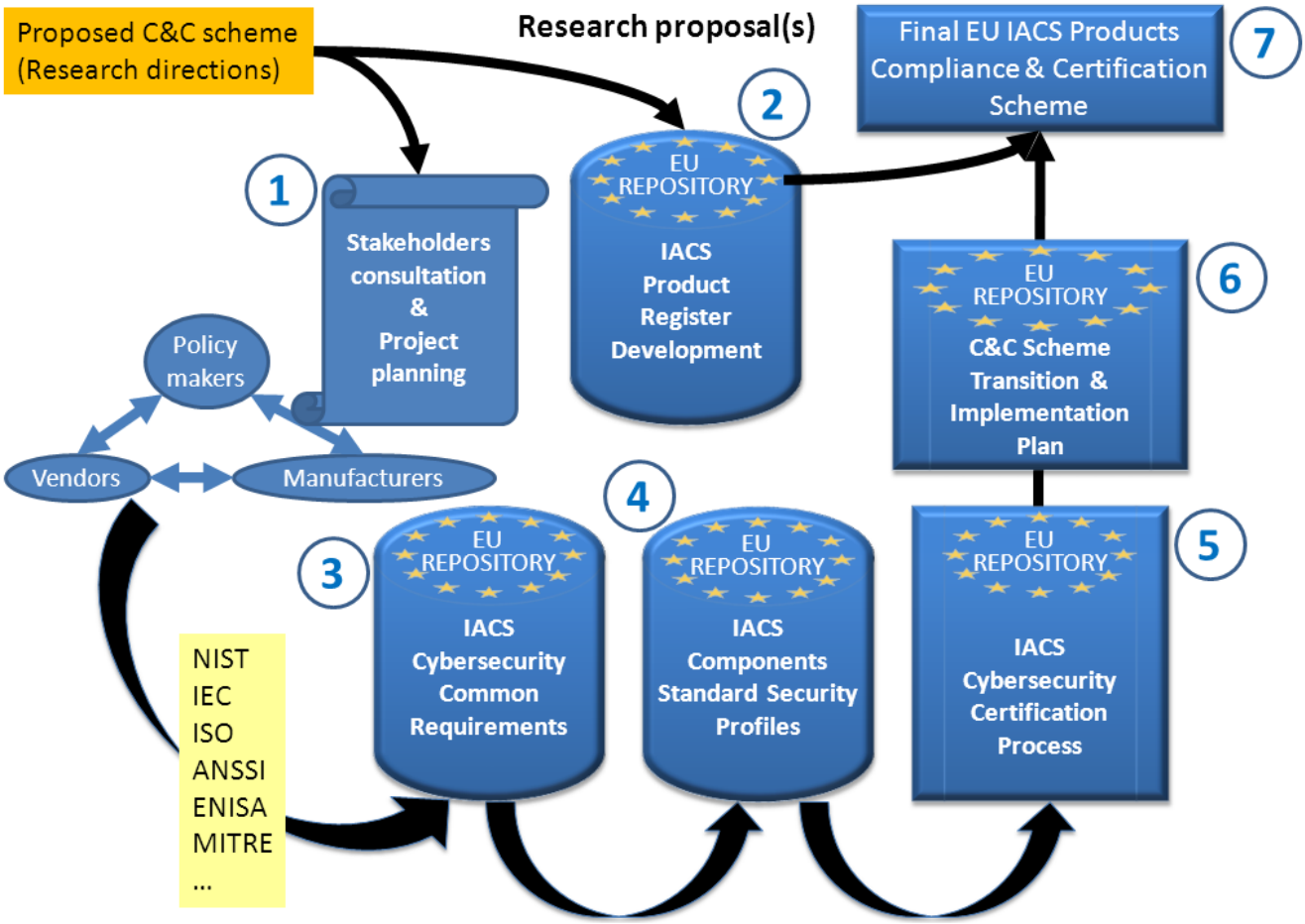



**Figure 17 The research and action plan for 2015-20**

**<u>Project No 1 is a key priority</u>** and will confirm and frame the rest of the plan.

Projects No 3, No 4 and No 5 could be conducted in parallel. In order to take advantage of a window of opportunity for Europe to develop its own scheme, they should be carried out by beginning or mid-2016. Today, IACS suppliers are ready to follow such a European scheme as existing standards are not yet widely adopted. Some participants wish that projects Nos 3 to 6 will be finished mid-2016. Project No 2 could be conducted either in parallel with projects Nos 3 to 5 or after. Project No 6 can be performed only after actions No 2 and No 5. This schedule, however, will be refined in project No 1 to take account of all possible goals, options and constraints.

