

JRC TECHNICAL REPORT

Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)

Authors

THERON, Paul; RUIZ GUALDA, Jose Francisco; BOSWELL, Tony; BRUN, Jean-Michel;
CASCELLA, Roberto; F., Luis; FREEMAN, Matthew; GONZALEZDE, Sergio; GORSKI,
Janusz; INZERILLI, Tiziano; JANSEN, Martijn Michiel; JARDIM, Mario Roberto;
KOBES, Pierre; KREUTZMANN, Helge; MENTING, Jos; PUC CETTI, Armand;
QUEMARD, Jean-Pierre; QUERREC, Emmanuel; SADMI, Franck; THEUERZEIT,
Michael; VENTER, Razvan; WOLLENWEBER, Kai; WYBOU, Nathanael

Editors

THEODORIDIS, Georgios
GIANNOPOULOS, Georgios

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

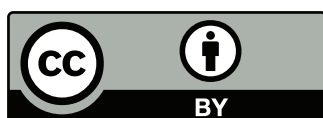
EU Science Hub

<https://ec.europa.eu/jrc>

JRC121520

Ispra: European Commission, 2020

© European Union, 2020



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union 2020

How to cite this report: THERON, Paul; RUIZ GUALDA, Jose Francisco; BOSWELL, Tony; BRUN, Jean-Michel; CASCELLA, Roberto; F., Luis; FREEMAN, Matthew; GONZALEZDE, Sergio; GORSKI, Janusz; INZERILLI, Tiziano; JANSEN, Martijn Michiel; JARDIM, Mario Roberto; KOBES, Pierre; KREUTZMANN, Helge; MENTING, Jos; PUCCETTI, Armand; QUEMARD, Jean-Pierre; QUERREC, Emmanuel; SADMI, Franck; THEUERZEIT, Michael; VENTER, Razvan; WOLLENWEBER, Kai; WYBOU, Nathanael, *Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)*, European Commission, Ispra, 2020, JRC121520

Table of Contents

Table of Contents	3
List of Figures	8
List of Tables	9
Executive Summary.....	10
Rationale of the proposed IACS Components Cybersecurity Certification Scheme (ICCS).13	
ERNCIP IACS Thematic Group	14
1 Terms, Definitions and Acronyms	16
1.1 Acronyms	16
1.2 Terms and Definitions	17
1.2.1 Accreditation.....	17
1.2.2 Applicant.....	17
1.2.3 Assessment Team.....	17
1.2.4 Asset	17
1.2.5 Assurance Level.....	18
1.2.6 Authenticity.....	18
1.2.7 Authorisation	18
1.2.8 Availability.....	18
1.2.9 Certificate	18
1.2.10 Certification	18
1.2.11 Certification Body.....	18
1.2.12 Confidentiality.....	18
1.2.13 Conformity Assessment Body (CAB).....	18
1.2.14 Component	19
1.2.15 Component Context Analysis (CCA).....	19
1.2.16 Component Cybersecurity Profile (CCP)	19
1.2.17 Component Cybersecurity Requirements (CCR)	19
1.2.18 Component Family	19
1.2.19 Component Part.....	19
1.2.20 Component under Assessment	19
1.2.21 Elements Necessary for Assessment	19
1.2.22 generic Component Context Analysis.....	20
1.2.23 Home National Cybersecurity Certification Authority.....	20
1.2.24 IACS Component	20
1.2.25 IACS Components Cybersecurity Certification Scheme (ICCS)	20
1.2.26 ICCS Governance Group (ICCSGG, 6.8)	20
1.2.27 Industrial Automation & Control System (IACS).....	20
1.2.28 Integrity	20
1.2.29 National Accreditation Body (NAB)	20
1.2.30 National Cybersecurity Certification Authority (NCCA)	20
1.2.31 National Cybersecurity Certification Authority / Certification (NCCA.Certification)	20
1.2.32 National Cybersecurity Certification Authority / Supervision (NCCA.Supervision)	21
1.2.33 Non-Repudiation	21

1.2.34	Operational Environment	21
1.2.35	Peer Assessment	21
1.2.36	Peer Review	21
1.2.37	Residual Threat	21
1.2.38	Robustness Testing.....	21
1.2.39	Security Testing Laboratory (TestLab)	21
1.2.40	Security Characteristic.....	22
1.2.41	Security Function.....	22
1.2.42	Security Objectives.....	22
1.2.43	Security Testing Laboratory (TestLab)	22
1.2.44	Technical Domain.....	22
1.2.45	Understandability.....	22
2	<i>Rationale and Scope of the ICCS</i>	23
2.1	Coverage and Scope of the ICCS	23
2.2	Evaluation Methods and Standards	23
2.3	Roles and Responsibilities of Stakeholders	24
2.3.1	Regulatory Authorities.....	24
2.3.2	Applicant.....	25
2.3.3	Certification Bodies/Assessment Teams, National Cybersecurity Certification Authorities and National Accreditation Bodies.	25
2.4	Prescriptive Character of the ICCS	25
3	<i>ICCS Overview</i>	27
3.1	ICCS Assessment Types.....	27
3.1.1	Self-Assessment leading to an EU Statement of Conformity	27
3.1.2	Third-party Assessment leading to an EU Cybersecurity Certificate	28
3.2	Evaluation Activities.....	29
3.2.1	Evaluations Activities per Assurance Level	29
3.2.2	Reuse of Non-ICCS Certificates.....	30
3.2.3	Use of verifications tools	30
3.3	EU Cybersecurity Certificates and EU Statements of Conformity	31
4	<i>Elements from the Applicant.....</i>	32
4.1	Elements Necessary for Assessment (ENA)	32
4.2	Component Cybersecurity Profile (CCP)	32
4.3	Contents of the Documentation	35
4.3.1	Assurance Level Basic	35
4.3.2	Assurance level Substantial.....	37
4.3.3	Assurance level High.....	38
4.4	Publicly Available End-User Documentation	38
5	<i>Evaluation Activities for Assessment Teams</i>	40
5.1	Component Cybersecurity Profile Evaluation.....	40

5.1.1	General Evaluation Activity Description	40
5.1.2	Evaluation Work Units	41
5.2	Documentation Review.....	42
5.2.1	General Evaluation Activity Description	42
5.2.2	Evaluation Work Units	42
5.2.2.1	Assurance Level Basic.....	43
5.2.2.2	Assurance Level Substantial.....	43
5.2.2.3	Assurance Level High.....	43
5.3	Installation, Configuration and Decommissioning Procedures Review.....	43
5.3.1	General Evaluation Activity Description	43
5.3.2	Evaluation Work Units	43
5.4	Security Functions Testing.....	44
5.4.1	General Evaluation Activity Description	44
5.4.2	Evaluation Work Units	44
5.5	Vulnerability Analysis.....	45
5.5.1	General Evaluation Activity Description	46
5.5.2	Evaluation Work Units	46
5.5.2.1	Assurance Level Substantial.....	46
5.5.2.2	Assurance Level High.....	47
5.6	Development Process Audit	48
5.6.1	General Evaluation Activity Description	48
5.6.2	Evaluation Work Units	48
5.7	Penetration Testing	48
5.7.1	General Evaluation Activity Description	48
5.7.2	Evaluation Work Units	49
5.8	Cryptographic Assessment	50
5.8.1	General Evaluation Activity Description	50
5.8.2	Evaluation Work Units	50
6	Evaluation and Certification Processes	52
6.1	Stakeholders and their Relationships.....	52
6.2	Evaluation and Accreditation of CB & Review Management.....	60
6.2.1	Authorisation of CBs.....	60
6.2.2	Accreditation of CB and Assessment Teams	62
6.2.3	Peer Assessment for the NCCA.Certification (Assurance Level High)	62
6.2.3.1	Preparation of the Peer Assessment.....	63
6.2.3.1.1	Preparation of the Peer Assessment by the Peer Assessment Team.....	63
6.2.3.1.2	Preparation of the Peer Assessment by the Auditee.....	64
6.2.3.2	On-Site Peer Assessment.....	65
6.2.3.3	Reporting of the Peer Assessment.....	66
6.2.3.4	Timeline of the Peer Assessment.....	67
6.2.4	Peer Assessment for the CB (Assurance Level Substantial)	68
6.2.5	Peer Review for the NCCA.Supervision.....	68
6.2.6	Requirements and Guidance in case Evaluation Activities are Delegated	69

6.2.7	Regular Meetings of CBs and Assessment Teams	70
6.3	Component Cybersecurity Profile (CCP) and generic Component Context Analysis (gCCA) elaboration and validation	70
6.3.1	Elaboration of Component Cybersecurity Profiles (CCP)	70
6.3.2	Elaboration of a generic Component Context Analysis (gCCA)	70
6.3.3	Validation of CCPs	71
6.3.4	Validation of EU gCCAs	71
6.4	Vulnerability Disclosure Management and Vulnerability Database Update and Communication	72
6.5	Certificate issuance – Mutual Recognition – International Validity.....	72
6.6	Monitoring, Maintenance, Renewal and Withdrawal of Certificates	72
6.7	Monitoring, Maintenance and Renewal of Statements of Conformity.....	73
6.7.1	Monitoring and maintenance of Statement of Conformity	73
6.7.2	Renewal of Statement of Conformity.....	75
6.8	The ICCS Governance Group: Role and responsibility of the ICCSGG.....	76
6.8.1	Responsibilities of the ICCSGG	77
7	ICCS Supporting Documents.....	78
7.1	IACS Components Cybersecurity Requirements (ICR) Catalogue.....	78
7.2	IACS Components Cybersecurity Evaluation Report Table of Contents (ICERT)	80
7.3	IACS Component Cybersecurity Certificates Contents (IC3).....	81
7.4	IACS Component Statement of Conformity Contents.....	82
Annex A	Coverage of CSA by ICCS and Existing Evaluation Approaches	83
A.1	Mapping Between CSA and ICCS	83
A.1.1	Correspondence of ICCS to Article 51 of the EU CyberSecurity Act (Security Objectives of European Cybersecurity Certification Schemes.....	83
A.1.2	Correspondence of ICCS to Article 52 of the EU CyberSecurity Act (Security Objectives of European Cybersecurity Certification Schemes).....	85
A.1.3	Correspondence of ICCS to Article 53 of the EU CyberSecurity Act (Conformity Self-Assessment)	89
A.1.4	Correspondence of ICCS to Article 54 of the EU CyberSecurity Act (Elements of European Cybersecurity Certification Schemes).....	90
A.1.5	Correspondence of ICCS to Article 55 of the EU CyberSecurity Act (Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes)	94
A.2	Mapping Between CSA Article 51 and Existing Evaluation Approaches	95
A.2.1	IEC 62443-4-1 & 62443-4-2.....	95

A.2.2	<i>Common Criteria (ISO/IEC 15408)</i>	99
Annex B	<i>Relevant Standards</i>	102
B.1	<i>The Standardisation Context</i>	102
B.2	<i>Relevant Standardisation Bodies</i>	102
B.3	<i>Standards Relevant to IACS Evaluation</i>	103
B.3.1	<i>General Standards</i>	104
B.3.2	<i>Risk and Management Systems Evaluation Standards</i>	104
B.3.3	<i>Security Requirements Standards</i>	104
B.3.4	<i>Security Evaluation Methods</i>	104
B.3.5	<i>Other relevant Standards</i>	105
B.4	<i>Status of the standards</i>	105
Annex C	<i>Standards vs Evaluation Activities Mapping</i>	107
Annex D	<i>Correspondence of the Agnostic Terminology with IEC 62443 4-2, Lightweight and Common Criteria Certification Paths</i>	108
D.1	<i>Validation of CCPs/gCCAs based on IEC 62443-4-2</i>	110
D.2	<i>Validation of CCPs/gCCAs based on Lightweight Methodologies</i>	110
D.3	<i>Validation of CCPs/gCCAs based on ISO/IEC 15408</i>	111
Annex E	<i>CCP and gCCA Examples</i>	112
E.1	<i>Example for a CCP</i>	112
E.2	<i>Example gCCA</i>	112
	<i>References</i>	115

List of Figures

Figure 1 - Mapping between the EU CSA Assurance Levels and the ICCS assessments.....	27
Figure 2 - Applicant in context	53
Figure 3 - NCCA.Supervision in context	54
Figure 4 - Issuing a Certificate on the Applicant request	55
Figure 5 - Security Testing Laboratory (TestLab) in the certification process	57
Figure 6 - Accreditation, Peer Assessment and Peer Review model.....	58
Figure 7 - Issuing an EU Statement of Conformity	59
Figure 8 - Consolidated organisation of the ICCS certification and Self-Assessment	60
Figure 9 - Relationship of the agnostic CCP/gCCA principles to certification approaches	108
Figure 10 - Relation of agnostic CCP/gCCA principles to the Lightweight certification approach ..	109
Figure 11 - Relation of agnostic CCP/gCCA principles to the Common Criteria certification approach	109
Figure 12 - Relation of agnostic CCP/gCCA principles to the IEC 62443 4-2 certification approach	110

List of Tables

Table 1 - Mapping between the CSA Assurance Levels and the Evaluation Activities.....	29
Table 2 - Mapping between the CSA Assurance Levels and the ENA.....	32
Table 3 – Graphical Conventions	52
Table 4 – Content and method for Peer Assessment.....	66
Table 5 – Example of format for the ICR catalogue	79
Table 6 – Table of contents for the ICERT	80
Table 7 – Correspondence of ICCS to Article 51	85
Table 8 – Correspondence of ICCS to Article 52	89
Table 9 – Correspondence of ICCS to Article 53	90
Table 10 – Correspondence of ICCS to Article 54	94
Table 11 – Correspondence of ICCS to Article 55	95
Table 12 – Mapping CyberSecurity Act Article 51 to IEC 62443-4-1 & IEC 62443-4-2	99
Table 13 – Mapping CyberSecurity Act Article 51 to Common Criteria (ISO/IEC 15408).....	101
Table 14 – Annex C Standards vs Evaluation Activities mapping.....	107

Executive Summary

The Cybersecurity Act (CSA) that was published on 17 April 2019 introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union.

Industrial Automation & Control Systems (IACS) are essential part of most critical infrastructures and critical services. The term IACS refers to all the Components (PLCs, SCADA, HMI, etc.) that are integrated into critical infrastructures and industrial production establishments. Health, power, water, transportation, just to name a few, all depend to a great extent on Industrial Automation & Control Systems for delivering such services. Furthermore, all industrial plants and sectors are employing Industrial Automation & Control Systems. The transformation process towards Industry 4.0 will lead to an even higher dependency on such systems. Past experience has shown that their cyber vulnerabilities can be exploited by adversaries and create huge impact on infrastructures and subsequent impact on the economy and human lives. Practically, cyberattacks against critical infrastructures are in fact cyberattacks against their Industrial Automation & Control Systems. Thus, it is of paramount importance to apply all possible measures in order to increase the level of cybersecurity of IACS.

The Industrial Automation & Control Systems (IACS) Thematic Group (TG) of ERNCIP (European Reference Network for Critical Infrastructure Protection) has been working for several years in this domain. The work it has performed was fundamental for picking up quickly the requirements of the CSA and for drafting a coherent report describing in great detail all the elements that are necessary in order to establish a Cybersecurity Certification Scheme for IACS Components. Members of this group are individual experts representing multiple EU Member States as well as their organisations and domains of interest: national cybersecurity agencies, IACS (Components) manufacturers, cybersecurity industries, cybersecurity evaluation laboratories, cybersecurity certification authorities, and academia.

IACS market is a fast growing one. Figures for 2019¹ refer to a market with an overall value of €100 billion. On the basis of the current growth rate, this market is expected to exceed €150 billion by 2025. Despite the high specialisation of IACS products, it is a relatively competitive market in which European companies have an important share. In addition, the experts involved in the development of the present report have considered private sector's concerns on the costs associated with the certification of IACS Components. To this end, a risk-based approach has been adopted with different levels of certification: from self-compliance to full third-party certification (including the product development process) in order to reassure that critical Components are screened accordingly while less critical Components undergo a much faster and simplified process without creating unnecessary burden to the manufacturers of such Components.

¹ Mordor Intelligence, <https://www.mordorintelligence.com/industry-reports/industrial-control-systems-market-industry>, last accessed 15/07/2020

Fostering the establishment of a minimum common level of security through a risk-based certification process would ensure that there is no market distortion and that an equal level of play is achieved.

There is a debate in the cybersecurity community between certification of Components vs certification of systems. In the present report, the cybersecurity certification of Industrial Automation & Control Systems (IACS) is considered to take place at the level of their Components, i.e. from PLCs or automation devices up to Supervisory Control And Data Acquisition systems (SCADA).

The fundamental principle behind this position is that for building cybersecure IACS (i.e. whole systems/subsystems) one needs to procure and assemble adequately cybersecure IACS Components, either hardware or software. Hence, it is crucial to focus on the certification/conformance of the separate Components of the IACS, in order to ensure that these Components, as the building elements of the whole IACS, satisfy the cybersecurity requirements that are foreseen for their design and development. Moreover, it is equally fundamental that this certificate/conformance is obtained and duly verified through a reliable and widely recognised evaluation and certification process. It should be finally noted that, by approaching the certification/compliance on per Component basis, it is possible to determine different security requirements and assurance levels for different elements of the overall IACS, depending on the system design, the intended use and operational environment, and the identified system-level security measures.

On the other hand, besides their comprising Components, the cybersecurity certification of entire IACS systems or subsystems depends on multiple and complex factors, from engineering, integration or maintenance practices to human behaviour, project management and managerial considerations. Therefore, the IACS (systems) cybersecurity certification does not belong in the scope of the present document.

The CyberSecurity Act sets the framework for establishing cybersecurity certification schemes. The Union Rolling Work Programme provides the priority areas for developing certification schemes and ENISA develops the respective candidate schemes. The goal of this report is to set up a solid basis for the elaboration of a future IACS Components Cybersecurity Certification Scheme under the responsibilities and procedures established by the CSA so as to help the community make a head start and reduce the development time of the candidate scheme by ENISA (under the assumption of course that IACS will be one of the priorities of the Union Rolling Work Programme).

To achieve this goal, the present report comes in the shape of a structured list of detailed requirements that reflect the consensus established between all IACS TG's members about how to frame and conduct the cybersecurity certification of IACS Components in order to guarantee that this common language will help the mutual recognition of Certificates across Europe, and beyond.

These requirements cover:

- Clear definitions and a summary of abbreviations used throughout, in Section 1;
- The function and scope of application of the ICCS, in Section 2;
- General requirements that frame IACS Components cybersecurity certification, in Section 3;

- The elements that should be fed as input of the evaluation process, in Section 4;
- Evaluation Activities to be performed by Assessment Teams, in Section 5;
- Evaluation and certification processes, in Section 6;
- And ICCS supporting documents, in Section 7.

Annexes are informative only:

- Annex A shows how the proposed ICCS matches the CSA's requirements;
- Annex B & Annex C reference standards of interest;
- Annex D shows how the ICCS bridges with existing Cybersecurity Certification Schemes;
- Annex E depicts briefly a Component Cybersecurity Profile, the keystone of the process.