Vendors, policy-makers and manufacturers (industry operators) must be involved in these projects.

The following GANTT planning summarises the schedule initially proposed for the seven projects:

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1- Stakeholders consultation & project planning | | | | | | | | | | | |
| 2- Product Register development | | | | | | | | | | | |
| 3- CS Common Requirements project | | | | | | | | | | | |
| 4- Standard Security Profiles project | | | | | | | | | | | |
| 5- Compliance & Certification Process project | | | | | | | | | | | |
| 6- Transition & Implementation Plan | | | | | | | | | | | |
| 7- Launch of the C&C Scheme | | | | | | | | | | | |

**Figure 18 Schedule of the research and action plan for 2015-20**

## 6.3 Initial specification of the projects

### 6.3.1 Project No 1: Stakeholders consultation & project planning

Goal: To verify the stakeholders' interest for the European IACS components Cyber-security Compliance & Certification Scheme proposal, their constraints and priorities, and to detail the plan for the subsequent six projects.

NB: This is a short project that could be established as an ERNCIP Thematic Group to be started soon and run in early 2015 in order to allow projects 2 to 5 to fit into their window of opportunity.

Method: This project should *a priori* include the following steps:

1. The identification of a wider group of IACS, cyber-security and cyber-security certification expert bodies, companies and people in order to provide future 2015-20 projects with possibilities to collect, analyse and discuss IACS cyber-security C&C related data and findings;
2. An enquiry about the TG's proposals for the European IACS components Cyber-security Compliance & Certification Scheme in order to validate and comment on them more widely than among the initial circle of our TG members;
3. A possible amendment of our initial proposals should the enquiry bring useful recommendations;
4. The detailed specification and organisation of the next six projects, along with their intended scheduling and refined budget estimate;
5. The practical launch of these following six projects through the organisation of one or several thematic groups, or call for proposals, or partnerships with institutions, companies or experts, including an ERNCIP conference.

### 6.3.2 Project No 2: Product Register development

Goal: To provide users with an EC-managed database of C&C evaluated IACS products.

Method: This project should *a priori* include the following steps:

1. General design;
2. Specification and design;
3. Development and testing;
4. Implementation and trials under EC's control;
5. Review;
6. Finalisation by the EC.

### 6.3.3 Project No 3: Cyber-security Common Requirements

Goal: To extract from existing standards common good practices and requirements and to organise them into a common classification covering an agreed set of domains of C&C: the assessment of cyber-security engineering practices, vulnerabilities assessment, development process assessment and cyber robustness testing, etc.

Method: This project should *a priori* include the following steps:

1. Definition of the project's scope, goals and orientations: this step should define what domains of good practices and requirements shall be included (assessment of cyber-security engineering practices, vulnerabilities assessment, development process assessment and cyber robustness testing, etc.);
2. Review of up to three cyber-security certification standards: these should include IEC 62443/ISASecure, ISO 15408/Common Criteria and possibly a NIST or equivalent reference;

3. Comparison of cyber-security certification standards: it will aim at establishing which good practices and requirements are common to standards of reference as well as gaps and explanation of gaps;
4. Definition of a list of common cyber-security requirements: in each selected domain, Common cyber-security Good Practices and Requirements will include the best ones found in standards of reference and will sort them according to a Common Classification;
5. Discussion and validation of cyber-security requirements.

### 6.3.4 Project No 4: Generic IACS Cyber-security Profiles

Goal: To define Generic IACS Cyber-security Profiles including classes of IACS products and target levels of cyber-security, operating and security environments, etc.