Besides these “technical” requirements, the document also expresses requirements meant for the ICCSGG or an ad hoc group in charge of elaborating or governing the ICCS. These specific requirements, agreed within the IACS TG, describe the future work suggested for building the definitive ICCS scheme.

DG JRC expresses its gratitude to the IACS TG members for their drive, open mind and strong commitment to this piece of work during the past 18 months of 2019 and 2020 and to DG CNECT for providing support and guidance for developing this report.

This work has received funding from DG CNECT through the administrative arrangement SMART 2018/0060 “Support on the development of the EU Cybersecurity policy package initiatives and ePrivacy policy” - (JRC contract number 35293).

Feedback and inquiries should be communicated to:

EC DG Joint Research Centre
 erncip-office@ec.europa.eu

Rationale of the proposed IACS Components Cybersecurity Certification Scheme (ICCS)

The present report on Recommendations for the Implementation of a European IACS Components Cybersecurity Certification Scheme (ICCS) has been produced with a close and consistent reference and relevance to the EU CyberSecurity Act, following a rationale that allows it to constitute the most solid basis for a future European Cybersecurity Certification Scheme dedicated to the subject of Industrial Automation & Control Systems Components. To this end, given its high quality and the completeness of its technical content, this report can be considered to be included in the Union Rolling Work Programme so as to be thereafter further developed by ENISA as a candidate European Cybersecurity Certification Scheme in the respective area.

In this respect, this “draft” ICCS has been prepared with the following requirements in mind:

1. The ICCS had to be prescriptive and unequivocal

This means that this document intends to give well structured, concise, clear and precise requirements to all stakeholders involved in the IACS cybersecurity certification process that will help guaranteeing the rigour and homogeneity of the evaluation and certification process wherever and whoever takes a part in it. This is a pre-condition of the equivalence and mutual recognition of Certificates delivered by different cybersecurity certification authorities across Europe and beyond.

2. The ICCS had to be usable and self-explanatory

This means that this document should contain all the requirements, recommendations, guidelines and useful elements of information and references that stakeholders would need when implementing the ICCS. Requirements must be self-explanatory. The document has to be easy to read by professional stakeholders involved in products’ cybersecurity engineering, evaluation and certification.

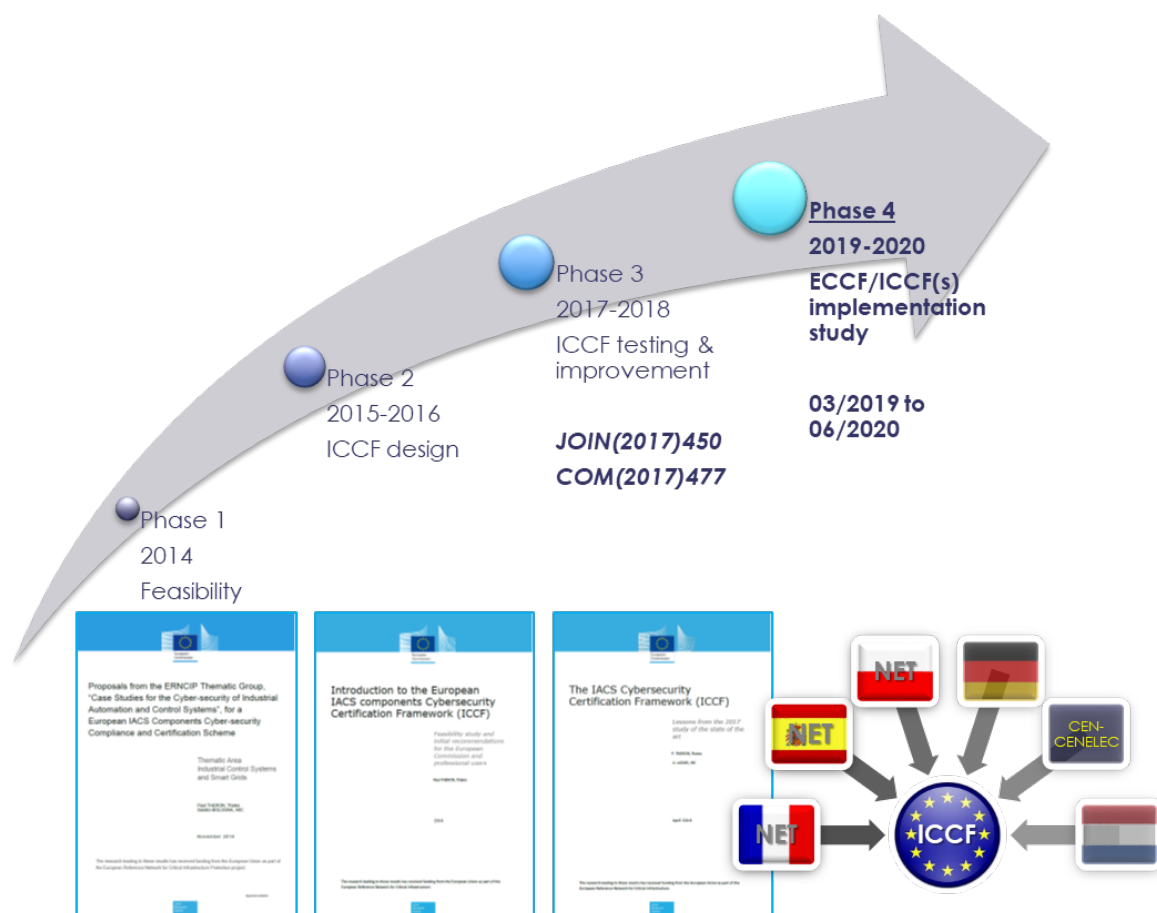
3. The ICCS had to be agnostic

This means that this document should provide recommendations for evaluation and certification activities defined in agnostic manner and with a terminology not biased by any existing scheme or standard. In defining the standard or set of standards that will support the requirement of the ICCS, the same principle of agnosticism should apply to guarantee the usability and acceptance of the ICCS across Europe, and beyond.

In addition, a European ICCS Governance Group should be established to monitor the use of the ICCS and to propose coordinated ways to resolve the issues that might arise in this context.

Finally, the present report abides with the terms of the 2019 CyberSecurity Act of the European Union. The absolute consistency between the ICCS and the CSA’s requirements is presented throughout the report as well as in a dedicated Annex.

This report is the outcome of the fourth phase of the ERNCIP (European Reference Network for Critical Infrastructure Protection) Thematic Group that focuses on the cybersecurity certification of Components of Industrial Automation & Control Systems. This IACS Thematic Group has undergone four phases since its establishment back in 2014, where the three first phases have laid down the groundworks for the development of the hereby proposed ICCS.



The ERNCIP IACS Thematic Group has as members highly reputable experts in the relevant fields from all over the European Union, and it is driven, as well as the overall ERNCIP project, by the EC DG JRC. In more detail, the members of the IACS Thematic Group that are also responsible for devising the present report are:

- Supervision: Georgios GIANNOPOULOS and Georgios THEODORIDIS (EC DG Joint Research Centre)
- Coordinator: Paul THERON (Thales, France)
- Co-Coordinator and Editor: Jose Francisco RUIZ GUALDA (jtsec Beyond IT Security, Spain)
- Members of the Thematic Group and authors of the proposed ICCS (in alphabetical order):
 - BOSWELL, Tony (CyTAL UK Ltd, United Kingdom)
 - BRUN, Jean-Michel (Schneider Electric, France)
 - CASCELLA, Roberto (European Cyber Security Organisation)
 - F., Luis (Centro Criptologico Nacional – CCN, Spain)

- FREEMAN, Matthew (CyTAL UK Ltd, United Kingdom)
- GONZALEZDE, Sergio (Applus+, Spain)
- GORSKI, Janusz (Gdansk University of Technology and ARGEVIDE sp. z o.o., Poland)
- INZERILLI, Tiziano (Ministero dello Sviluppo Economico, Italy)
- JANSEN, Martijn Michiel (Netherlands)
- JARDIM, Mario Roberto (Schneider Electric, France)
- KOBES, Pierre (Siemens AG, Germany)
- KREUTZMANN, Helge (Bundesamt für Sicherheit in der Informationstechnik – BSI, Germany)
- MENTING, Jos (ENGIE Laborelec, Belgium)
- PUCCETTI, Armand (Commissariat à l'Energie Atomique et aux Energies Alternatives – CEA, France)
- QUEMARD, Jean-Pierre (Kuzul An Traezhenn – KAT, France)
- QUERREC, Emmanuel (Turku University of Applied Sciences, Finland)
- SADMI, Franck (Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, France)
- THEUERZEIT, Michael (Hudson Cybertec, Netherlands)
- VENTER, Razvan (Secura B.V., Netherlands)
- WOLLENWEBER, Kai (Siemens AG, Germany)
- WYBOU, Nathanael (ENGIE Laborelec, Belgium)

1 1 Terms, Definitions and Acronyms

2 1.1 Acronyms

Acronym	Term
CAB	Conformity Assessment Body
CB	Certification Body
CCA	Component Context Analysis
CCP	Component Cybersecurity Profile
COTS	Commercial off-the-shelf
CCR	Component Cybersecurity Requirements
CSA	European Union CyberSecurity Act
CuA	Component under Assessment
CVE	Common Vulnerabilities and Exposures
ECC	European Cybersecurity Certificate
ECCG	European Cybersecurity Certification Group
ENA	Elements necessary for assessment
ENISA	European Network and Information Security Agency
gCCA	generic Component Context Analysis
IACS	Industrial Automation & Control System
ICCS	IACS Cybersecurity Certification Scheme
ICCSGG	ICCS Governance Group
ICERT	IACS Components Cybersecurity Evaluation Report Table of contents
ICR	IACS Components Cybersecurity Requirements
IC3	IACS Component Cybersecurity Certificates Contents
NAB	National Accreditation Body

NCCA	National Cybersecurity Certification Authority
NCCA.Certification	National Cybersecurity Certification Authority / Certification
NCCA.Supervision	National Cybersecurity Certification Authority / Supervision
OSS	Operations Support Systems
PLC	Programmable logic controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
TestLab	Security Testing Laboratory

1.2 Terms and Definitions

1.2.1 Accreditation

A process by which a National Accreditation Body (NAB) formally declares that a Certification Body (1.2.11) or a TestLab (1.2.39) is competent to conduct Component Conformity Assessment activities.

Note: The scope of Accreditation covers both certification and evaluation functions. Accreditation will be performed on the basis of ISO/IEC EN 17065 for Certification Bodies and by ISO/IEC EN 17025 for Assessment Teams.

1.2.2 Applicant

A legal entity requesting certification

Note: The Applicants can be entities of different type and scope. For instance, an Applicant can be a Manufacturer (i.e. the developer and/or producer of the IACS Component) or a supplier (i.e. an entity placing the IACS Component on the market).

1.2.3 Assessment Team

A group of persons that performs Evaluation Activities for the Certification Body

Note: The Assessment Team can be internal resources (cf. §6.2.1 of ISO/IEC EN 17065) of the Certification Body or external resources (cf. §6.2.2 of ISO/IEC EN 17065) of the Certification Body in the ICCS. In the latter case the Assessment Team is part of a body called Security Testing Laboratory (1.2.39).

1.2.4 Asset

Anything (tangible or intangible) that has value and which, therefore, requires protection.

24 **1.2.5 Assurance Level**

25 The Assurance Level of an ICCS is a basis (qualitative measure) for confidence that an IACS
26 Component, under certification by this ICCS, actually meets the security requirements of the ICCS
27 (cf. CyberSecurity Act).

28 **Note:** In accordance with the CyberSecurity Act, the ICCS considers three distinct Assurance
29 Levels: Basic, Substantial or High. In addition, the ICCS covers the EU Statement of
30 Conformity, which refers to the Assurance Level Basic.

31 **1.2.6 Authenticity**

32 A security characteristic that assures that an entity is what it claims to be

33 **1.2.7 Authorisation**

34 A process by which a Certification Body receives from an NCCA.Supervision (1.2.32) the right to
35 perform ICCS-related assessments in a particular Technical Domain of competence

36 **1.2.8 Availability**

37 A security characteristic that ensures the timely and reliable access to and use of an IACS
38 information and functionality

39 **1.2.9 Certificate**

40 Official document attesting that an IACS Component meets the requirements of a specific ICCS
41 Assurance Level (i.e. Basic, Substantial or High)

42 **1.2.10 Certification**

43 A process by which a Certificate is issued by a Certification Body (1.2.11) on the foundation of the
44 evaluation report of a given IACS Component

45 **1.2.11 Certification Body**

46 A body that performs certification activities corresponding to the Accreditation(s) (1.2.1) received
47 by the National Accreditation Body and to the Authorisation(s) (1.2.7) received by the
48 NCCA.Supervision

49 **1.2.12 Confidentiality**

50 A security characteristic that preserves authorised restrictions on information access and disclosure,
51 including means for protecting personal privacy and proprietary information

52 **1.2.13 Conformity Assessment Body (CAB)**

53 A body that performs Conformity Assessment activities including calibration, testing, certification
54 and inspection (EU Regulation 765/2008)

55 **Note:** In the ICCS, the certification activities of a CAB are performed by a Certification Body
56 and the Evaluation Activities of a CAB (i.e. calibration, testing and inspection) are
57 performed by Assessment Teams.

1.2.14 Component

A device or piece of software/hardware i) that belongs to or is developed by a Manufacturer, ii) that has a reference and/or branding name (e.g. product number), and iii) the instances of which may be assigned with a serial number so as to identify each specific instance built by the Manufacturer.

1.2.15 Component Context Analysis (CCA)

The specification of the Security Objectives to be fulfilled by an IACS Component, based on a description of the intended use, the intended operational environment, the included assets and the applicable threats.

1.2.16 Component Cybersecurity Profile (CCP)

The Specification of the security requirements that apply to a specific IACS Component, consisting of the definition of the CuA (Component under Assessment), the CCA (1.2.15) and the CCR (1.2.17)

Note: The Component Cybersecurity Profile is the basis for the Conformity Assessment activities.

1.2.17 Component Cybersecurity Requirements (CCR)

The specification of implementation-dependent security requirements to be fulfilled by an IACS Component associated to an intended use and context described in the CCA.

1.2.18 Component Family

A group/set of IACS Components that share the same gCCA (1.2.22)

1.2.19 Component Part

A hardware or software unit with distinct boundaries

Note: Parts, in this context, are: programs, libraries, Operating Systems, packages, tools and other software elements, including third party libraries.

Note: A Component may be composed of only one part, i.e. no logical or meaningful subdivision is applicable.

Example of a Component Part in the case of a Component Family:

A PLC includes a “user program”

1.2.20 Component under Assessment

An IACS Component subject to a Conformity Assessment

1.2.21 Elements Necessary for Assessment

The Component’s technical documentation and any other relevant information that is related to the scope of the foreseen assessment

Note: The equipment required for the Component testing may also be part of the Elements Necessary for Assessment.

1.2.22 generic Component Context Analysis

The specification of the Security Objectives to be fulfilled by a family of IACS Components based on a description of the generic intended use, the generic intended operational environment, the included assets and the applicable threats. This description can be optionally extended with a set of generic security requirements.

1.2.23 Home National Cybersecurity Certification Authority

The NCCA.Supervision (1.2.32) of the Member State where the Manufacturer performing the Self-Assessment or the Certification Body (in the case of Assurance Level Basic, Substantial or High) is established.

1.2.24 IACS Component

A software and/or hardware element of an Industrial Automation & Control System

1.2.25 IACS Components Cybersecurity Certification Scheme (ICCS)

The Cybersecurity Certification Scheme created within the framework of the CSA for the cybersecurity certification of IACS Components

1.2.26 ICCS Governance Group (ICCSGG, 6.8)

An EU entity in charge of:

- monitoring the implementation of the ICCS,
- identifying issues arising from the implementation of the ICCS,
- proposing solutions to resolve issues relating to the implementation of the ICCS.

1.2.27 Industrial Automation & Control System (IACS)

A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

1.2.28 Integrity

A security characteristic that protects the accuracy and completeness of assets.

1.2.29 National Accreditation Body (NAB)

The sole body in a Member State that performs accreditation with authority derived from the State (EU regulation 765/2008)

1.2.30 National Cybersecurity Certification Authority (NCCA)

According to the CSA, this is the national governmental body that is the competent authority for all aspects of cybersecurity certification at national level. It covers activities of certification and supervision.

Note: In the ICCS, the certification activities are performed by the NCCA.Certification (1.2.31) and the supervision activities are performed by the NCCA.Supervision (1.2.32).

1.2.31 National Cybersecurity Certification Authority / Certification (NCCA.Certification)

The National Conformity Assessment Body that acts as a certification body for Assurance Level “High” certification according to the CSA.

1.2.32 National Cybersecurity Certification Authority / Supervision (NCCA.Supervision)

The Member State authority(s) that are responsible for supervising the ICCS scheme.

1.2.33 Non-Repudiation

A security characteristic that proves the occurrence of a claimed event or action and its originating entity.

1.2.34 Operational Environment

The requirements for i) the physical layout of buildings (e.g. peripheral security), ii) the Components (e.g. no USB port on an Engineering Workstation or PLC), iii) the people working in the environment of the product (e.g. technicians are trustworthy) or iv) the processes applied in relation to the operation of the product.

Note: Compensating countermeasures are part of the operational environment.

1.2.35 Peer Assessment

The periodical and reciprocal assessment between Certification Bodies that issue Certificates of Assurance Level Substantial or High, so as to harmonize practices regarding Conformity Assessment

Note: Objectives are defined in the Preamble Paragraph 100 of the CSA

1.2.36 Peer Review

The periodical and reciprocal assessment between NCCA.Supervision, so as to harmonize practices regarding the monitoring and supervision of the scheme.

Note: Objectives are defined in the Preamble Paragraph 99 of the CSA

1.2.37 Residual Threat

A threat that remains even in the presence of the formulated protection assumptions.

1.2.38 Robustness Testing

Any quality assurance methodology focused on testing the robustness of the Component against cyber-attack methods. There are several means to carry out robustness testing and different attack methods can be applied.

Example of Robustness Testing:

- Static code analysis: An analysis could be carried out using automated tools to identify flaws in the source code;
- Tool-based Assessment Method: An assessment may be carried out using security testing tools (OSS or COTS). This assessment may include different kind of attacks such as Automated port scans against the device, Known-Vulnerability Scans, Fuzzing testing, etc.

1.2.39 Security Testing Laboratory (TestLab)

An evaluation body that may be licensed by a Certification Body for conducting specific Evaluation Activities related to the assessment of an IACS Component.

153 **Note:** The related Evaluation Activities can vary broadly, covering the whole range of an
154 IACS Component evaluation. They can include validation testing, penetration
155 testing, vulnerability analysis, documentation and code review, site visits, etc.

156 **Note:** The accreditation of TestLabs is optional; it is not mandatory.

157 **1.2.40 Security Characteristic**

158 A security property which a CuA claims to fulfil

159 **1.2.41 Security Function**

160 The implementation of a Security Characteristic of a CuA

161 **1.2.42 Security Objectives**

162 The cybersecurity aptitudes that an IACS Component must achieve

163 **Note:** The Security Objectives are specified in Article 51 of the CSA

164 **1.2.43 Security Testing Laboratory (TestLab)**

165 An evaluation body that may be licensed by a Certification Body for conducting specific Evaluation
166 Activities related to the assessment of an IACS Component.

167 **Note:** The related Evaluation Activities can vary broadly, covering the whole range of an
168 IACS Component evaluation. They can include validation testing, penetration
169 testing, vulnerability analysis, documentation and code review, site visits, etc.

170 **Note:** The accreditation of TestLabs is optional; it is not mandatory.

171 **1.2.44 Technical Domain**

172 A particular technical area of evaluation, in which the CB demonstrates its expertise and capabilities
173 and for which it is accredited

Example of Technical Domain:

Embedded products, PLC, Software applications, etc.

174 **1.2.45 Understandability**

175 Understandability in the context of ICCS means that the language and depth of description are
176 commensurable with the knowledge of the anticipated end customer, including the expected
177 knowledge about terms and concepts

2 Rationale and Scope of the ICCS

2.1 Coverage and Scope of the ICCS

The scope of the ICCS is the cybersecurity certification of the Components of an Industrial Automation & Control System (IACS).

The Components of an IACS can be, for instance:

- [a] Automation devices that affect the industrial production process;
- [b] Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU) that monitor and command automation devices;
- [c] Distributed servers that monitor and control PLCs;
- [d] Engineering Workstations through which engineers and technicians configure RTUs and PLCs;
- [e] Industrial networks that connect the Components of an IACS;
- [f] The Supervisory Control And Data Acquisition system (SCADA) that monitors the entire IACS;
- [g] The Historian of the SCADA that logs everything happening in the flow of commands and events of an IACS.

The ICCS is not intended for the certification of entire IACS systems or their subsystems. This issue belongs to a more global and complex engineering and integration process under the governance of the IACS owners themselves, as part of the industrial buyers and/or system integrators responsibilities.

Three Assurance Levels (i.e. Basic, Substantial and High) are considered in the ICCS, in compliance with the CSA.

2.2 Evaluation Methods and Standards

Different approaches are available for the cybersecurity certification of IACS Components.

On one hand, Industrial Automation & Control Systems are associated with a system approach as well as with different vertical markets (e.g. oil & gas, automotive, energy etc.). There is a big diversity and modularity of IACS products to which specific requirements of safety and availability are applied. With this in mind, the IEC 62443 standard and its different parts cover the entire life-cycle of an IACS from Manufacturer's product design to the system design and to its installation and related operational aspects from the end-user side. The international IECEE certification scheme is for instance addressing these different steps, especially regarding the certification of IACS.

On the other hand, existing national and international certification schemes, such as CSPN (by the French ANSSI), BSZ (by the German BSI), LINCE (by the Spanish CCN) or Common Criteria, focus on specific IT security products as the primary object of evaluation (e.g. security hardware chip, firewall, etc.).

In addition, Manufacturers may in some cases need to comply with different national or international regulations, each one of which requires its own certification. This increases significantly the certification cost (in terms of finances, time and effort) for a given product, since the technical approach (e.g. used vocabulary, Evaluation Methodology etc.) as well as the administrative procedures may substantially vary among the various certification schemes.

Hence, as it becomes apparent, the certification of IACS Components is rather challenging, since it has to bridge this kind of gaps and to help the “convergence” between these different worlds. In this respect, in order to address all these issues of divergence in the area of IACS cybersecurity certification, the IACS TG has decided on purpose not to choose a specific standard or scheme of reference for the ICCS.

Thereby, different alternative certification paths are foreseen (listed in Annex D). Moreover, different standards that could be used as a foundation for certification are considered (listed in Annex C). **This agnostic approach described in this ICCS scheme** ensures the compatibility between the aforementioned different certification paths.

For instance, the specification of a Component Cybersecurity Profile (CCP) based on an agnostic Cybersecurity Context Analysis (CCA) allows for an independent description of the Security Objectives of a product without being locked in one standard or scheme of reference.

Note: Should a choice of standards of reference be made in the context of the elaboration of the definitive, official ICCS, this choice is left to the respective ENISA Ad hoc Working Group.

2.3 Roles and Responsibilities of Stakeholders

This Section summarises the main roles and responsibilities of the various stakeholders involved in the European cybersecurity evaluation and certification process.

The cybersecurity certification requirements that are expressed in the present document are framed on the basis of these definitions.

2.3.1 Regulatory Authorities

The European CyberSecurity Act defines three levels of cybersecurity certification: Basic, Substantial and High. They are complemented by the possibility of a Manufacturer’s Self-Assessment based on the Basic Assurance Level requirements, which delivers only an indicative Statement of Conformity.

Currently, the cybersecurity certification is a voluntary process. However, in 2023, the European Commission will review whether the cybersecurity certification will remain voluntary or it will become mandatory for a list of products, solutions and services.

240 ENISA contributes to the establishment and maintenance of European Cybersecurity Certification
241 Schemes. To support this new role, the mandate of ENISA has been adequately adapted under the
242 2019 European CyberSecurity Act (CSA).

243 In accordance with CSA, the subject of the candidate European Cybersecurity Certification Schemes
244 that are developed by ENISA are proposed by the European Commission through the Union Rolling
245 Work Programme, which is prepared in collaboration with the ECCG (European Cybersecurity
246 Certification Group, i.e. representatives of the Member States competent authorities) and the SCCG
247 (Stakeholder Cybersecurity Certification Group, i.e. representatives of the Industry).

248 For each candidate European Cybersecurity Certification Schemes, ENISA will create an Ad hoc
249 Working Group that will support ENISA in preparing the specific draft candidate cybersecurity
250 certification scheme.

251 The ICCS Governance Group will be the entity in charge of handling the implementation of the ICCS
252 (6.8).

253 The National Cybersecurity Certification Authorities (NCCA) have the following roles under the CSA:

- 254 [a] To foster and enforce the application of the CSA and ICCS at the national level;
- 255 [b] To deliver the Certificates of the Assurance Level High in their capacity as National
256 Cybersecurity Certification Authority / Certification;
- 257 [c] To control the validity of Certificates and statements of conformity in their capacity as
258 National Cybersecurity Certification Authority / Supervision.

259 **2.3.2 Applicant**

260 In the context of the ICCS, the Applicant is the legal entity requesting the certification (1.2.2).

261 **Note:** The Applicants can be entities of various type and scope, e.g. manufacturer, sponsor,
262 developer, producer or the supplier of an IACS Component.

263 **2.3.3 Certification Bodies/Assessment Teams, National Cybersecurity Certification Authorities 264 and National Accreditation Bodies.**

265 The Assessment Teams and the Certification Bodies (CB) are those entities that will perform the
266 assessments or technical evaluation tests, and associated processes, that allow assessing the
267 compliance of a designated IACS Component with the cybersecurity requirements set in its
268 Component Cybersecurity Profile (CCP).

269 National Accreditation Bodies accredit CBs/TestLabs under applicable standards such as ISO/IEC EN
270 17065 for CBs or ISO/IEC EN 17025 for TestLabs.

271 The NCCA acts as a Member State's competent authority for cybersecurity certification. CBs deliver
272 the ICCS-related Certificates under the terms of the CSA and the applied ICCS.

273 **2.4 Prescriptive Character of the ICCS**

274 ICCS in the form of the present report follow a descriptive approach:

- *'Shall'* is used along the lines of this document to indicate a mandatory requirement.
- *'Should'* indicates a requirement that is preferred but not mandatory (note that some elements of a *'should'* statement may turn out to be necessary for a specific Component to meet an associated *'shall'* –a case-by-case decision may then have to be made). *'Should'* requirements generally indicate areas in which it can be expected that requirements will be strengthened in the future. This is especially relevant for IACS Components since there is a recognition that the cybersecurity of IACS has been limited by legacy systems and needs to be enhanced.

Moreover, the following formatting conventions have been followed throughout the document:

- Requirements of the ICCS are marked as: Req.YXX0, where Y is the Section of the document and XX a sequential number.
- Requirements for the ICCSGG are marked as: ICCSGG-Req.XXX0, where XXX is a sequential number.
- The requirements for the ICCSGG are enclosed in a box with grey background.
- The examples are enclosed in a box with white background and double-line border.

3 ICCS Overview

3.1 ICCS Assessment Types

As illustrated in the picture below, the IACS Components Cybersecurity Certification Scheme (ICCS) allows two different types of assessments: one leading to an **EU Cybersecurity Certificate** and another one that allows the Manufacturers to issue by themselves an **EU Statement of Conformity**.

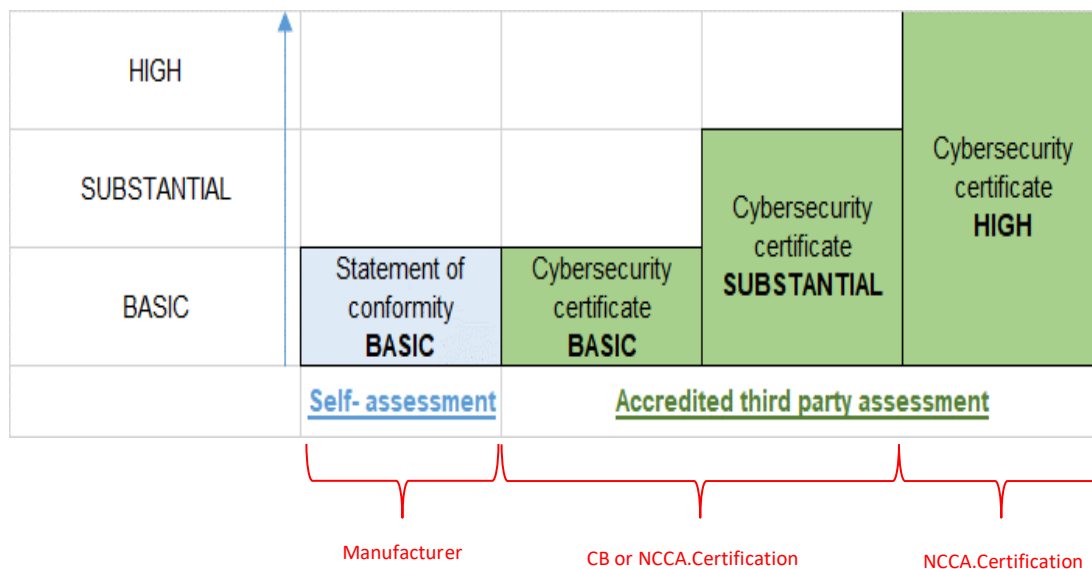


Figure 1 - Mapping between the EU CSA Assurance Levels and the ICCS assessments

3.1.1 Self-Assessment leading to an EU Statement of Conformity

Req.3010 The Self-Assessment shall be limited to the Assurance Level Basic.

Req.3020 The Self-Assessment activities shall be conducted under the sole responsibility of the Manufacturer.

Req.3030 The Assessment Team members (internal and/or external to the Manufacturer) shall be different from the design team members. Staff carrying out assessment activities shall be demonstrably free of personal conflict of interest, i.e. they shall not assess any item or characteristic of the CuA for which they are currently responsible or they have contributed to the development of any pieces of evidence that are used in the concerned assessment. In more detail, it would be acceptable for the Assessment Team members to have been involved in the review of parts of the CuA (e.g. design reviews), but it would not be acceptable for them to have participated in the actual development of the design (either the initial version of any updates to it) of any CuA parts.

Note: The Self-Assessment activities can be outsourced. Even in this case, they are conducted under the sole responsibility of the Manufacturer.

Req.3040 The Self-Assessment shall include all the Evaluation Activities that are defined in Table 1 for the Assurance Level Basic.

317	Note:	For the Assurance Level Basic, the Evaluation Activities assess whether the
318		Components are secure by default and by design, so as to minimize the known Basic
319		risks of cybersecurity incidents and cyberattacks.
320	Req.3050	After collecting the necessary pieces of evidence and successfully completing the
321		assessment, the Manufacturer may issue an EU Statement of Conformity. If issued,
322		the EU Statement of Conformity shall state that:
323		[a] Appropriate measures were taken to fulfil the requirements related to the
324		composition of the Assessment Team (Req.3030); AND
325		[b] The objectives and requirements stated in the Component Cybersecurity
326		Profile are fulfilled; AND
327		[c] The Assessment Team reaches this conclusion after a Conformity Assessment
328		process that meets the requirements of the Assurance Level Basic
329	Req.3060	As soon as an EU Statement of Conformity for an IACS Component is issued, the
330		Component Manufacturer shall submit the EU Statement of Conformity to both ENISA
331		and the NCCA.Supervision.
332	Req.3070	The EU Statement of Conformity shall be part of the publicly available end-user
333		documentation.
334	Req.3080	Upon request, the Manufacturer shall provide the NCCA.Supervision with the
335		relevant information collected to issue the EU Statement of Conformity, including a
336		description of the measures taken to fulfil the requirements related to the
337		composition of the Assessment Team.
338	3.1.2 Third-party Assessment leading to an EU Cybersecurity Certificate	
339	Req.3090	The third-party assessment shall be performed by an accredited and authorized
340		Certification Body (CB).
341	Req.3100	The third-party assessment shall include all Evaluation Activities defined in Table 1 for
342		the targeted Assurance Level.
343	Note:	The Evaluation Activities assess whether the Components are secure by default and
344		by design to:
345		[a] At Assurance Level Basic, minimize the known Basic risks of cybersecurity
346		incidents and cyberattacks.
347		[b] At Assurance Level Substantial, minimize the known cybersecurity risks, and
348		the risk of cybersecurity incidents and cyberattacks carried out by actors with
349		limited skills and resources.
350		[c] At Assurance Level High, minimize the known cybersecurity risks, and the risk
351		of state-of-the-art cyberattacks carried out by actors with significant skills and
352		resources.

Req.3110 After collecting the necessary pieces of evidence, and successful completion of the assessment, the CB shall issue an EU Cybersecurity Certificate to the Manufacturer stating that:

- [a] The features stated in the Component Cybersecurity Profile are fulfilled; AND
- [b] The CB reaches this conclusion after a Conformity Assessment process that meets the requirements of the targeted Assurance Level (Basic, Substantial or High)

Req.3120 As soon as an EU Cybersecurity Certificate is issued, it shall be submitted by the CB both to ENISA and the NCCA.Supervision.

Req.3130 The EU Cybersecurity Certificate shall be part of the publicly available end-user documentation.

Req.3140 Upon request, the Manufacturer and the CB shall provide the NCCA.Supervision with the relevant information collected to issue the Cybersecurity Certificate.

3.2 Evaluation Activities

3.2.1 Evaluations Activities per Assurance Level

Table 1 lists the Evaluation Activities required per Assurance Level. Section 5 - Evaluation Activities for Assessment Teams provides a more detailed explanation of those activities.

CSA / ICCS Assurance Level	Evaluation Activities
Basic	<ul style="list-style-type: none"> [a] Component Cybersecurity Profile Evaluation [b] Documentation Review (Basic) [c] Installation, Configuration and Decommissioning Procedures Review
Substantial	<p>Additional Evaluation Activities required for the Assurance Level Substantial</p> <ul style="list-style-type: none"> [a] Documentation Review (Substantial) [b] Security Functions Testing [c] Vulnerability Analysis (Substantial)
High	<p>Additional Evaluation Activities required for the Assurance Level High</p> <ul style="list-style-type: none"> [a] Documentation Review (High) [b] Development Process Audit [c] Vulnerability Analysis (High) [d] Penetration Testing [e] Cryptographic Assessment

Table 1 - Mapping between the CSA Assurance Levels and the Evaluation Activities

3.2.2 Reuse of Non-ICCS Certificates

The term non-ICCS Certificates refers to Certificates that are not issued based on the ICCS.

ICCSGG- Req.0010	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define which third-party non-ICCS Certificates shall be reused by the CBs for performing specific Evaluation Activities.
-----------------------------	--

Req.3150 If i) a CuA has already received an independent third-party non-ICCS certification for a specific part of an individual ICCS requirement, and ii) this non-ICCS certification is formally acknowledged by the ICCSGG as a valid way of certifying that this part of the ICCS requirement is met, and iii) this non-ICCS certification applies to the version and scope of the CuA as these are described by the respective ICCS Component Cybersecurity Profile for this CuA, then the CB shall accept this non-ICCS Certificate as evidence that the concerned part of the ICCS requirement has been met.

Example:

The ICCS has defined that IEC 62443-4-1 Certificates shall be reused by the CBs to perform the Evaluation Activity of Development Process Audit (5.6).

An Applicant shall provide evidence to the CB that the scope of the Certificate applies to the Component development.

The CB shall verify the IEC 62443-4-1 Certificate and reuse it to certify that the CuA meets the requirements of the aforementioned Evaluation Activity.

3.2.3 Use of verifications tools

Req.3160 The ICCS is compatible with the use of verification tools that automate well-identified tasks either during the development of IACS Components or during the execution of Evaluation Activities.

Note: The use of verification tools can give confidence and can increase the productivity of the development of the Components. Verification tools allow to execute tasks in a systematic and reproducible way. Verification tools implement formal models, languages, syntax and semantic in tasks such as specification, design, evidence collection, etc. Verification tools can be used to manage requirements, to model architectures (with multiple layers of design), to verify source code, to compile code, to perform fuzz testing or regression testing. They provide non-ambiguous results that can be used in following tasks or for quality control.

Req.3170 In case verification tools are used, the user shall document:

[a] How verification tools are used to automate a task (scope, metrics, pass/fail criteria); AND

[b] How their use is validated to ensure they are fit for purpose.

397 **3.3 EU Cybersecurity Certificates and EU Statements of Conformity**

ICCSGG- Req.0020	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define validity periods for the EU Cybersecurity Certificates and the EU Statements of Conformity.
-----------------------------	--

398

ICCSGG- Req.0030	<p>The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define the format of EU Cybersecurity Certificates and of EU Statements of Conformity to ensure that end-users can:</p> <ul style="list-style-type: none">[a] Easily differentiate EU Cybersecurity Certificates from EU Statements of Conformity;[b] Recognize the Assurance Level of the EU Cybersecurity Certificates;[c] Compare the security features of the Components;[d] Unambiguously identify the version of the Component under Evaluation (CuA) that has been awarded an EU Cybersecurity Certificate or an EU Statement of Conformity.
-----------------------------	---

399 **Note:** Sections 7.3 and 7.4 provide recommendations for the contents of EU Cybersecurity
400 Certificates and EU Statements of Conformity.

401

402

4 Elements from the Applicant

The elements from the Applicant are the objects, documents or pieces of information that the Applicant must provide to the Certification Body or Assessment Team.

4.1 Elements Necessary for Assessment (ENA)

Req.4010 Depending on the targeted Assurance Level, the Applicant shall provide the ENA listed in Table 2.