Method: This project should *a priori* include the following steps:

1. Definition of the project's scope, goals and orientations: this step should include the definition of the notion of Protection Profile and how they are intended to be used in the C&C scheme;
2. Review of existing notions of generic Protection Profiles (PP) and specific Security Targets (TS) in existing standards, guidelines and good practices: this should include the standards of reference from Project No 2 as well as the guidelines provided by MS national cyber-security authorities;
3. Proposition of a common definition of Generic IACS Cyber-security Profiles (GICP): this should include at least such elements as a conceptual definition articulated with complementary concepts, a description of contents, a context and method of application, the particulars of an application to at least the five types of IACS products identified in the IACS case studies TG;
4. Discussion of proposed GICPs: this should involve stakeholders (as defined in Project No 1);
5. Amendment of the propositions, taking remarks into account;
6. Validation of GICPs with TG members.

### 6.3.5 Project No 5: Compliance & Certification Process

Goal: To define a common process for each of the four levels of the proposed European IACS components Cyber-security Compliance & Certification Scheme.

Method: This project should *a priori* include the following steps:

1. Definition of the project's scope, goals and orientations: the scope should include the definition of the target of evaluation, the assessment of cyber-security engineering practices, vulnerabilities assessment, development process assessment and cyber robustness testing domains;
2. Definition of each C&C level's process, including the who, what, why, how and when criteria for the framing and preparation stage, the data collection and verification stage, the data analysis stage and certificate delivery stage, as well as for certificates' maintenance, certificate renewal activities, etc.;
3. Discussion and validation of C&C processes;
4. Amendments of processes.

### 6.3.6 Project No 6: Transition & Implementation Plan

Goal: To define how the European Commission, and first of all maybe the DG JRC, and stakeholders (in particular vendors, but also integrators and users) will implement the proposed European IACS components Cyber-security Compliance & Certification Scheme and what kind of support will be required to that end.

Method: This project should *a priori* include the following steps:

1. Definition of the scope, goals and structuring elements of the C&C scheme's implementation plan;

2. Gap analysis between stakeholders' current practices and those required for the implementation of the C&C scheme: this step should include building on the development of good practices elaborated in project No 3;
3. Definition of a baseline transition plan for vendors, integrators and users to enhance their practices: this plan should be founded upon the gaps previously identified;
4. Discussion and validation of the transition plan with stakeholders, possibly through an ERNCIP conference: these discussions may be followed by amendments of the original plan;
5. Definition of a European C&C implementation plan: this plan should include legislative and regulations aspects if needed ([37]), standardisation if still required ([38]), awareness raising, financial incentives planning for instance, etc.;
6. Presentation and negotiation of the implementation plan with European Institutions.

### 6.3.7 Project No 7: Launch of the C&C Scheme

Goal: To plan how to promote the European IACS components Cyber-security Compliance & Certification Scheme, to run, support and assess the plan.
Method: This project should *a priori* include the following steps:

1. C&C fostering activities undertaken by the European Commission/DG JRC: this may take the form of an annual ERNCIP conference during the 2020-25 period, publications, IACS products' Cyber-security C&C awareness weeks or challenges during the same period of time, etc.;
2. Monitoring of implementation activities undertaken by European Institutions and stakeholders: this may involve indicators, surveys, working in partnership with ENISA or other European or professional Institutions, etc.;
3. Reporting activities: activities internal to the JRC and the European Commission.

([37]) It may be the case that law/regulations enforcement may have to be envisaged at this point, for instance.
([38]) It would be best to plan and foster standardisation activities during projects 2 to 5 as far as feasible.

# 7 In conclusion

This thematic group has performed a research project on behalf of the DG JRC. It has confirmed the interest of the IACS market's stakeholders for the certification of IACS components/products. It has left aside the certification of IACS sub-systems/systems because this is a far too complex endeavour, not within the remit of IACS vendors in their capacity of suppliers of the devices. It has also ignored the issue of competence certification.