Targeted Assurance Level	Elements Necessary for Assessment (ENA)
Basic	<ul style="list-style-type: none">[a] Component Cybersecurity Profile (CCP)[b] End-user guidance and recommendations[c] Development process documentation including:<ul style="list-style-type: none">○ Vulnerability management procedure○ Patch and obsolescence management procedure○ Internal cybersecurity knowledge management procedure○ Secure by default and by design strategy[d] Component under Assessment (CuA)
Substantial	<p>Additional ENA required for the Assurance Level Substantial</p> <ul style="list-style-type: none">[a] Development process documentation including:<ul style="list-style-type: none">○ Configuration management○ Life-cycle definition○ Incident handlings plan[b] Robustness testing documentation[c] Design documentation:<ul style="list-style-type: none">○ Interfaces description○ List of parts of the Component under Assessment (CuA)
High	<p>Additional ENA required for the Assurance Level High</p> <ul style="list-style-type: none">[a] Internal Design documentation[b] Cryptography Information[c] Access to the development team, the development site and the manufacturing sites shall be provided

Table 2 - Mapping between the CSA Assurance Levels and the ENA

Req.4020 ENA shall be available to CBs during the assessment, and available to NCCA.Supervision during the whole validity period of the EU Cybersecurity Certificate or EU Statement of Conformity.

4.2 Component Cybersecurity Profile (CCP)

414	Req.4030	Each cybersecurity assessment of an IACS Component shall be based on a Component Cybersecurity Profile (CCP) which will be specific to the Component.
415		
416	Req.4040	The security properties and the expected operating environment of the Component shall be described in a CCP document.
417		
418	Note:	A mapping of the CCP, gCCA, CCA and CCR to various standards is given in Annex D.
419	Req.4050	The Component Cybersecurity Profile (CCP) shall be composed of:
420		[a] The definition of the Component under Assessment (CuA);
421		[b] Component Context Analysis (CCA);
422		[c] Component Cybersecurity Requirements (CCR).
423		
424	Req.4060	The definition of the CuA shall be precise as it is determining the scope of the assessment.
425		
426		
427	Req.4070	The CCA shall be composed of the:
428		[a] Description of the intended use and the intended operational environment;
429		[b] Description of the assets included in the Component;
430		[c] Description of the threats applicable to the assets in the intended operational environment;
431		
432		[d] Description of the Security Objectives to be fulfilled by the Component written in natural language;
433		
434		[e] Rationale for the Security Objectives.
435		The CCA can optionally be based on a generic CCA (gCCA).
436		
437	Note:	If a gCCA exists and is suitable for an IACS Component, its CCA may be based on the gCCA.
438		
439	Req.4080	If the Applicant decides to use a gCCA, it shall serve as a template to write a CCP for a given Component of the same family. In this case all the contents of the gCCA shall be present in the CCP. The CCP may extend the security requirements of the gCCA that it is based on.
440		
441		
442		
443	Req.4090	The CCR shall be composed of the:
444		[a] Set of security requirements fulfilled by the Component;
445		[b] Rationale for the security requirements;
446		[c] Implementation decisions (Security Functions) for fulfilling the security requirements.
447		
448	Req.4100	The Security Functions needed to reduce Residual Threats shall be selected according to the risk analysis, ensuring that all assets are protected and threats mitigated by a combination of the Security Functions and the security assumptions of the intended operational environment.
449		
450		
451		

452	Req.4110	For each part of the CuA, the security characteristics to be met and the associated
453		asset(s) shall be listed.
454	Req.4120	Threats shall be identified through a risk analysis.
455	Note:	Risk analysis should include the identification of measures that reduce security risks
456		faced by critical assets. The threats should also be prioritised depending on the
457		criticality.
458	Req.4130	For each critical asset, there shall be documented in the CCA/gCCA any (zero or
459		several) assumptions resulting from the intended use (CCA) or generic intended use
460		(gCCA) and operational environment and how these assumptions reduce threats
461		against the critical assets.
462	Req.4140	The set of assumptions associated with a critical asset shall leave only Residual
463		Threats.
464	Note:	A risk analysis may conclude to the management of only a subset of all Residual
465		Threats depending on factors such as their likelihood or potential impacts if
466		materialised into incidents, for instance. Unaddressed Residual Threats constitute
467		accepted known risks. Residual Threat(s) on a critical asset require implementation
468		decisions (Security Functions) to be documented in the CCR.
469	Req.4150	A generic CCA (gCCA) can be defined for a family of IACS Components. The gCCA shall
470		be a generic description for a selected family of IACS Components.
471	Note:	From a purchaser's perspective, a gCCA can serve as a reference: if the CCP of the
472		certified Component is based on the same gCCA with other Components, these
473		different Components can be better compared. Also, a gCCA can be used to establish
474		a minimum set of Security Objectives or requirements for a family of Components.
475	Note:	From a Manufacturer's perspective, a gCCA can give a reference of Security Objectives
476		that could be considered for the development of their respective Components.
477	Req.4160	The gCCA shall be composed of the:
478		[a] Description of the generic intended use and the generic intended operational
479		environment for the family of IACS Components;
480		[b] Description of the assets included in the family of IACS Components;
481		[c] Description of the threats applicable to the assets in the generic intended use
482		and the generic operational environment;
483		[d] Description of the Security Objectives to be fulfilled by the family of IACS
484		Components written in natural language;
485		[e] Rationale for the Security Objectives.
486		[f] Set of generic security requirements for the family of IACS Components
487		○ This is optional

488 **Note:** The gCCA could be written in an agnostic form allowing compatibility to the different
489 paths/alternative identified by the ICCS scheme.

490 **Req.4170** The gCCAs shall give special consideration to interoperability aspects for security
491 related functionality, e.g. protocols.

492 **Req.4180** The motivation of a gCCA shall be described including market relevance, technical
493 maturity, existence of several independent Manufacturers, relevance of scope of the
494 gCCA in the overall certification market.

495 **4.3 Contents of the Documentation**

ICCSGG- Req.0040	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define the contents and expected level of details (and possibly examples) of the documents referenced in this Section.
-----------------------------	--

496 **4.3.1 Assurance Level Basic**

497 **Req.4190** The end-user guidance and recommendations shall include, if applicable:

498 [a] The Integration guidelines (including the defence-in-depth protection strategy,
499 secure usage recommendations, and security measures expected in the
500 operational environment of the Component);

501 [b] The Hardening Guidelines;

502 [c] The Backup & Restore guidelines;

503 [d] The End-user incident handling guidelines;

504 [e] The Decommissioning guidelines;

505 [f] The Cybersecurity Monitoring guidelines (including the procedure to configure
506 and review the security logs);

507 [g] The Vulnerability Management & Patch Management guidelines.

508 **Note:** The end-user guidance and recommendations have the purpose to assist end-users
509 with the secure configuration, installation, deployment, operation, maintenance, and
510 decommissioning of the Component.

511 **Req.4200** The Vulnerability Management procedure shall include:

512 [a] Internal Procedure for Continuous monitoring of known vulnerabilities (CVEs
513 and other relevant sources);

514 [b] Contact information of the Manufacturer or provider and accepted methods
515 for receiving vulnerability information from end-users and security
516 researchers;

517 [c] A reference to publicly disclosed vulnerabilities related to the Component and
518 to any relevant cybersecurity advisories.

519 **Note:** The Vulnerability Management procedure shall take into account the cases where a
520 certified Component is dependent on other Components that have their own
521 vulnerability handling processes.

- 522 **Req.4210** The Patch and Obsolescence Management procedure shall:
- 523 [a] Identify how, when and why updates are applied to the CuA;
- 524 [b] Define process(es) by which updates are notified and communicated to end-
- 525 user, how updates are delivered, how they are authenticated and authorised,
- 526 how they are applied and (where appropriate) how they are tested before
- 527 being rolled out;
- 528 [c] Ensure that the updates for different parts of the CuA (if applicable) are
- 529 compatible and whether they need to be rolled-out simultaneously or in a
- 530 specific order;
- 531 [d] Specify what to do when parts (hardware or software) are no longer
- 532 supported, reflecting the need to avoid situations where hardware spares may
- 533 become difficult to obtain, or software updates may no longer be available to
- 534 patch discovered vulnerabilities;
- 535 [e] Define the period during which security support will be offered to end-users,
- 536 in particular as regards the availability of cybersecurity related updates.
- 537 **Req.4220** The Internal Cybersecurity Knowledge Management procedure shall include:
- 538 [a] A description of the process to maintain development team knowledge
- 539 (including the security team) at the right level of expertise (skills and training)
- 540 to develop secure Components.
- 541 **Req.4230** The Secure by Default and by Design strategy shall include:
- 542 [a] The secure by default development procedures;
- 543 [b] The defence-in-depth protection strategy;
- 544 [c] A description of the mechanism implemented by the Component for secure
- 545 updates.

ICCSGG- Req.0050	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall be in charge of identifying suitable standards to meet the Secure by default and by design strategy that is mandatory for all the CSA schemes. Standards will strengthen the assessment of a 'secure by default and by design strategy' for a Component, consistently, and with strong relevance to meeting CSA's Art.52 requirements.
-----------------------------	--

546

Example of Secure by default and by design requirements:

- [a] No universal default passwords;
- [b] Keep software updated securely;
- [c] Securely store and deletion of sensitive security parameters;
- [d] Communicate securely;
- [e] Minimise exposed attack surfaces;
- [f] Ensure software integrity;
- [g] Ensure that personal data is protected;

- [h] Make systems resilient to outages;
- [i] Make installation and maintenance of devices easy;
- [j] Provide security documentation and guidance;
- [k] Validate input data.

4.3.2 Assurance level Substantial

Req.4240 In addition to the documentation required at Assurance Level Basic, at Assurance Level Substantial the product development/maintenance/support process shall be documented and it should be ensured that is consistent with the product development processes accepted by the ICCS.

Req.4250 The documentation of the product development/maintenance/support shall include at minimum:

- [a] Configuration management with access control, audit logging and a review/approval mechanism for all the changes (including the process of generation of the software parts);
- [b] Life-cycle Definition including specifying all the sites involved in the development and the activities carried out at each site;
- [c] Incident handling plans, procedures and evidences. It is expected that an incident handling mechanism is in place to handle incidents that occur during the development/production of the Component. It is not expected to include the handling of incidents during operation.

ICCSGG-Req.0060 The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group will define the product development processes' specifications against which ICCS assessments can be made. These requirements may evolve both through science, technology and practice (e.g. standards).

Req.4260 The Robustness Testing documentation shall include:

- [a] The description of the security review and test processes applied during the development process including:
 - Coverage of Security Functions;
 - Tests designed to demonstrate suitable security behaviour when encountering unusual conditions (including malformed or other invalid inputs).
- [b] The rationale of the criteria used to judge when sufficient security testing that has been defined and executed for Component versions and updates (including patches).

Note: Robustness testing activities themselves (including the provisioning of pieces of evidence) shall be carried out by the Applicant and reviewed by the Assessment Team. If the Assessment Team identifies missing coverage, it may conduct independent testing instead of failing this Evaluation Activity.

ICCSGG- Req.0070	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall be in charge of defining the specific robustness testing activities to be carried out and the methods/tools to be used.
-----------------------------	---

Req.4270 The Interface Description shall document all the interfaces of the CuA with a level of detail that allows a tester to test the external interfaces knowing all the parameters, return values and error messages. The interface shall be described even if a third-party library is used for implementing the interface.

Req.4280 The list of parts of the Component shall include all relevant internal parts of the CuA.

Note: Details such as version number and end-of-support/end-of-production dates should be provided.

4.3.3 Assurance level High

Req.4290 In addition to the documentation required at Assurance Level Substantial, at Assurance Level High the internal design documentation shall include:

- [a] Documentation describing how cybersecurity features stated in the Component Cybersecurity Profile are implemented;
- [b] Security Architecture documentation and its relation to the defence-in-depth strategy, as this is explained in the end-user documentation shall be provided;
- [c] Description of the cryptographic algorithms in use.

4.4 Publicly Available End-User Documentation

Req.4300 The following elements shall be part of the publicly available end-user documentation:

- [a] The EU Cybersecurity Certificate or the EU Statement of Conformity;
- [b] The Component Cybersecurity Profile of the Component;
- [c] The end-user guidance and recommendations as specified in Req.4400;
- [d] The period during which support shall be offered to end-users, in particular as regards the availability of cybersecurity related updates;
- [e] The information related to the communication of cybersecurity-related updates to the end-users;
- [f] A reference to publicly disclosed vulnerabilities related to the Component and to any relevant cybersecurity advisories;
- [g] Contact information of the Manufacturer along with accepted methods for receiving vulnerability information from end-users and security researchers.

Note: The end-user guidance and recommendations have the purpose to assist end-users with the secure configuration, installation, deployment, operation, maintenance, and decommissioning of the Component.

612 **Req.4310** Additional ENA shall be part of the end-user documentation if they can help to better
613 secure the Component.

614 **Req.4320** End-user documentation listed in this Section shall be made publicly available in
615 electronic form, and shall remain available and updated until the expiry of the
616 corresponding EU Cybersecurity Certificate or EU Statement of Conformity.

617

5 Evaluation Activities for Assessment Teams

The IACS Components Cybersecurity Certification Scheme (ICCS) defines different Evaluation Activities. A certification scheme has to rely on standards that specify the Evaluation Methodology to assess if a Component under Assessment (CuA) meets the specific criteria/requirements determined by the standard or the ICCS itself.

At the moment of delivery of this report, there is no single standard that adequately covers the whole set of the Evaluation Activities defined by the ICCS as necessary to evaluate IACS Components. Therefore, references to applicable standards have been included.

For IEC 62443-4-2, currently, no standardized and public Evaluation Methodology (EM) exists. To fill this gap in the IEC 62443 series, the IT Security Association Germany (TeleTrust) has developed an Evaluation Methodology (<https://www.teletrust.de/publikationen/iec-62443-4-2-pruefschema/>), which is publicly available. Also, at the moment of writing this report, there are ongoing activities at IEC/IECEE regarding evaluation methodologies addressing IEC 62443-4-2 and some initial documents are expected to be published in the very near future.

For ISO/IEC 15408:2008, the Evaluation Methodology has to be ISO/IEC 18045:2008.

Several Lightweight evaluation methodologies exist at national level, such as the French CSPN, the Spanish LINCE or the German BSZ. However, no harmonized Evaluation Methodology currently exists at an EU level. Such an EU Evaluation Methodology may be devised for example by CEN/Cenelec JTC13 WG3, which is working on a project called “Cybersecurity Evaluation Methodology for ICT products” that could be used as a basis.

The set of Evaluation Activities that have to be carried out by the Assessment Teams are presented in detail in the following Subsections. Each Subsection provides an overall description of the Evaluation Activity along with a detailed analysis of the Evaluation Work Units that comprise it. Unless otherwise indicated, all these Evaluation Activities have to be performed by the TestLab/CB.

ICCSGG-Req.0080	The ICCSGG Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall review the situation of the evaluation standards and propose the most suitable one(s) when defining the ICCS. It will be the responsibility of the governance group to determine the evaluation methods to be chosen. The ICCSGG shall define at least one Evaluation Methodology while there should be laid emphasis on achieving the maximum possible reuse of applicable standards.
------------------------	--

5.1 Component Cybersecurity Profile Evaluation

5.1.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to verify that the Component Cybersecurity Profile is sound, consistent and suitable as the basis for the Evaluation Activities to be carried out by the Assessment Teams.

647 **5.1.2 Evaluation Work Units**

648 **Req.5010** The Assessment Team shall check that the Component Cybersecurity Profile follows
649 the structural requirements stated by the ICCS.

ICCSGG- Req.0090	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall devise a template for the Component Cybersecurity Profile (CCP) based on the requirements in Section 6.3.1 - Elaboration of Component Cybersecurity Profiles (CCP).
-----------------------------	---

650

651 **Req.5020** The Assessment Team shall review that the Component Cybersecurity Profile is
652 understandable by the potential end-customers.

653 **Req.5030** The Assessment Team shall verify that the information in the Component
654 Cybersecurity Profile is free of contradictions within the context of CCP itself as well
655 as free of inconsistencies with respect to other information provided along the ENA,
656 especially the end-user documentation and the overview of the design.

657 **Req.5040** The Assessment Team shall verify that the Component Cybersecurity Profile specifies
658 the Assurance Level: i.e. Basic, Substantial or High.

659 **Req.5050** The Assessment Team shall confirm that the boundaries of the CuA and the
660 boundaries of the evaluation are clearly and unambiguously defined in the
661 Component Cybersecurity Profile.

662 **Req.5060** The Assessment Team shall verify that the Component Cybersecurity Profile describes
663 Security Functions relevant for the intended use.

664 **Req.5070** The Assessment Team shall verify that all claimed Security Functions are clearly
665 tested.

666 **Req.5080** The Assessment Team shall confirm that the assumptions stated in the Component
667 Cybersecurity Profile are realistic for the intended use of the CuA.

668 **Req.5090** The Assessment Team shall confirm that the set of attackers/threats are realistic and
669 understandable considering the intended use of the CuA and that they are aligned
670 with the assumed attackers for the chosen Assurance Level.

671 **Req.5100** The Assessment Team shall check that the assets protected by the CuA are
672 understandable.

673 **Req.5110** The Assessment Team shall check that there is consistency among assets, threats,
674 Security Objectives and Security Functions.

675 **Req.5120** The Assessment Team shall verify that the Component Cybersecurity Profile specifies
676 the cryptographic mechanisms used by the CuA.

Note: The main cryptographic parameters (e.g. TLS version) that are available on external interfaces or accessible by potential attackers need to be provided by the Applicant as part of the ENA, so as to verify that obsoleted (vulnerable) cryptographic parameters are no longer used. Implementation details or low-level parameters of the cryptographic mechanisms are not required to be provided.

Req.5130 In case the Applicant claims conformance to a generic Component Context Analysis, the Assessment Team shall review the conformity of the Component Context Analysis to the generic Component Context Analysis.

Req.5140 If the CCP is not validated by the Assessment Team, detailed explanations about the reasons shall be provided by the Assessment Team to the Applicant. The Applicants shall be offered with the opportunity to defend their position in order, if possible, to reach an agreement about the CCP with the Assessment Team.

5.2 Documentation Review

5.2.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to assess the completeness, coherency, consistency and correctness of the documentation and evidence that the Assessment Team has been provided with.

Example of assurance activity:

The Assessment Team shall check the design documentation to ensure that it describes how the Component chooses which Certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the Component can use the Certificates. The Assessment Team shall examine the design documentation to confirm that it describes the behaviour of the Component when a connection cannot be established during the validity check of a Certificate used in establishing a trusted channel. The Assessment Team shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the Assessment Team shall ensure that the operational guidance contains instructions on how this configuration action is performed.