As for the question of the feasibility of an IACS components certification scheme, assuming:

1. that in existing cyber-security certification standards and guidelines (IEC 62443/ISASecure, and ISO 15408/Common Criteria) there are a number of common elements despite apparent major differences, and
2. that the C&C scheme should engage IACS vendors progressively towards delivering certified products.

The TG proposes a four-level European IACS components Cyber-security Compliance & Certification Scheme (C&C):

- Level 1: self- declaration of compliance;
- Level 2: third-party compliance assessment;
- Level 3: third-party product certification;
- Level 4: third-party full certification.

To implement this framework, the TG proposes a plan of research and action for 2015-20:

| |
|---|
| Project No 1: Stakeholders consultation and project planning |
| Project No 2: Product Register development |
| Project No 3: Cyber-security Common Requirements |
| Project No 4: Standard Security Profiles |
| Project No 5: Compliance & Certification Process |
| Project No 6: Transition & Implementation Plan |
| Project No 7: Launch of the C&C Scheme |

An initial schedule and content has been drafted to help planning tasks with two particular recommendations:

1) Project No 1 is a key priority and will frame the rest of the plan. This is a short project that could be established as an ERNCIP Thematic Group to be started soon and run in early 2015.

2) Projects No 3, No 4, No 5 and No 6 should be carried out as early as feasible, some TG members say by mid-2016, to take advantage of a window of opportunity for Europe to make decisions for itself.

Now, it pertains to decision-makers and to IACS stakeholders, including European Institutions and ENISA, to consider the TG's propositions, and to confirm the next steps.

This TG has demonstrated that a limited number of experts representative of the different families of stakeholders were able to agree on a proposal and to reach what looks like a hands-on scheme.

We want to thank all those who took part in our TG meetings and work.

Finally, we want to thank DG JRC for their constant support and the high-quality discussions held with them.

# 8 Annexes

## 8.1 Annex 1: Phase 1 questionnaire

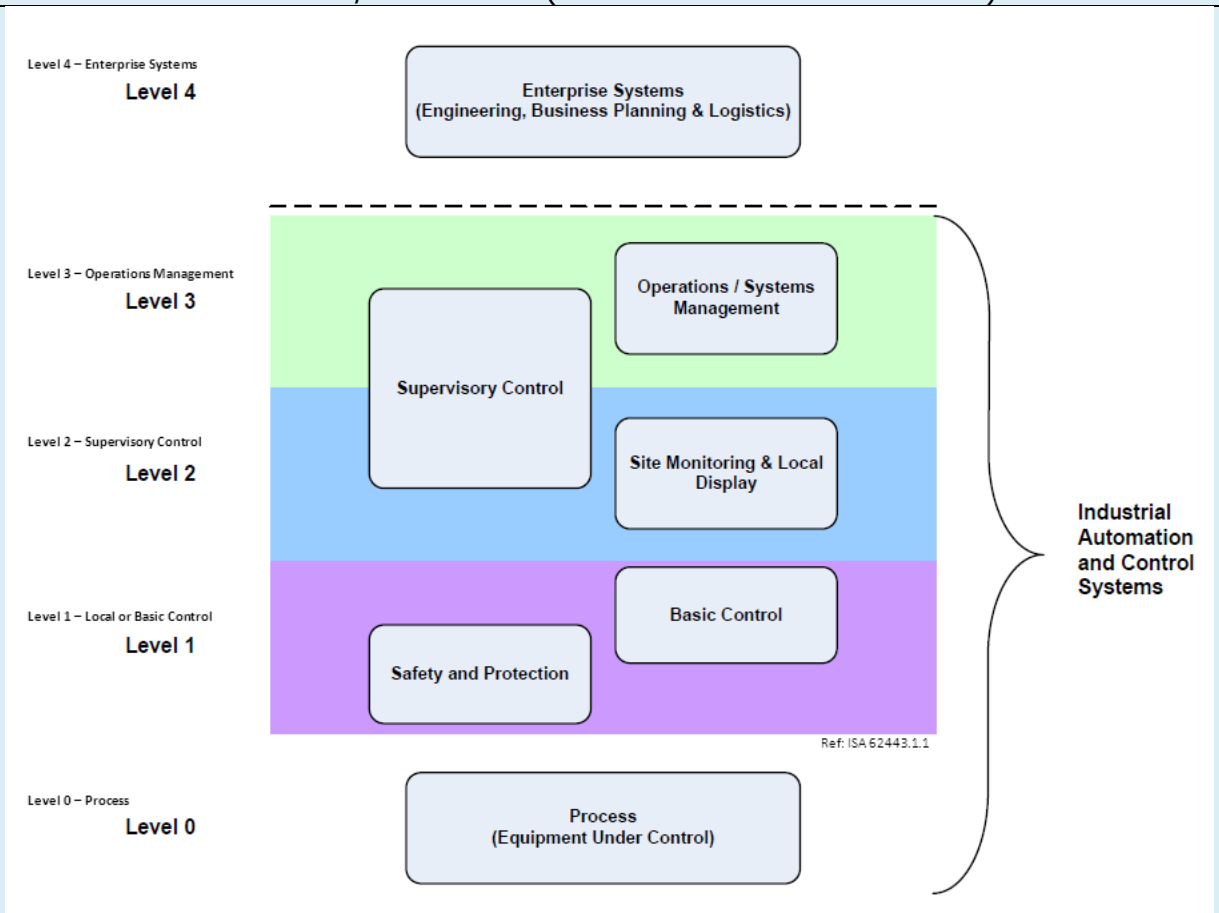
Analysis method for the
Case studies for the Cyber Security of Industrial Automation & Control Systems
Thematic Group