ICCSGG-Req.0100 The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall be in charge of defining the set of Pass/Fail criteria. Section 4.1 provides recommendations for the documentation that shall be required by the Applicant for each Assurance Level. The documentation required for each Assurance Level should be reviewed by the aforementioned ENISA Ad hoc Working Group.

5.2.2 Evaluation Work Units

Req.5150 The TestLabs/CBs shall review the requested documentation and ensure that it meets the content requirements as specified in Sections 4.2 and 4.3. For any of the documentation requirements, if the specified criterion is not met, the Applicant shall provide further evidences upon request by the Assessment Team.

700 5.2.2.1 *Assurance Level Basic*

701 **Req.5160** The documents specified in Section 4.3.1 shall be requested for the Assurance Level

702 Basic.

703 5.2.2.2 *Assurance Level Substantial*

704 **Req.5170** The documents specified in Section 4.3.2 shall be requested for the Assurance Level

705 Substantial, in addition to the documentation required for the Assurance Level Basic.

706 5.2.2.3 *Assurance Level High*

707 **Req.5180** The documents specified in Section 4.3.3 shall be requested for the Assurance Level

708 High, in addition to the documentation required for the Assurance Level Substantial.

709 **5.3 Installation, Configuration and Decommissioning Procedures Review**

710 **5.3.1 General Evaluation Activity Description**

711 The aim of this Evaluation Activity is to verify that the installation, configuration and

712 decommissioning steps are clear, reasonable and yield a functioning and cybersecure Component.

713 **5.3.2 Evaluation Work Units**

714 **Req.5190** The Assessment Team shall verify (by testing) that the CuA can be installed and

715 configured as described in the end-user documentation. No access to the

716 documented information besides the end-user documentation shall be required.

717 **Note:** At Assessment Level Basic, the Assessment Team may verify by witnessing that the

718 steps can be executed following the applicable guidance. A review of logs is not

719 considered a valid mean to fulfil this activity.

720 **Req.5200** The Assessment Team shall check that all supporting systems necessary to operate

721 the CuA are present and correctly set up. The setup of these additional systems might

722 be carried out together with the Applicant and it is itself not part of the evaluation.

723 The evaluation shall not proceed until the setup of the aforementioned additional

724 systems, if any, has been completed successfully.

Example:

The CuA needs a backend cloud service. In this case, the developer needs to provide test accounts or a local (working) cloud installation to the Assessment Team.

725

726 **Req.5210** The Assessment Team shall verify that the security configuration settings of the CuA

727 are applied.

728 **Req.5220** The Assessment Team shall determine how hard it is not to apply the security

729 configuration settings.

730 **Note:** A possible way would be to expose a warning to the user if the security configuration

731 settings are not applied.

732 **Req.5230** The Assessment Team shall follow the decommissioning steps and verify that it is
733 possible to carry them out in a secure manner.

734 **5.4 Security Functions Testing**

735 **5.4.1 General Evaluation Activity Description**

736 The aim of this Evaluation Activity is to carry out the conformity testing of the Component.

737 The Evaluation Activities to be undertaken shall include at least the necessary tests to demonstrate
738 that the Component correctly implements the Security Functions stated in the Component
739 Cybersecurity Profile.

ICCSGG- Req.0110	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall be in charge of producing supporting documents to ensure the alignment of the various Assessment Teams that are active within the framework of the ICCS (as it is used for Cybersecurity Certification evaluations in the SOG-IS community) and increase the confidence that evaluations carried out by different Assessment Teams are consistent and reach the same results.
-----------------------------	---

740

741 **Note:** The usage of supporting documents facilitates the repeatability and harmonization
742 across the Assessment Teams. As the creation of supporting documents requires
743 significant resources, it is expected to be completed in due time, i.e. the supporting
744 documents will be written while the ICCS is already operating.

Example of testing activity:

Test 1: The Assessment Team shall use the test environment to deploy policies to the Component.

Test 2: The Assessment Team shall create policies which collectively include all management functions, and which are controlled by the (enterprise) administrator and cannot be overridden/relaxed by the user. The Assessment Team shall apply these policies to the Component, attempt to override/relax each setting both as the user (if a setting is available) and as an application (if an API is available), and ensure that the Component does not permit it. Note that the user may still apply a more restrictive policy than that of the administrator.

745

746 **5.4.2 Evaluation Work Units**

747 **Req.5240** For each security requirement defined in the Component Cybersecurity Profile, the
748 Assessment Team shall perform tests. The Assessment Team shall attempt to find
749 non-conformities of the CuA with respect to the security requirements. The test cases
750 for each security requirement shall be defined by setting up a risk-based sampling
751 strategy, taking into account previous evaluation results, the entire documentation
752 received for the CuA, information received from the ICCS (e.g. supporting documents
753 and guidance) and the experience with similar CuAs. For each sampled security

754 requirement (or part thereof) the Assessment Team shall employ the test case
755 derivation procedure given in the following Req. For each failed conformity test, the
756 Assessment Team shall review the reasons for the failure and inform the Applicant.

757 **Req.5250** The process model for transforming requirements into test cases consists of the
758 following steps:

759 [a] Identify the technical (testable) security characteristics of each claimed security
760 requirement of the CuA;

761 [b] For each security characteristics define an acceptance criterion, i.e. the result(s)
762 necessary to achieve the Security Objectives of this characteristic;

763 [c] Define a test case for this characteristic.

764 If the result of the test case fulfils the acceptance criterion, this will contribute to a
765 positive result for this Evaluation Work Unit. If the test result deviates, then the result
766 of this Evaluation Work Unit will be negative (fail).

767 If no test case can be specified for a security requirement (e.g. if one implementation
768 detail cannot be addressed via an external interface), an alternative proof of correct
769 implementation shall be given. This can be done as part of a different evaluation
770 method.

771 **Req.5260** A test case shall be defined including at least the following characteristics:

772 [a] Test description with test expectation, test preparation, test environment and
773 testing steps;

774 [b] Test result;

775 [c] Assessment (pass/fail).

776 The test expectation is the expected test result, which will occur if the Component
777 functions correctly. The test expectation shall result from the Component's intended
778 behaviour and the acceptance criteria. The test result is the actually detected
779 behaviour of the Component during the testing steps.

780 **Req.5270** Where no verification testing tool exists, the given functional security requirements
781 for the CuA shall be transferred into test cases by the tester.

782 **Req.5280** The Assessment Team shall use verification tools where possible to perform the
783 Security Functions testing. The Assessment Team shall justify how the tools are
784 validated to ensure their fit for purpose.

785 **Req.5290** The Assessment Team shall record the testing strategy and the results.

786 **5.5 Vulnerability Analysis**

5.5.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to determine the existence and exploitability of security flaws or weaknesses (i.e. security vulnerabilities) in the CuA. This analysis will be carried out by the Assessment Team using public sources and the ENA listed in Table 2.

5.5.2 Evaluation Work Units

5.5.2.1 Assurance Level Substantial

The aim of this Evaluation Activity is to verify that the CuA is not vulnerable to publicly known vulnerabilities and to ensure that the Defence-in-depth protection strategy is consistent.

ICCSGG-Req.0120	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall provide/maintain a list of sources of potential vulnerabilities (and associated tests) as input for this task.
------------------------	--

Req.5300 The following activities shall be carried out at Substantial level:

[a] Verify (by analysis) the absence of known vulnerabilities in the CuA

○ This process implies the following steps:

- Identify the CuA parts (e.g. programs, libraries and tools);
- Search for known vulnerabilities in respective public databases (e.g. CVE);
- Review whether there are outdated Components that may contain vulnerabilities. In such a case, there should be reviewed whether additional security mechanisms are in place, which prevent the exploitation of these vulnerabilities. The Applicant shall provide evidence that the vulnerabilities are not exploitable.

Example:

A library used by the CuA may contain a parsing flaw when encountering certain input yielding in an unintended behaviour. This should not be relevant, if the Manufacturer implemented a filter for all input, so that only valid input is forwarded to this actual library.

[b] High-level review (by analysis) of the security architecture to ensure that it is consistent with the Defence-in-depth protection strategy

○ This process implies the following steps:

- Analyse of the available evidences (public and proprietary);
- Identify whether there are exploitable vulnerabilities in the CuA.

Note: The term “by analysis” means that testing is not expected but it is still considered as a possibility. Other means which can be used are static code analysis or vulnerability scanners.

5.5.2.2 Assurance Level High

The aim of this Evaluation Activity is to verify that the CuA is not vulnerable to publicly known vulnerabilities, identify potential vulnerabilities that are applicable for the CuA and analyse if the CuA configuration introduces vulnerabilities in the host system.

Req.5310 The following activities shall be carried out in the case of Assessment Level High, in addition to the ones required for the Assessment Level Substantial:

[a] Extended search for vulnerabilities:

○ This process implies the following steps:

- Analysis of the available evidences (public and proprietary) including the security architecture;
- Identifying of potential vulnerabilities taken into account the CuA and the technology. Vulnerabilities from similar CuAs may be used to identify attack paths and potential vulnerabilities;
- Devise a Penetration Test plan.

Note: The expertise and knowledge of the Assessment Team in the CuA technology is a key factor for the successful completion of this Evaluation Activity.

[b] Host system vulnerability analysis (if applicable)

○ This activity is carried out to show that the CuA does not add attack surfaces to the host.

Example:

If an industrial device has wireless connectivity, it adds a wireless entry point into the industrial network, which can be leveraged by an attacker. Basically, the host system vulnerability analysis addresses the risk that the evaluated CuA creates a potential threat on other assets than those described in the Component Cybersecurity Profile.

Req.5320 The Vulnerability Analysis activity shall be carried out as a complement to Penetration Testing activity. The results of one activity shall feed the other activity to enhance the outcome of both.

ICCSGG-Req.0130 The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define the supporting documents/attack catalogues to ensure the alignment of the various Assessment Teams when carrying out this Evaluation Activity and increase the confidence that the evaluations carried out by different Assessment Teams are consistent and reach the same results. E.g. OWASP Testing Guides, MITRE CAPEC etc. This should be an evolving work, which, after the establishment of the ICCS, shall be taken over by the ICCSGG.

ICCSGG-Req.0140	The ICCS Governance Group (ICCSGG) or the respective ENISA Ad hoc Working Group shall define requirements regarding the expertise and knowledge of the Assessment Team in relation to the CuA technology.
------------------------	---

5.6 Development Process Audit

5.6.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to verify that the development processes are operational, they comply with the relevant scheme requirements and they are implemented as explained in the documentation.

This assessment is carried out through an audit.

ICCSGG-Req.0150	The ICCSGG or the respective ENISA Ad hoc Working Group shall define the most suitable standard to audit the development sites of IACS Components. Once the standard(s) is chosen, the Evaluation Work Units will be updated.
------------------------	---

5.6.2 Evaluation Work Units

Note: The development process documents are verified by the Assessment Team as part of the Evaluation Activity 5.2.

Req.5330 The Assessment Team shall confirm by audit that the process followed in practice by the Applicant complies with the development process described in the documentation and the process aspects defined by the ICCS for the Assurance Level stated in the CCP.

ICCSGG-Req.0160	The ICCSGG or the respective ENISA Ad hoc Working Group shall define the process aspects to be met by the Manufacturer in the development process for the ICCS.
------------------------	---

Req.5340 The Assessment Team shall audit the development environment security measures and their sufficiency to protect the authenticity, integrity and, where applicable, the confidentiality of the critical items in the development environment.

Req.5350 The Assessment Team shall be provided with access to the development team, the development site and the manufacturing sites.

5.7 Penetration Testing

5.7.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to confirm whether the potential vulnerabilities identified during the Vulnerability Analysis activity are exploitable or not. To this end a sampling testing strategy based on the flaw hypothesis methodology needs to be devised and applied, so as to conclude that the CuA does not contain exploitable vulnerabilities from the class of known vulnerabilities.

Penetration testing is the simulation of a real-world attack on the CuA. It does not necessarily require a full exploitation of vulnerabilities, but still requires the Assessment Team to assess whether an attack scenario is likely or not in the defined operational environment, given the attacker's supposed skills and resources. It may include attacks against the IACS hardware or software depending on the definition of the Component Cybersecurity Profile.

A penetration testing typically exploits several kinds of vulnerabilities, e.g.:

- [a] Conceptual vulnerabilities (e.g. bad cryptography or badly designed protocols);
- [b] Implementation errors (lack of adherence to a specification, incorrect implementations, or unsafe implementations such as a lack of bounds checking leading to a buffer overflow);
- [c] Persistence of privileged test features (e.g. privileged accounts, debug interfaces);
- [d] Lack of adherence to the state-of-the-art (e.g. time-of-computations leakage allowing side channel attacks, inappropriate code obfuscation, lack of appropriate countermeasures when using a vulnerable technology).

ICCSGG-Req.0170	The ICCSGG or the respective ENISA Ad hoc Working Group shall define precisely how the penetration testing shall be carried out as part of the ICCS (e.g. setting a minimum workload or defining specific guidelines). It is recommended that the aforementioned ENISA Ad hoc Working Group already defines a baseline or an initial version of this workload.
------------------------	--

ICCSGG-Req.0180	The ICCSGG or the respective ENISA Ad hoc Working Group shall define the methodology (e.g. attack potential calculation) for assessing whether a vulnerability can safely be considered as not applicable or beyond the attack potential (e.g. the expected resistance shall be clearly defined).
------------------------	---

5.7.2 Evaluation Work Units

Req.5360 The Assessment Team shall verify the resistance of the Security Functions and the protection of the sensitive assets as identified in the Component Cybersecurity Profile. The input to carry out this activity shall be the penetration testing plan that shall be executed to measure the resistance of the Security Functions and sensitive assets.

Req.5370 The Assessment Team shall assess, during the penetration testing activity, that the operation of the sensitive functionalities is ensured and that they keep functioning as stated by the Applicant when the CuA is under attack. The Assessment Team shall verify that, under attack, the Security Functions listed in the CCP work properly or in a degraded mode (if specifically defined as such by the Applicant).

Example:

If the confidentiality of the firmware is an asset: “the goal is to make sure that there is no way to disclose it”.

Req.5380 The Assessment Team shall attempt to bypass the Security Functions of the CuA. For this the Assessment Team shall set up a risk-based sampling strategy, taking into account publicly known vulnerability/vulnerability classes, previous evaluation results, information received from the ICCS, and the experience with similar CuAs. The Assessment Team shall also employ the ENA received for the CuA to further devise the testing strategy.

5.8 Cryptographic Assessment

5.8.1 General Evaluation Activity Description

The aim of this Evaluation Activity is to assess the cryptographic implementations included in the Component.

Cryptographic assessments may be conducted in different manners and with different depths of testing.

Two different approaches may be followed when assessing a cryptographic implementation:

- **Cryptographic Conformity:** The aim of this Evaluation Activity is to validate that the cryptography used complies with the cryptographic specification stated in the Component Cybersecurity Profile. This task is a probabilistic conformance testing tailored to cryptographic protocols and algorithms.
- **Cryptographic Analysis:** The aim of this Evaluation Activity is to validate that the cryptography used complies with the cryptographic specification stated in the Component Cybersecurity Profile and analyse the cryptographic algorithm implementation in depth to ensure that there are no exploitable vulnerabilities.

ICCSGG-Req.0190 At the time that this report is written, due to the maturity of the cybersecurity of industrial Components, it is considered as more appropriate to require Cryptographic Conformity. Nonetheless, the ICCSGG or the respective ENISA Ad hoc Working Group shall review the state of the art in cryptographic analysis periodically and update the requirements accordingly. The work carried out by dedicated working groups such as SOG-IS shall be taken into account.

5.8.2 Evaluation Work Units

Req.5390 The Assessment Team shall attempt to find nonconformities of the CuA with respect to the cryptographic requirements specified in the Component Cybersecurity Profile.

919 The Assessment Team shall use validated tools and standardised test vectors where
920 possible to complete this task.

Example:

If properties on an interface are claimed to be random, a suitable tool can check if obvious defects in the random number generator or processor exist.

921

922 **Req.5400** The Assessment Team shall further employ the entire documentation received for the
923 CuA as well as the ICCS documents with respect to cryptography.

**ICCSGG-
Req.0200**

The ICCSGG or the respective ENISA Ad hoc Working Group shall define the allowed cryptographic mechanisms.

924

925 **Req.5410** The Assessment Team shall carry out Cryptographic Conformity testing as follows (if
926 applicable):

- 927 [a] Positive test cases for cryptographic algorithms and schemes shall comprise
928 randomly generated known-answer tests and iterated Monte-Carlo tests if
929 applicable. The test vectors shall be standardized where possible, otherwise the
930 test vectors shall be generated or verified by an independent, known-good
931 implementation and shall not be static. Algorithms accepting variable-length
932 inputs shall be tested with inputs of different lengths (including border cases
933 like length zero);
- 934 [b] Positive testing of cryptographic protocols shall be done by communicating with
935 an independent, known-good implementation. The cryptographic algorithms
936 and schemes used by the protocol shall be tested separately as described above;
- 937 [c] Negative test cases for cryptographic algorithms and schemes shall be
938 specifically crafted to trigger certain error conditions (e.g. illegal-value errors,
939 out-of-bounds errors, padding errors, etc.);
- 940 [d] Negative testing of cryptographic protocols shall comprise test cases for
941 unspecified configurations (unspecified ciphers, protocol version downgrade,
942 etc.), test cases for illegal inputs (e.g. malformed packets, oversized packets,
943 etc.), and test cases for illegal transitions in the protocol's state machine (e.g.
944 insertion of unexpected packets, omission of required packets, etc.);
- 945 [e] Random sources shall be tested using a statistical test suite according to
946 relevant standards;
- 947 [f] If certain algorithms, interfaces or cryptographic mechanisms have not been
948 analysed during sampling, the Assessment Team shall provide a justification for
949 this.

950

6 Evaluation and Certification Processes

6.1 Stakeholders and their Relationships

In this Section, the main actors of the IACS Cybersecurity Certification Scheme (ICCS) and the relevant actors foreseen by the CyberSecurity Act (CSA) along with their relationships are illustrated using conceptual models. The models are either derived from the text of CSA or represent the roles and relationships that are specific to the ICCS. To reduce complexity, instead of devising a single overall (complex) model including all the various aspects of ICCS, several partial (and therefore simpler) models are devised, presenting these different complementary aspects one by one.

The graphical conventions used in the models are explained in the table below.





	Organizational/institutional entity playing a role in the ICCS
	Organizational/institutional entity outside the ICCS
	Information resource playing a role in ICCS
	A relationship between elements of the model. If pointing from element A to element B it should be read: "A <text> B". E.g. if <text> = "designates", the relationship is read as: "A designates B". Each <text> string starts with the label 'n:' (where n is a natural number) to allow for the unambiguous referencing of each relationship within a given model.

Table 3 – Graphical Conventions

The certification process is being initiated by an Applicant submitting its request for certification. The Applicant in context is shown in Figure 2 - Applicant in context. The Applicant is interested in having its Industrial Automation & Control System (IACS) Component certified based on the European ICCS. The Applicant is also responsible for collecting and making available all the elements necessary for assessment (ENA).