NB: Fill-in or tick boxes, and follow instructions; blue shaded rows are not to be filled in. Grey are optional.

| |
|---|
| YOUR ORGANISATION'S NAME: |
| YOUR ORGANISATION'S ACTIVITY: |
| YOUR NAME: ☐ Do not disclose my name |
| YOUR RESPONSIBILITY/JOB TITLE: |
| VERSION OF THIS DOCUMENT: |
| DATE OF THE DOCUMENT: |
| TRAFFIC LIGHT PROTOCOL LEVEL (Double click the tick box corresponding to the level of confidentiality of this study you desire): |
| ☐ RED — personal for named recipients only<br>In the context of a meeting, for example, RED information is limited to those Representatives present at the meeting. In most circumstances, RED information will be passed orally or in person. Representatives must not disseminate the information outside of the meeting. RED information may be discussed during a meeting but only when all Representatives present have signed up to this Membership Agreement. Other external participants, such as visiting speakers, who are not Members of the TG, will be required to leave before such information is disclosed and discussed. |
| ☐ AMBER — limited distribution<br>The recipient may share AMBER information with others within their organisation (whether direct employees, consultants, contractors or outsource-staff working in the organisation), but only on a strict 'need-to-know' basis. The originator may specify the intended limits of that sharing. |
| ☐ GREEN — community wide<br>Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community. |
| ☐ WHITE — unlimited<br>Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any Member may publish the information, subject to copyright acknowledgement of the source. |
| COMMENTS ON CONFIDENTIALITY IF NEEDED: |

THE CASE YOU STUDY IN THIS DOCUMENT

| SELECT THE CASE YOU ARE STUDYING IN THIS QUESTIONNAIRE (Double click & **select 1 only**): |
|---|
| ☐ A SCADA system that supervises entire industrial systems<br>☐ Field process automation and control equipment<br>☐ An engineering/programming workstation that staff connect to<br>☐ A database used for process control (if corrupted may create safety issues, e.g. in luggage handling)<br>☐ A telecommunication link (for instance for remote equipment maintenance)<br>☐ Other, like a link between IACS and IS, etc. (specify): |
| NAME/BRAND OF THE COMPONENT/SUB-SYSTEM CORRESPONDING TO THE CASE: |
| DESCRIPTION AND FUNCTION OF THE COMPONENT/SUB-SYSTEM: |
| LOCATION OF THE COMPONENT/SUB-SYSTEM (Ref. ISA 62443 IACS architecture): |




| PLEASE PROVIDE DETAILS OF LOCATION OF THE COMPONENT IN THIS ARCHITECTURE: |
|---|

| CAN YOU DESCRIBE THE TECHNOLOGY OF THIS COMPONENT/SUB-SYSTEM? |
|---|
| WHERE IN HIS LIFECYCLE IS THIS COMPONENT/SUB-SYSTEM? (Double click & select 1 only; you may add comments after the selected option): |
| ☐ ACQUISITION? |
| ☐ DEVELOPMENT? |
| ☐ TEST? |
| ☐ INSTALLATION/DEPLOYMENT? |
| ☐ IN SERVICE/RUNNING? |
| ☐ DECOMMISSIONING? |

FIRST ANALYSIS OF CORRESPONDING CYBER-RISKS FOR THE CASE UNDER STUDY

| WHAT KIND(S) OF DISRUPTIONS/INCIDENTS/FAILURES/ATTACKS OF THIS COMPONENT/SUB-SYSTEM DO YOU MOST FEAR? AND WHY? (you may add lines below) | |
|---|---|
| KIND OF DISRUPTION/INCIDENT/FAILURE/ATTACK | POTENTIAL CONSEQUENCES OF DISRUPTION/INCIDENT/FAILURE |
| | |
| | |
| | |

| WHAT COULD BE THE SOURCE(S) OF SUCH CYBER-ATTACKS? AND FOR WHAT LIKELY PURPOSE(S)? (Double click & select options; you may add comments after each selected option) | |
|---|---|
| SOURCE | PURPOSE |
| ☐ NON-IT/PROCESS AUTOMATION EMPLOYEES | ☐ Extortion/Vengeance? ☐ Causing accident? ☐ Extracting key data? ☐ Tarnishing your reputation? |
| ☐ IT/PROCESS AUTOMATION EMPLOYEES | ☐ Extortion/Vengeance? ☐ Causing accident? ☐ Extracting key data? ☐ Tarnishing your reputation? |
| ☐ EXTERNAL CONTRACTORS/MAINTENANCE/VENDORS STAFF | ☐ Extortion/ Vengeance? ☐ Causing accident? ☐ Extracting key data? ☐ Tarnishing your reputation? |
| ☐ EXTERNAL ENTITIES (STATE, ORGANISED CRIME, HACKERS …) | ☐ Extortion/ Vengeance? ☐ Causing accident? ☐ Extracting key data? ☐ Tarnishing your reputation? |
| ☐ OTHER (specify): | ☐ Extortion/ Vengeance? ☐ Causing accident? ☐ Extracting key data? ☐ Tarnishing your reputation? |

| HOW DO YOU THINK THE ATTACKERS WOULD BE MOST LIKELY TO CYBER-ATTACK THE COMPONENT/SUB-SYSTEM? (Double click & select options; you may add comments after the selected option) |
|---|
| ☐ By embedding malware in components at source, during development or integration? |
| ☐ By way of USB keys/external media? |
| ☐ By loading malware through a network link or aerial? |
| ☐ By loading malware through spam/e-mail/corrupted files (Word, PDF, etc.)? |
| ☐ By other means (specify): |

| DO YOU KNOW/SUSPECT CYBER-VULNERABILITIES THAT COULD BE USED TO ATTACK THE COMPONENT/SUB-SYSTEM? |
|---|
| ☐ DO NOT KNOW (comment if you wish): |
| ☐ VULNERABILITIES THAT DIRECTLY AFFECT THE ELEMENT (provide at least some generic information): |
| ☐ VULNERABILITIES THAT AFFECT SURROUNDING ELEMENTS (specify): |

| HOW DO YOU THINK THESE VULNERABILITIES COULD BE IDENTIFIED? |
|---|
| ☐ THROUGH CYBER-SECURITY CHECKS DURING UNIT TESTS OF THE COMPONENT? (specify): |
| ☐ THROUGH CYBER-SECURITY CHECKS DURING INTEGRATION TESTS? (specify): |
| ☐ THROUGH OTHER FORMS OF SPECIFIC CYBER-SECURITY TESTS? (specify): |