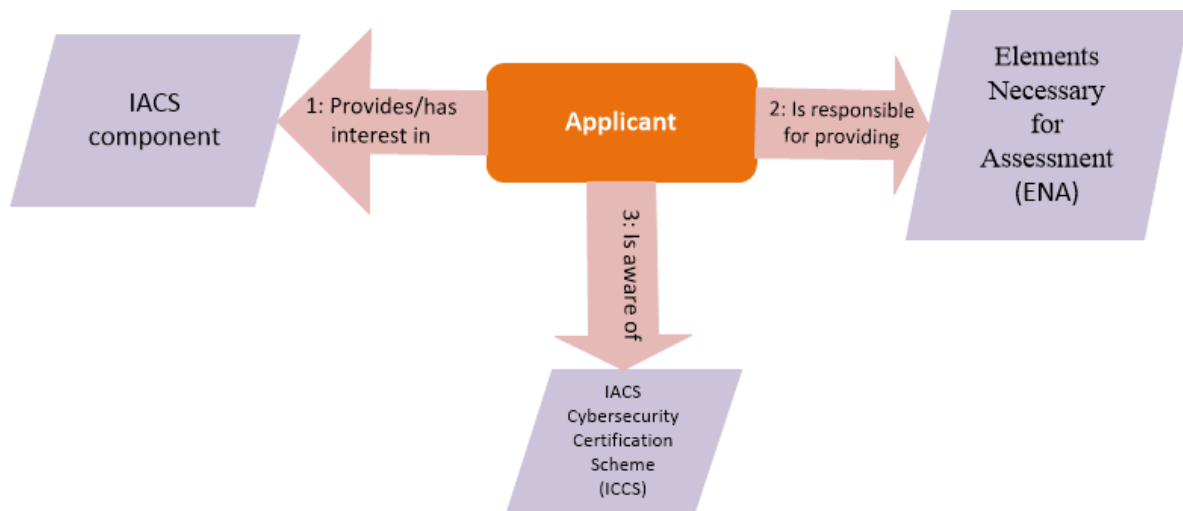


Figure 2 - Applicant in context

Req.6010 The Applicant shall be aware of the requirements of ICCS and shall prepare the complete Elements Necessary for Assessment (ENA).

The ICCS certification process is under the supervision of NCCA.Supervision where NCCA.Supervision are entities designated by the Member States (single NCCA.Supervision per Member State). The relationships of NCCA.Supervision with the associated entities are illustrated in Figure 3 - NCCA.Supervision in context. The NCCA.Supervision is designated by each Member State (Figure 3: Relationship#1). Additionally, the Member States designate also a NCCA.Certification body (Figure 3: Relationship#7). The NCCA.Supervision is in charge of enforcing and supervising the rules of the ICCS (Figure 3: Relationship#3). In order to facilitate the evaluation of IACS Components, the NCCA.Supervision is authorising Certification Bodies (CB) (Figure 3: Relationship#4) for performing the relevant security Evaluation Activities. The NCCA.Supervision bodies of the various Member States are responsible for performing Peer Reviews to each other (Figure 3: Relationship#2). The designated NCCA.Certification of the various Member States are responsible for conducting Peer Assessments to each other (Figure 3: Relationship#5), while the authorised CBs (for Assurance Level Substantial) are also conducting Peer Assessments to each other (Figure 3: Relationship#6).

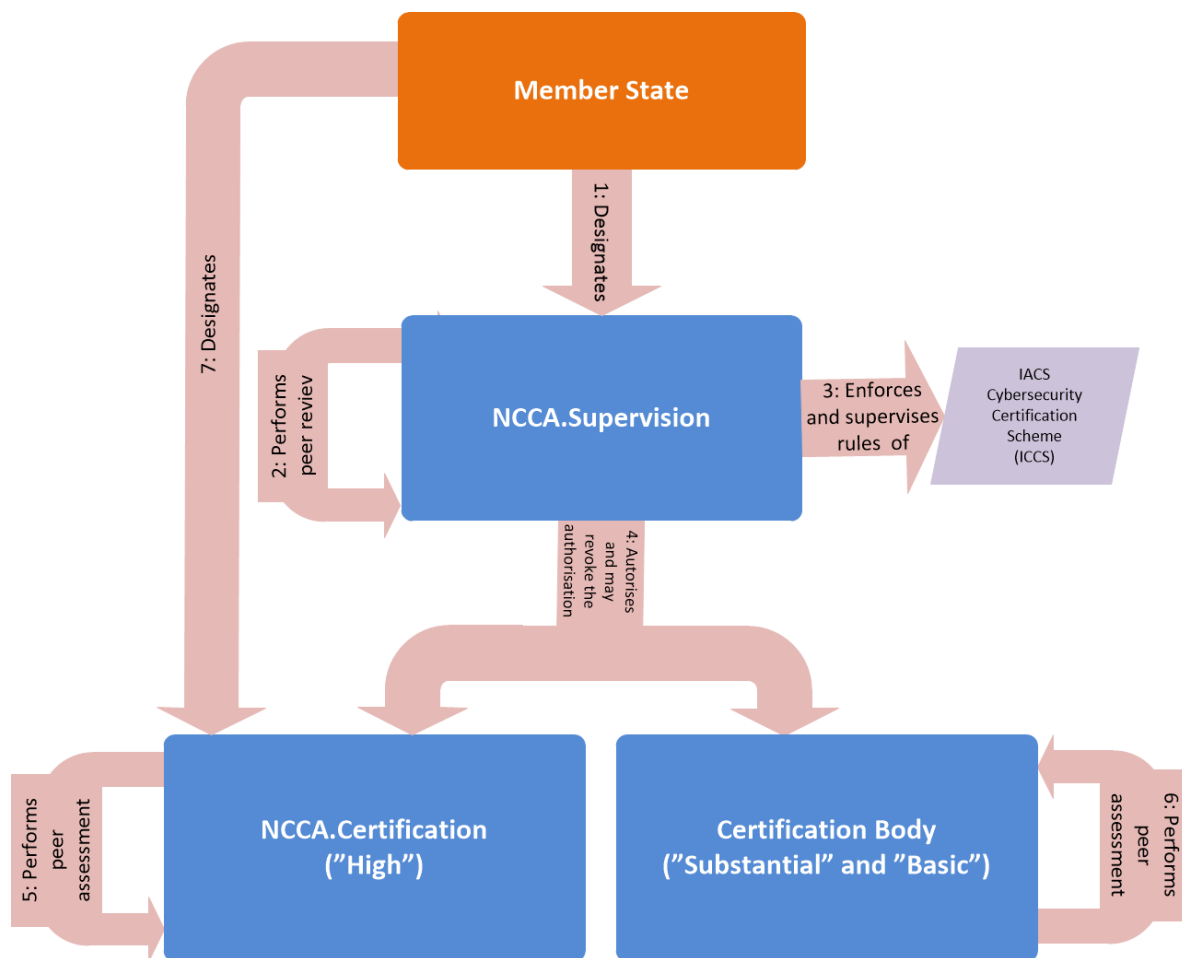


Figure 3 - NCCA.Supervision in context

- Req.6020** Each Member State shall designate at most one NCCA.Supervision being in charge of enforcing and supervising the rules of the ICCS.
- Req.6030** The NCCA.Supervision entities shall run Peer Reviews to each other, to ensure appropriate level of technical knowledge and operating quality.
- Req.6040** Each CB (for Assurance Level Substantial and Basic) and each NCCA.Certification that are involved in the ICCS shall have the authorisation of the Home NCCA.Supervision. This authorisation may be revoked by the Home NCCA.Supervision.
- Req.6050** The authorised CB shall be involved in Peer Assessment process by other CB so as to ensure appropriate level of technical knowledge and operating quality.
- Req.6060** Each Member State shall designate at most one NCCA.Certification being in charge of performing the ICCS related certification process.
- Req.6070** The authorised NCCA.Certification shall be involved in Peer Assessment process by other NCCA.Certificate to ensure appropriate level of technical knowledge and operating quality.

The request for certification is submitted by the Applicant to a CB. The overall process of requesting and issuing a Certificate is illustrated in Figure 4 - Issuing a Certificate on the Applicant request. Before an evaluation is started, the CB obtains all the Elements Necessary for Assessment (Figure 4: Relationship#4) for the CuA, as well as the CuA itself (Figure 4: Relationship#5), and performs the evaluation of the Component in line with the specific criteria associated with the considered Assurance Level (Figure 4: Relationship#6). The Applicant is responsible for providing all the Elements Necessary for Assessment (Figure 4: Relationship#2).

If the evaluation is successfully completed, the CB issues the Certificate for the CuA (Figure 4: Relationship#7). The Certificate is also submitted to ENISA (Figure 4: Relationship#10) and the local NCCA.Supervision (Figure 4: Relationship#8). The NCCA.Supervision may have access to all the evaluation documentation associated with the CuA (Figure 4: Relationship#1), as well as control over the issued Certificate (Figure 4: Relationship#9, it may withdraw the issued Certificate).

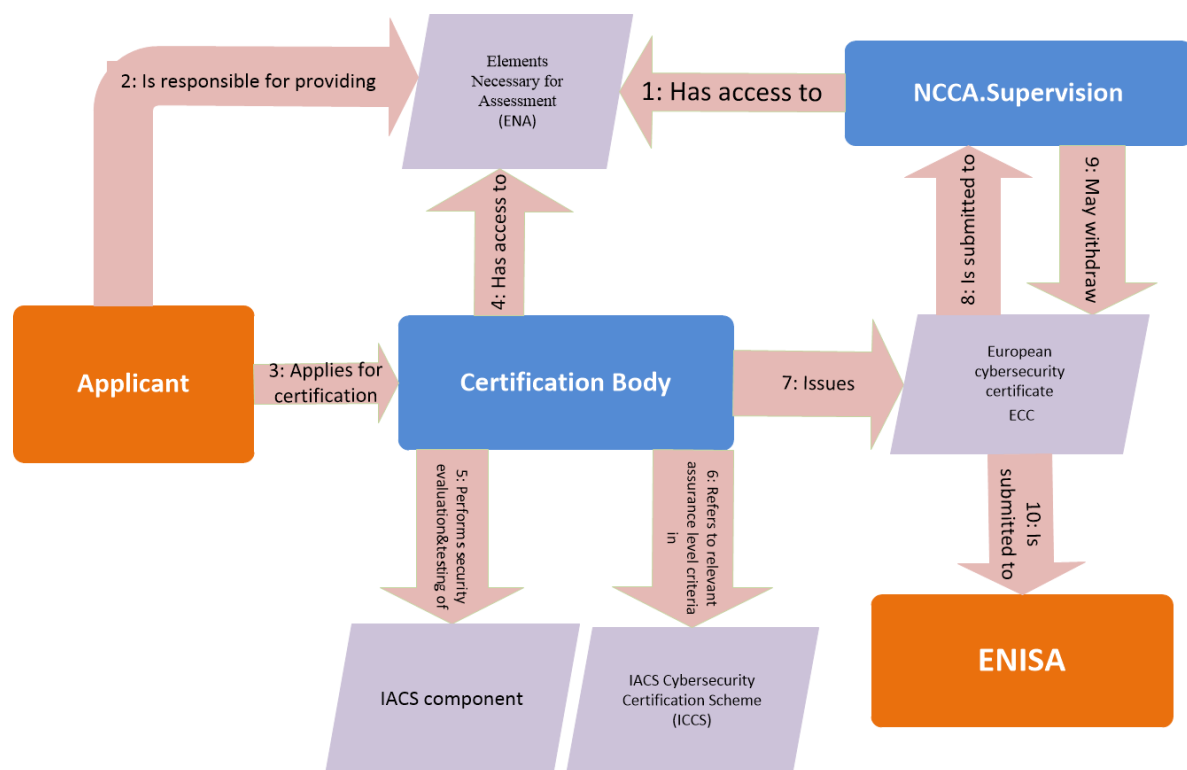


Figure 4 - Issuing a Certificate on the Applicant request

Req.6080 To initiate the ICCS certification process, the Applicant shall submit an explicit application to the chosen CB. Together with the application, the Applicant shall submit the complete Elements Necessary for Assessment (ENA).

Req.6090 The Applicant shall submit the request for certification to an authorised CB.

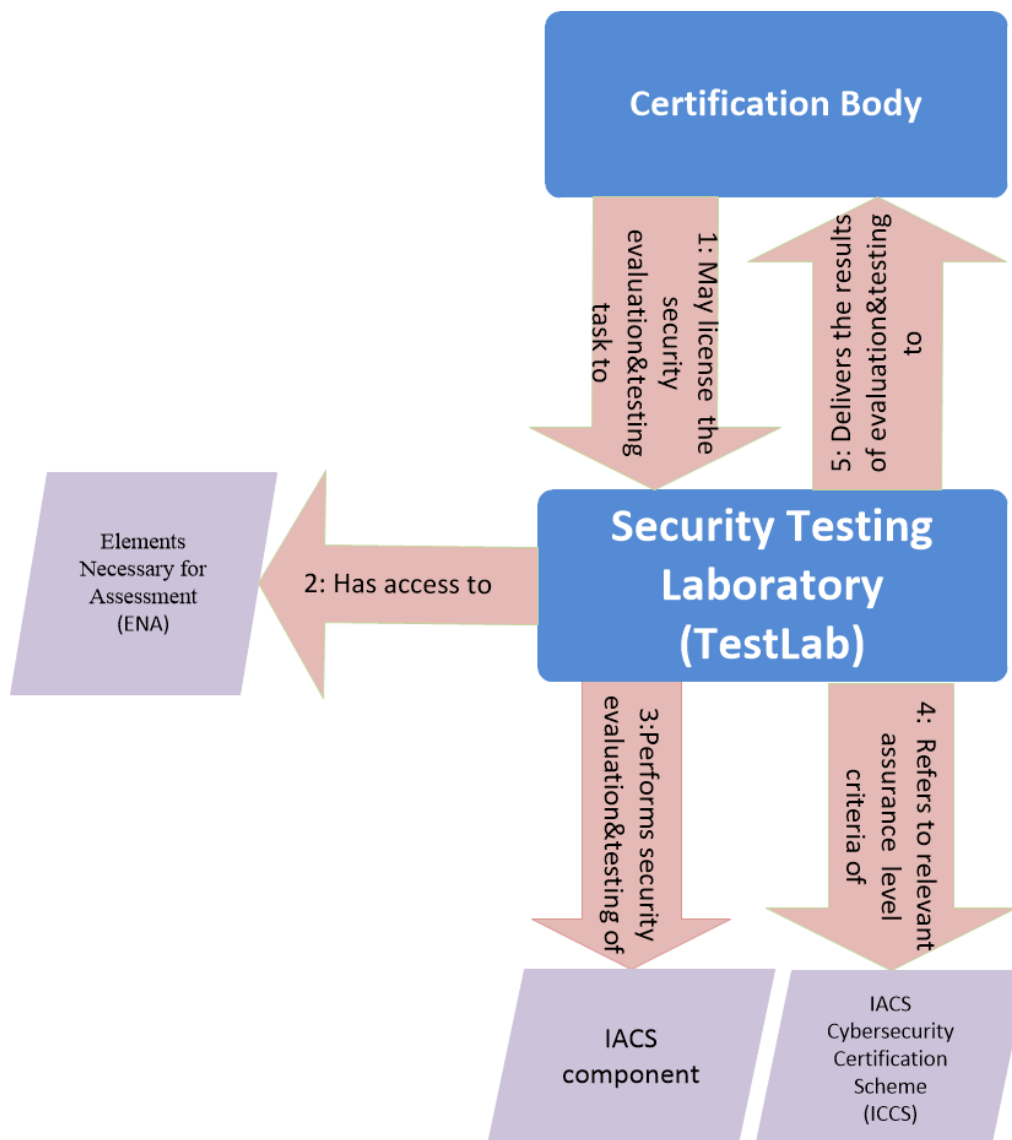
Req.6100 On the successful completion of the certification process (as this has been initiated by the Applicant), the involved CB shall issue the corresponding Certificate and submit it to the Applicant, ENISA and the relevant NCCA.Supervision.

1021 **Req.6110** The NCCA.Supervision shall withdraw the Certificate in case the rules of ICCS were
 1022 violated.

1023 **Req.6120** Each CB (for Assurance Level Substantial and Basic) and each NCCA.Certification shall
 1024 implement a procedure to handle complaints.

1025 **Req.6130** If a CB issues the European Cybersecurity Certificate (ECC), it shall make use of the
 1026 relevant Assurance Level criteria in the ICCS.

1027 Instead of performing the evaluation itself, the CB may assign a Security Testing Laboratory
 1028 (TestLab) to perform Evaluation Activities (including the security testing tasks), as illustrated in
 1029 Figure 5 - Security Testing Laboratory (TestLab) in the certification process. In such a case, the CB is
 1030 licensing specific TestLabs (Figure 5: Relationship#1) for delivering these evaluation services. The
 1031 licensed TestLab has access to all the Elements Necessary for Assessment (Figure 5: Relationship#2)
 1032 and performs the evaluation of the CuA (Figure 5: Relationship#3) based on the specific evaluation
 1033 requirements (Figure 5: Relationship#4). Finally, the TestLab provides the evaluation results in a
 1034 report to the CB (Figure 5: Relationship#5).



1035

1036 Figure 5 - Security Testing Laboratory (TestLab) in the certification process

1037 **Req.6140** A TestLab shall deliver the results of security evaluation & testing to the CB that
1038 requested (and licensed) the TestLab.

1039 **Req.6150** The CB shall have the option to license TestLabs for performing the parts of the
1040 certification that are related to the evaluation and testing of the CuA.

1041 The dependencies among the National Accreditation Body (NAB), CB and TestLabs are illustrated in
1042 Figure 6 - Accreditation, Peer Assessment and Peer Review model.

1043 A NAB is in charge of accrediting CBs, as well as TestLabs for performing the relevant assessment
1044 and certification activities. The accreditations are made in line with the corresponding standards
1045 (for example ISO/IEC EN 17065 or ISO/IEC EN 17025).

1046 The NAB is accrediting the CB (Figure 6: Relationship#3), while at the same time it is accrediting the
1047 TestLabs (Figure 6: Relationship#1) (which is optional in ICCS in accordance with the CSA).

1048 The NAB is also ensuring a continuous monitoring of the issued accreditation, and may withdraw
1049 this accreditation if deficiencies are being discovered (Figure 6: Relationship#2 and Figure 6:
1050 Relationship#4).

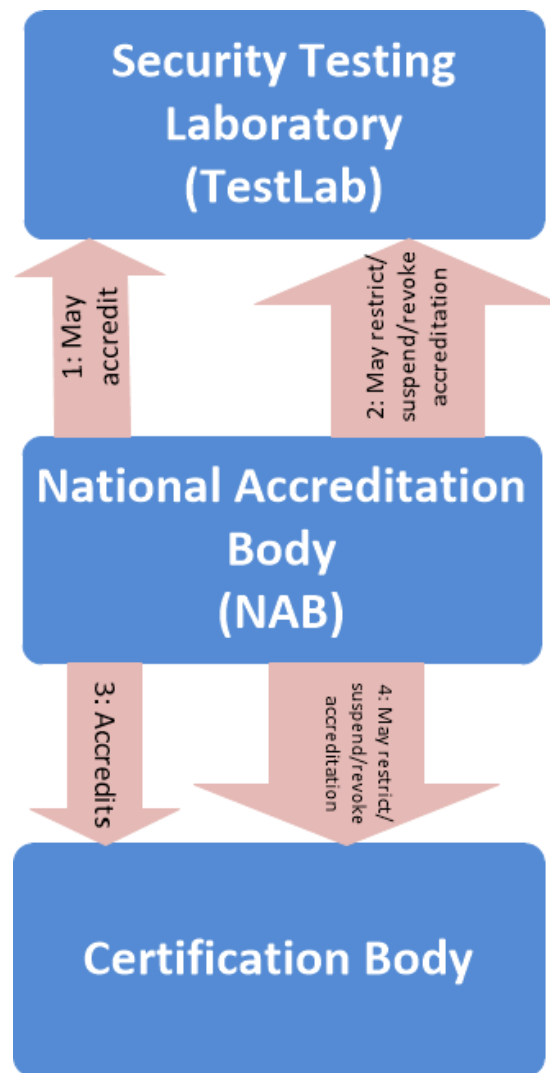


Figure 6 - Accreditation, Peer Assessment and Peer Review model

Req.6160 Each CB involved in the ICCS certification process shall be accredited by a NAB.

Note: If a TestLab is involved in the ICCS certification process, it may be accredited by a NAB.

The model of the Self-Assessment is presented in Figure 7 - Issuing an EU Statement of Conformity. In case of a Self-Assessment, the Manufacturer is in charge of collecting and maintaining any necessary evidence related to the concerned Component (Figure 7: Relationship#2). This evidence is available at any time for review by the NCCA.Supervision (Figure 7: Relationship#1). Based on this evidence, the Manufacturer may issue an EU Statement of Conformity for its Component (Figure 7: Relationship#5). For issuing the EU Statement of Conformity, the Manufacturer makes use of the criteria for the Assurance Level Basic of the ICCS (Figure 7: Relationship#7), applied to a specific IACS Component (Figure 7: Relationship#6).

The Statement of Conformity is submitted both to the NCCA.Supervision (Figure 7: Relationship#3), as well as to ENISA (Figure 7: Relationship#8). ENISA maintains an overview of all the Certificates and EU Statements of Conformity issued under the ICCS. The NCCA.Supervision has the authority to impose penalties on the Manufacturer, in case any issues are detected (Figure 7: Relationship#8).

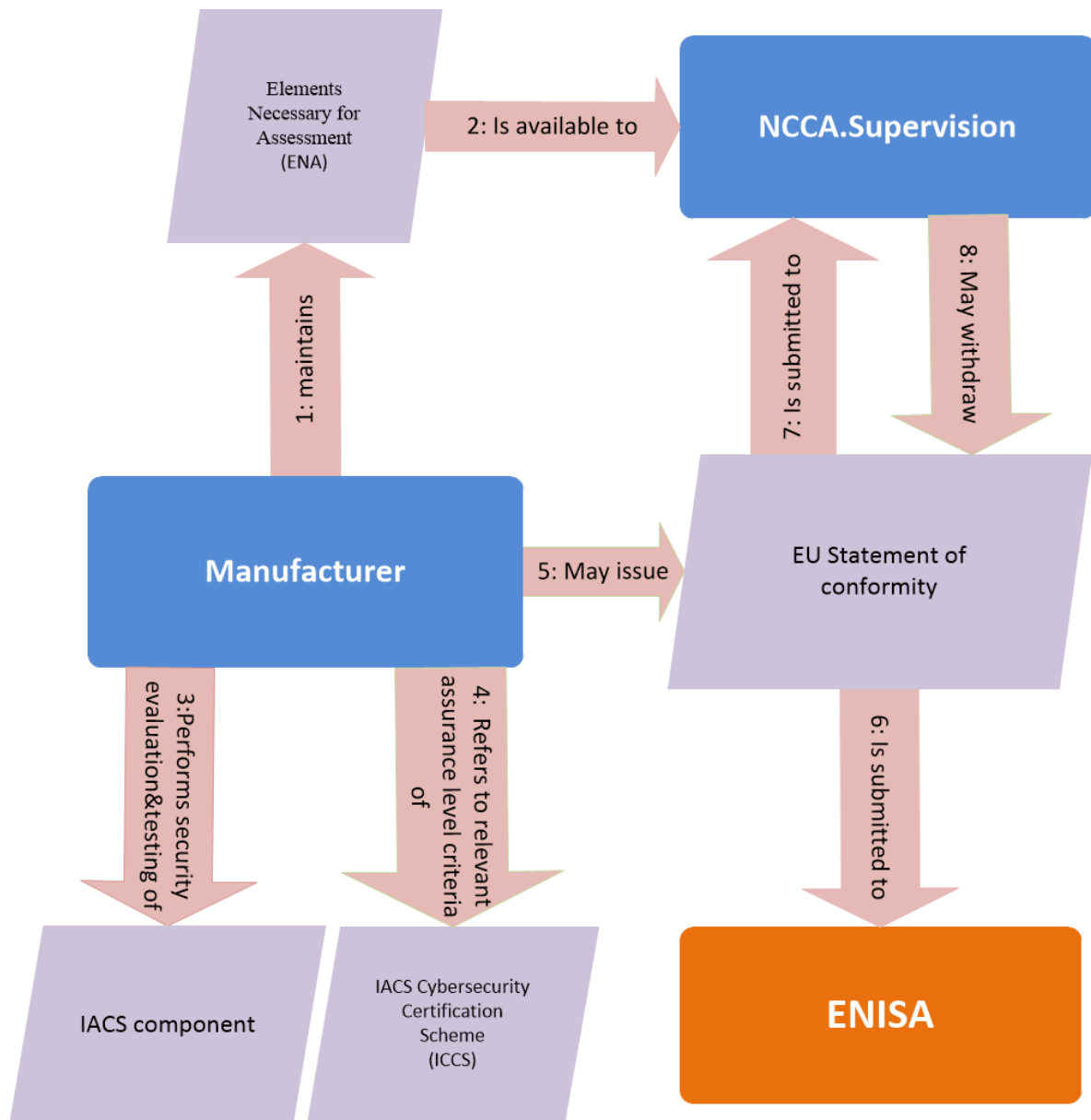


Figure 7 - Issuing an EU Statement of Conformity

- Req.6170** As soon as an EU Statement of Conformity for a Component is issued, the Component Manufacturer shall submit the Statement of Conformity to both ENISA and the NCCA.Supervision.
- Req.6180** The Manufacturer that issues an EU Statement of Conformity shall maintain the related pieces of evidence and shall make them available upon request to the relevant NCCA.Supervision.
- Req.6190** The Manufacturer that issues an EU Statement of Conformity shall make use of the criteria of the Assurance Level Basic of the ICCS.

Figure 8 - Consolidated organisation of the ICCS certification and Self-Assessment gives a consolidated view of the processes for issuing Certificates or EU Statements of Conformity for the

different Assurance Levels (Basic, Substantial and High). The NCCA.Supervision is responsible for authorising, supervising and monitoring the CBs (including NCCA.Certification for the Assurance Level “High”), as well as for monitoring of EU Statements of Conformity on the basis of the ICCS (Figure 8: Reference#1). Depending on the targeted Assurance Level, the NCCA.Certification for the Assurance Level High (Figure 8: Reference#2), the CB for the Assurance Levels Basic and Substantial (Figure 8: Reference#3) or the Manufacturer for the EU Self-Assessment at Assurance Level Basic (Figure 8: Reference#5) issue the Certificate or the EU Statement of Conformity, after evaluating the Component in scope (Figure 8: Reference#4, Figure 8: Reference#6 and Figure 8: Reference#7 respectively).

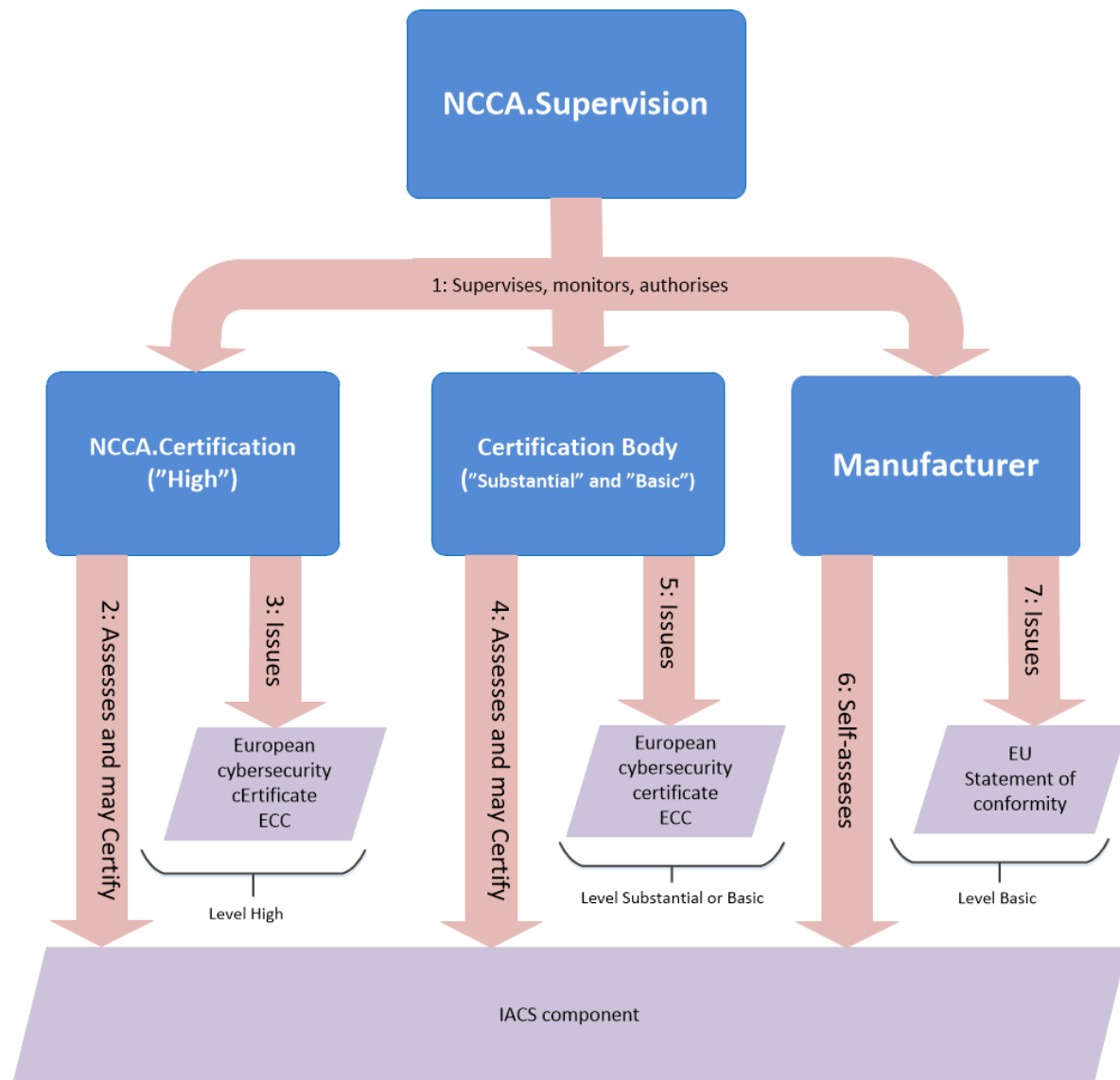


Figure 8 - Consolidated organisation of the ICCS certification and Self-Assessment

6.2 Evaluation and Accreditation of CB & Review Management

6.2.1 Authorisation of CBs

This Section describes the requirements that a CB must fulfil in order to get this authorisation.

1093 **Req.6200** To certify CuAs under the ICCS, a CB (including the NCCA.Certification for Assurance
1094 Level High) shall obtain an authorisation from the NCCA.Supervision.

ICCSGG- Req.0210	The ICCSGG or the respective ENISA Ad hoc Working Group shall define Technical Domains for which CBs may operate.
-----------------------------	---

1095

1096 **Note:** At the time of the development of this report, the necessity of identifying different
1097 Technical Domains for the purposes of the ICCS was still unclear. If no Technical
1098 Domains are necessary, the following paragraph applies to the entire scheme, i.e. the
1099 following paragraph should be read and interpreted as if the entire ICCS covers one
1100 single Technical Domain.

1101 **Req.6210** For each Technical Domain the CB shall fulfil the requirements of this Technical
1102 Domain, both for its site as well as well as for its personnel. To show its technical
1103 expertise for this Technical Domain, the CB shall perform an evaluation / certification
1104 under close oversight of the responsible NCCA.Supervision.

1105 **Req.6220** Responsible for defining the exact process for a CB to be authorised for a Technical
1106 Domain shall be the NCCA.Supervision, unless the ICCSGG has set up specific
1107 requirements for the authorisation process in this Technical Domain.

1108 **Req.6230** The authorisation given by the NCCA.Supervision to the CB to operate under the ICCS
1109 shall be based on the following requirements:

- 1110 [a] Sufficient expertise in the contents and procedures of the ICCS is
1111 demonstrated by the personnel of the CB. This can be demonstrated by
1112 attending a recognised training covering the objectives, scope and elements of
1113 the ICCS;
- 1114 [b] A valid ISO/IEC EN 17065 accreditation of the CB enabling it to issue
1115 Certificates based on the ICCS;
- 1116 [c] The CB shall ensure that Assessment Teams (irrespective of whether they are
1117 internal to the CB or they are part of an external TestLab) meet the applicable
1118 requirements of the ISO/IEC EN 17025;
- 1119 [d] The Assessment Team, either internally or the TestLab, has successfully
1120 completed a test evaluation under the ICCS, with the CB carefully monitoring
1121 the executing of the test evaluation and approving its results and conclusions;
- 1122 [e] A CB has been successfully audited and examined by the NCCA.Supervision to
1123 demonstrate that its procedures are suitable for performing certification
1124 within this Technical Domain. This includes proofs of competency (including
1125 the skills of the Assessment Team, either internal or a TestLab) for penetration
1126 testing and robustness assessment activities.

1127 **Note:** If a Technical Domain allows several evaluation methodologies, the authorisation of
1128 a CB applies only to the Evaluation Methodology that was used during the evaluation
1129 / certification that was performed under the oversight of the NCCA.Supervision as

1130 part of the CB's authorisation procedure (Req.6210). The authorisation of a CB may
1131 be extended to another Evaluation Methodology by an additional authorisation
1132 procedure for this other Evaluation Methodology, i.e. the authorisation of a CB always
1133 applies to the combination of the Technical Domain and the Evaluation Methodology.
1134 This additional authorisation for the other Evaluation Methodology may be omitted,
1135 if the set of evaluators have already proven their competence and adequacy for this
1136 second Evaluation Methodology in another Technical Domain with at least the same
1137 Assurance Level (see following examples) and the ICCSGG has not objected such
1138 procedure for this Technical Domain.

Example:

A CB has been authorized for IEC 62443-4-2 and ISO/IEC 15408 for Assurance Level High for the Technical Domain "A" in the past. Now it got authorised for the Technical Domain "B" for IEC 62443-4-2 for Assurance Level Substantial. If the CB uses the same set of personnel, it is already authorised for the Technical Domain "B" for ISO/IEC 15408 as well.

A CB has been authorized for IEC 62443-4-2 and ISO/IEC 15408 for Assurance Level Substantial for the Technical Domain "A" in the past. Now it got authorised for the Technical Domain "B" for IEC 62443-4-2 for Assurance Level High. If the CB wishes to use ISO/IEC 15408 for the Technical Domain "B" as well, then an additional authorization using ISO/IEC 15408 (with at least EAL 4) is required.

1139 **6.2.2 Accreditation of CB and Assessment Teams**

1140 **Req.6240** CBs shall be accredited by a National Accreditation Body (NAB) according to ISO/IEC
1141 EN 17065 (pursuant to Regulation (EC) No 765/2008).

1142 **Req.6250** Assessment Teams (either internal to the CB or the TestLab) shall meet the applicable
1143 requirements of ISO/IEC EN 17025, which may be demonstrated e.g. by accreditation
1144 according to ISO/IEC EN 17025 (pursuant to Regulation (EC) No 765/2008).

1145 **Note:** The ICCSGG may set up additional requirements relevant to the accreditation of CBs.

1146 **Req.6260** CBs and Assessment Teams shall retain records of the assessments carried out at least
1147 in the last five years.

1148 **6.2.3 Peer Assessment for the NCCA.Certification (Assurance Level High)**

1149 The Peer Assessment for the ICCS (according to the CSA article 54.1.u) defines a mechanism to
1150 harmonise assessments performed by different NCCA.Certification (dealing with Assurance Level
1151 "High").

1152 The Peer Assessment consists of three phases: preparation, on-site assessment and reporting.

1153 **Note:** The NCCA.Certification that is the object of the Peer Assessment is hereafter referred
1154 to as the Auditee.

1155 *6.2.3.1 Preparation of the Peer Assessment*

1156 The preparation includes actions dedicated to the Peer Assessment Team and to the
1157 NCCA.Certification under the Peer Assessment.

1158 *6.2.3.1.1 Preparation of the Peer Assessment by the Peer Assessment Team*

1159 The first step is to select the composition of the Peer Assessment Team.

1160 **Req.6270** The Peer Assessment Team shall be made up of at least 3 assessors from two other
1161 NCCA.Certification. Further NCCA.Certification may join the reviewer team as
1162 observers.

1163 **Req.6280** The ICCSGG shall set up a policy for choosing the lead and the secondary
1164 NCCA.Certification for the Peer Reviews. For the same NCCA a different lead NCCA in
1165 the next Peer Assessment (e.g. after 2 years) shall be chosen.

1166 **Req.6290** The lead NCCA.Certification shall provide at least two assessors, one of which is
1167 responsible for collecting evidence and providing written notes from the Peer
1168 Assessment proceedings and the other assessor is responsible for the organisation of
1169 the Peer Assessment itself (from the reviewer side). If possible, both assessors shall
1170 have been involved in previous Peer Assessments (e.g. as part of the secondary
1171 NCCA).

1172 **Req.6300** All assessors shall have a professional background under the ICCS (or a comparable
1173 Industrial Automation & Control Systems assessment experience), if possible of at
1174 least 2 years. The assessors may be accompanied by technical experts from the
1175 NCCA.Certification for certain technical issues or certain Technical Domains.

1176 **Note:** The NCCA.Certification under Peer Assessment may raise objections against certain
1177 assessors at the ICCSGG, if it cannot resolve this issue with the lead
1178 NCCA.Certification.