| |
|---|
| ☐ THROUGH CYBER-SECURITY CHECKS PERFORMED IN PRODUCTION? (specify): |
| ☐ OTHER? (specify): |

| WHO DO YOU THINK COULD REDUCE THESE VULNERABILITIES? (you may add comments after the selected options) |
|---|
| ☐ VENDORS (specify): |
| ☐ INTEGRATORS (specify): |
| ☐ INTERNAL IT SECURITY STAFF (specify): |
| ☐ INTERNAL PROCESS AUTOMATION STAFF (specify): |
| ☐ EXTERNAL SPECIALISTS IN CYBER-SECURITY (specify): |
| ☐ THIRD-PARTY SPECIALIST CYBER-SECURITY TEST LAB (specify): |
| ☐ REGULATOR/NATIONAL CYBER SECURITY AGENCY (specify): |
| ☐ OTHER (specify): |

## 8.2 Annex 2: Bibliography

ENISA. (2011). *Protecting Industrial Control Systems. Recommendations for Europe and Member States.*

ENISA. (2011a). *Enabling and managing end-to-end resilience.* Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

ENISA. (2011a). *Protecting Industrial Control Systems. Annex I: Desktop Research Results.*

ENISA. (2013). *ENISA Threat Landscape 2013. Overview of current and emerging cyber-threats.*

ENISA. (2013a). *Good Practices for an EU ICS Testing Coordination Capability.*

EUROCONTROL. (2012). *Manual for National ATM Security Oversight document - Directorate Single Sky, DSS/CM/SEC/DEL/12-044.*

Mahan, R. E., Fluckiger, J. D., Clements, S. L., Tews, C., Burnette, J. R., Goranson, C. A., & Kirkham, H. (2011). *Secure Data Transfer Guidance for Industrial Control and SCADA Systems.* Richland, Washington: Pacific Northwest National Laboratory.

MITRE. (2011). *Cyber Resiliency Engineering Framework. Report MTR110237.*

MITRE. (2013). *Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls. Technical Report MTR130531.*

Stamp, J. E., Laviolette, R. A., Phillips, L. R., & Richardson, B. T. (2009). *Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY08).* Sandia National Laboratories, Albuquerque, New Mexico.

THERON, P. (2013). ICT Resilience as Dynamic Process and Cumulative Aptitude. In P. THERON, & S. BOLOGNA (Eds.), *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (pp. 1-35). IGI Global, http://www.igi-global.com/newsroom/archive/igi-global-editor.

# 9 Table of illustrations

European Commission
EUR 27098 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Proposals from the ERNCIP Thematic Group, Case studies for the cyber-security of Industrial Automation & Control Systems, for a European IACS Components Cyber-security Compliance & Certification scheme

Authors: Paul THERON, Sandro BOLOGNA

2014 – 55 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-45417-2

doi:10.2788/21726

Abstract

All studies recently published agree. Industrial Automation and Control Systems (IACS) increasingly constitutes a target for cyber-attacks aiming at disturbing Member States' economies, at disabling our critical infrastructures or at taking advantage of our people. Such hostile acts take place in a context of geostrategic tensions, for the satisfaction of organised crime's purposes, or else in support of possible activist causes. In this context, the ERNCIP Thematic Group (TG), Case studies for the cyber-security of Industrial Automation & Control Systems, was started in January 2014 to answer the question: Do European critical infrastructure operators need to get IACS' components or subsystems tested and "certified" (T&C) with regards to their cyber-security?' And should the answer have been yes, it had to answer a corollary question: What are (roughly) the conditions of feasibility for successfully implementing a European IACS components cyber-security Compliance & Certification Scheme?' This TG's undertaking was a research project, not a task force seeking to deliver an immediately applicable standard. It mobilised representatives of IACS vendors, industrial operators, European Institutions and national cyber-security authorities.

LB-NA-27098-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.


doi:10.2788/21726

ISBN 978-92-79-45417-2