1179 **Note:** The second step is to set up the Peer Assessment plan (including the work
1180 assignments for each member of the Assessment Team)

1181 **Req.6310** The Peer Assessment plan shall be provided to the Auditee at latest 2 weeks before
1182 the agreed date.

1183 **Req.6320** The Peer Assessment shall require 4 business days of on-site work (additional time is
1184 required for preparation and reporting) covering the following activities:

- 1185 [a] One day on-site assessment of the Auditee for generic (but IACS-specific)
1186 topics like qualification of staff, licensing of TestLabs (if applicable), etc. This
1187 includes the opening of the assessment and the closing of the assessment;
1188 [b] One day on-site assessment of the Auditee where the Assessment Team
1189 (splitting up) reviews the two IACS Components in detail with the appropriate
1190 certifiers;

1191		[c] Two days (one per selected IACS Component) to review in detail the
1192		assessment performed with the appropriate evaluators (at the site of the
1193		TestLab, when applicable).
1194	Note:	The exact order of the Req. 6320 activities, is subject to the individual Peer
1195		Assessment. For example, the generic topics might be split in two half days (e.g.
1196		Monday afternoon and Friday morning), and the order of the review on-site may
1197		differ.
1198	6.2.3.1.2	Preparation of the Peer Assessment by the Auditee
1199	Req.6330	The Auditee shall provide a single point of contact for the Peer Assessment Team for
1200		the entire assessment.
1201	Req.6340	The Auditee shall select two IACS Components which were certified recently or are in
1202		the final stages of certification. If the Auditee is active in several Technical Domains
1203		those two IACS shall be from different Technical Domains. If possible, the two
1204		certifications shall involve different Assessment Teams and differ in technology (e.g.
1205		different gCCAs). If the Auditee is unable to provide IACS certifications according to
1206		these rules (e.g. because it was not active in the last years), the ICCSGG shall decide
1207		upon alternative means of providing evidence.
1208	Req.6350	The Auditee shall be responsible for contacting the TestLabs or internal Assessment
1209		Teams (and where necessary the Applicants of the IACS Components) which carried
1210		out the evaluation for the selected applications and to ensure that they appropriately
1211		participate in the Peer Review.
1212	Req.6360	The Auditee shall provide all evidence regarding the Peer Assessment (e.g. public and
1213		internal scheme documents like written policy and procedure documents, evidence
1214		and certification documents for the selected IACS Components) to the assessors. If
1215		possible, confidentiality should be assured using rules adopted in the European
1216		Cybersecurity Certification Group (ECCG) or the ICCSGG.
1217	Req.6370	All members of the Peer Assessment Team, including observers, shall have access to
1218		the information on-site. However, the Auditee may request that the evidence
1219		regarding specific IACS Components may only be distributed to the assessors, not the
1220		observers.
1221	Req.6380	The Auditee shall translate all evidence necessary to perform the Peer Assessment
1222		before distribution or Peer Assessment to English, unless a different agreement has
1223		been made with the Peer Assessment Team in advance. For any of its personnel that
1224		may not be fluent in English, the Auditee has to provide interpreters (not necessarily
1225		professional ones, members of the NCCA should suffice).
1226	Req.6390	The Auditee shall send to the Peer Assessment Team the documentation (including
1227		the documentation for the IACS Components) at latest 4 weeks before the Peer
1228		Assessment date. The assessors shall review the documents so as them to be able to
1229		perform the audit.

1230	Req.6400	To prepare the on-site Peer Assessment, the Auditee shall make available their
1231		internal (assessment, technical) team to the Peer Assessment Team and provide a
1232		dedicated room for the Peer Assessment Team (for their internal discussion and
1233		preparation).
1234	6.2.3.2 On-Site Peer Assessment	
1235	Req.6410	The on-site phase shall start with an opening meeting, where the schedule, logistics
1236		(separate room, access to Auditee personnel and sites) and the relevance (up to
1237		date?) of the previously provided evidence shall be confirmed.
1238	Req.6420	Where applicable, the on-site phase shall follow the guidelines of ISO 19011 (cf.
1239		“Guidelines for auditing management systems”, 2018).
1240	Req.6430	The activities shall include the following items:
1241		[a] The generic on-site audit;
1242		[b] The review of the two IACS Components and the visits of other sites (i.e. if
1243		external TestLabs are used).
1244	Note:	The exact order is up to the Assessment Team. Usually the Assessment Team splits up
1245		for the review of the IACS Components.
1246	Req.6440	During the Peer Assessment, evidence shall be reviewed and personnel interviewed
1247		at both NCCA.Certification and Assessment Team levels. Where necessary, evidence
1248		might need to be recorded for the report; in this case, the Auditee should provide
1249		redacted (black-end) versions.
1250	Req.6450	For the interviews, the personnel responsible for the IACS Components evaluation
1251		shall be available. Additionally, the Auditee needs to provide a selection of further
1252		certifiers/evaluators (both junior and senior) and the relevant process owners (or
1253		their deputies). The assessors then will select those to be interviewed from this pool.
1254	Note:	The Peer Assessment focuses on whether the assessed entity holds the technical
1255		expertise for carrying out certification under the ICCS for the Assurance Level High.
1256		To this end, the Peer Assessment focuses on all the ICCS-specific procedures and the
1257		two selected ICCS Components , i.e. the criteria mentioned in Article 59, Paragraphs
1258		3.d and 3.e of the CSA.
1259	Req.6460	The following topics shall be audited, either at the level of the NCCA.Certification or
1260		at the level of the Assessment Team (Table 4).

What to Review	Suggested Review Method
Qualification of certifiers/evaluators	Interviews with at least one junior and one senior certifier
Continuous education	<ul style="list-style-type: none"> Review of the training concept and material

	<ul style="list-style-type: none"> • Review of the effectiveness of training • Review of personnel records
Mentoring programme for new certifiers/evaluators	Interviews with mentors
Effectiveness of lab oversight	Interviews with evaluators and certifiers
Technical consistency	Minutes of workshops and lab /NCCA meetings Interviews Examples for the dissemination of technical decisions with the ICCS and application of such decisions in specific procedures
Finding from previous Peer Assessments	<ul style="list-style-type: none"> • Document review • Interviews
Technical skills of certifiers and evaluators	Interviews (e.g. as part of the review of IACS Components or mock up problems)
Adherence to written policies and procedures	Sample relevant ICCS policies and procedures and verify (evidence, interview) their implementation
Technical upkeep of skills required	<ul style="list-style-type: none"> • Review of job descriptions, strategic training plans, knowledge management procedures • Interviews with management personnel
Internal review (QA)	Review QA procedures and examples for QA

Table 4 – Content and method for Peer Assessment

Note: Here, the term “junior” refers to personnel with less than 3 years in the service, while the term “senior” refers to personnel with at least 3 years in the service.

Req.6470 Before the closing meeting, the Assessment Team shall review the evidence found. It shall agree upon the verdict and the recommendations and suggestions to the Auditee.

Req.6480 In the closing meeting, the lead assessor shall present the recommendations and suggestions to the Auditee and shall present the verdict of the Assessment Team. If the Auditee does not agree to any of the results presented by the Assessment Team this shall be formally recorded.

6.2.3.3 Reporting of the Peer Assessment

Req.6490 The Peer Assessment Team shall present the written report to the Auditee no later than 4 weeks after the end of the on-site part. Where possible, findings should not include names of individuals (e.g. certifiers, evaluators). At this stage the Auditee has the final opportunity to raise objections and correct factual (and editorial) errors.

1276	Req.6500	If the Auditee does not return a reply after 2 weeks, the report shall be considered
1277		accepted. If the Auditee raises any objection or corrects any errors, the assessors shall
1278		review the issues and correct all the points that they agree with within 2 weeks after
1279		receiving the remarks. In the final report they shall clearly mark all disagreements,
1280		including those from the closing meeting.
1281	Req.6510	The Auditee shall resolve all recommendations of the Peer Assessment report and
1282		address all suggestions within 2 months after the report has been accepted and all
1283		possible disputes have been resolved by the ICCSGG.
1284	Note:	The term “address a suggestion” does not imply the resolution of the issue, but rather
1285		a sound justification of how to deal with this suggestion, including a time schedule;
1286		this might include rejection of the suggestion (with justification).
1287	Req.6520	The final report shall be forwarded to the ICCSGG which in turn shall processes it
1288		according to the rules laid out in the CSA and implementing acts (if any).
1289	Req.6530	The ICCS specific part of the Peer Assessment shall be aligned with the general Peer
1290		Review for the NCCA.Supervision.
1291	Req.6540	The results of the Peer Assessment shall be provided for the general Peer Review to
1292		avoid any overlap. Where possible, the ICCS general Peer Review shall be consecutive
1293		or in parallel to the Peer Assessment.
1294	Note:	The relationships of the entities involve in the Peer Assessment of the CB and the Peer
1295		Review of the NCCA.Supervision are illustrated in Figure 3 - NCCA.Supervision in
1296		context.
1297	6.2.3.4	<i>Timeline of the Peer Assessment</i>
1298	Req.6550	The Peer Assessment should follow this schedule; any deviation shall be approved by
1299		both the Assessment Team and the Auditee:
1300		[a] Peer Assessment date - 4 weeks: Sending the documentation to the Peer
1301		Assessment Team;
1302		[b] Peer Assessment date - 2 weeks: Sending of the assessment plan by the Peer
1303		Assessment Team;
1304		[c] On-site Peer Assessment date: 4 days on-site;
1305		[d] Peer Assessment date + 4 weeks: Sending of the Peer Assessment report;
1306		[e] Peer Assessment date + 6 weeks: Acceptance (or not) of the Peer Assessment
1307		report from the Auditee;
1308		[f] Peer Assessment date + 8 weeks: Sending of the final Peer Assessment report
1309		(accepted or with Auditee comments) by the Peer Assessment Team to
1310		ICCSGG and the NCCA.Supervision;
1311		[g] Peer Assessment date + 16 weeks: Sending of the action plan by the Auditee to
1312		the Peer Assessment Team.

1313 **6.2.4 Peer Assessment for the CB (Assurance Level Substantial)**

1314 The aim of this Peer Assessment is to harmonise practices among CB that deal with Assurance Level
1315 Substantial.

1316 **Req.6560** The Peer Assessment for the CB shall be identical to the Peer Assessment for the
1317 NCCA.Certification (Section 6.2.3) with the following exceptions:

1318 [a] The Peer Assessment Team consists of at least 2 assessors (instead of 3 for
1319 Assurance Level High);

1320 [b] The Peer Assessment shall require 2 business days on-site (instead of 4 for
1321 Assurance Level High).

1322 **Note:** There is no Peer Assessment for CB certifying with the Assurance Level Basic.

1323 **6.2.5 Peer Review for the NCCA.Supervision**

1324 The Peer Review for the ICCS (according to CSA Article 59) aims at harmonising the supervision
1325 activities performed by the various NCCA.Supervision.

1326 **Note:** In case the rules defined here and by the CSA Article 59 (and its implementing acts)
1327 contradict, the latter prevail.

1328 **Req.6570** Pursuant to CSA Article 59, the Peer Review shall:

1329 [a] Be carried out by 2 NCCA.Supervision (each NCCA providing an auditor);

1330 [b] Require 2 business days on-site;

1331 [c] Be done at least once every 5 years.

1332 **Req.6580** The Peer Review should follow this schedule; any deviation shall be approved both by
1333 the Peer Review team and the Auditee:

1334 [a] Peer Review date - 6 weeks: Sending of the Global agenda (with dates) by the
1335 Peer Review team;

1336 [b] Peer Review date - 5 weeks: Acceptance of the agenda by the peer-reviewed
1337 NCCA.Supervision;

1338 [c] Peer Review date - 4 weeks: Sending of the documentation to the Peer Review
1339 team;

1340 [d] Peer Review date - 2 weeks: Sending of of the detailed agenda by the Peer
1341 Review team;

1342 [e] Peer Review date: 2 days of Peer Review on-site;

1343 [f] Peer Review date + 4 weeks: Sending of the Peer Review report;

1344 [g] Peer Review date + 6 weeks: Acceptance (or not) of the Peer Review report by
1345 the Auditee;

1346 [h] Peer Review date + 8 weeks: Sending the Peer Review report (accepted or with
1347 Auditee comments) by the Peer Review team to the ECCG.

1348 **Req.6590** The following topics shall be addressed during the Peer Review:

1349 [a] Strict separation of the NCCA.Certification and NCCA.Supervision activities;

1350		[b] The procedures to monitor certification activities (CB) by the NCCA.Supervision
1351		are defined and performed. The results of the Peer Assessment between CBs
1352		(linked to the NCCA.Supervision) are monitored by the NCCA.Supervision;
1353		[c] The procedures to monitor Self-Assessments (Manufacturer) by the
1354		NCCA.Supervision are defined and performed;
1355		[d] The procedure to authorise the CBs to perform ICCS assessments is defined,
1356		adhered to and a list of authorized bodies is maintained;
1357		[e] The procedure to check skills of the NCCA.Certification and CBs is defined;
1358		[f] The list of complaints is maintained and managed;
1359		[g] The recommendation of the ECCG on supervision activities are followed by the
1360		NCCA.Supervision (according to CSA Article 59, Paragraph 6).
1361	Req.6600	If a finding (partially) covers one or more CBs, the NCCA.Supervision shall initiate the
1362		appropriate corrective actions within the ICCS to resolve the issue within the CBs.
1363	6.2.6 Requirements and Guidance in case Evaluation Activities are Delegated	
1364	Req.6610	A CB shall issue a Certificate after having performed an assessment/evaluation
1365		successfully. Depending on the organisation of the CB, this evaluation which is
1366		performed by an Assessment Team, can be internal resources (cf. §6.2.1 of ISO/IEC
1367		EN 17065) or external resources (cf. §6.2.2 of ISO/IEC EN 17065). The latter case is
1368		called "TestLab" in this document.
1369	Req.6620	In the case of external resources, the CB shall define a procedure to license the
1370		TestLabs in charge of the evaluation.
1371	Note:	This procedure aims to ensure that even if delegated, the evaluation will meet the
1372		same level of expectations. The scope of the Evaluation Activities conducted by the
1373		TestLabs (especially the Technical Domains) will depend on the agreement between
1374		the TestLab and the CB. This may include re-evaluations (if the CuA has been
1375		previously evaluated and certified, and it has been subject to minor upgrades
1376		impacting the security) or full new evaluations (if the CuA has not been previously
1377		evaluated). In all situations, the CB remains responsible for the evaluation results and
1378		for issuing (or updating) the Certificate.
1379	Req.6630	The procedure of licensing a TestLab shall define at least that the evaluation body has
1380		successfully completed a test evaluation under the ICCS, with the CB carefully
1381		monitoring the execution of the test evaluation and approving its results and
1382		conclusions.
1383	Note:	The model of involving TestLabs in the certification process is illustrated in Figure 5 -
1384		Security Testing Laboratory (TestLab) in the certification process. In this figure, the
1385		term "security testing" refers to all Evaluation Activities necessary for the purpose of
1386		certification. This can include Security Functions testing, fuzz testing, penetration
1387		testing, documentation review or site audits.

6.2.7 Regular Meetings of CBs and Assessment Teams

Req.6640 Each NCCA supervision shall organize a meeting at least once a year in order to ensure common applicability of the ICCS requirements, and to ensure proper information flow (e.g. to discuss any planned updates/changes to the ICCS and to ensure that the CBs and their Assessment Teams, especially for TestLabs, are able to provide feedback).

Req.6650 Each CB and each Assessment Team (including those from TestLabs) supervised by the NCCA Supervision, including the NCCA Certification, shall be represented at this meeting. It is possible that several NCCA Supervision perform a joint meeting specifically for all CBs and Assessment Teams that are supervised by them, e.g. to reduce the effort for Member States with only few CBs/Assessment Teams.

Req.6660 During this meeting sufficient time shall be allocated for the CBs and Assessment Teams to comment and provide feedback and the following topics shall be discussed (at least):

- [a] Questions from certifications/evaluations from the CBs/Assessment Teams of general nature, e.g. for consistency of approaches (but without giving away any specifics on the procedures);
- [b] Issues discussed at the ICCSGG;
- [c] Issues of general nature dealt by NCCA Supervision, for example with Peer Assessment and Peer Review results (but without giving away any specifics on the procedures);
- [d] Proposed or requested changes/updates requested to any or all of the participants, e.g. changes to the standards or the ICCS.

6.3 Component Cybersecurity Profile (CCP) and generic Component Context Analysis (gCCA) elaboration and validation

6.3.1 Elaboration of Component Cybersecurity Profiles (CCP)

Req.6670 CCP shall be elaborated by the Applicant of the IACS Components.

Note: The Applicant may involve other parties to elaborate the CCP (e.g. TestLab). If a TestLab has been involved in the elaboration of the CCP, then it shall be excluded from further evaluation work on the same IACS Component (including the validation of the CCP and the security validation of the CuA).

6.3.2 Elaboration of a generic Component Context Analysis (gCCA)

There are two types of gCCAs which can be used in an ICCS Conformity Assessment process:

- [a] **EU gCCA (certified).** It is managed by the ICCSGG and recognised by the ICCS and the EU.
- [b] **Other gCCA.** It can be elaborated and validated by any other organisation / interest group by their own rules.

1424	Req.6680	A proposal for a new EU gCCA can be submitted by any interested entity. This proposal
1425		shall be submitted to the responsible Home NCCA, depending on the submitting
1426		entity.
1427	Req.6690	The Home NCCA shall provide a first assessment of the proposal (Section 6.3.2) and,
1428		if the proposal is assessed to be useful and suitably separate from other EU gCCAs, it
1429		shall forward the proposal and its assessment to the ICCSGG.
1430	Req.6700	The ICCSGG (or an appropriate subgroup thereof) shall decide on the necessity and
1431		validity of the approach according to the ToR (Terms of Reference) of the elaboration
1432		group.
1433	Req.6710	The editorial lead on the elaboration of the EU gCCA in the elaboration group is by
1434		default held by the Home NCCA, but it may be delegated to another NCCA. The
1435		responsible NCCA shall ensure that all relevant stakeholders are appropriately
1436		involved in the elaboration group.
1437	Req.6720	The elaboration group shall be in charge of writing the EU gCCA.
1438		
1439	6.3.3 Validation of CCPs	
1440	Req.6730	A validated CCP shall be the entry point for any Component certification, i.e. the point
1441		of reference for judging the other evaluation deliverables (e.g. the potential impact
1442		of a bug in a Component is assessed with respect to the assets, threats, assumptions,
1443		etc. described in the CCP).
1444	Req.6740	The CCP shall be validated by i) the Manufacturer in the case of a Self-Assessment or
1445		ii) the CB in the case of a Component certification.
1446	6.3.4 Validation of EU gCCAs	
1447	Req.6750	Before being formally published, an EU gCCA shall be validated and certified.
1448	Req.6760	The content of an EU gCCA shall be validated by verifying if the definition of the
1449		security problem (threats, assumptions etc.) and the risk situation are appropriate
1450		and consistently followed up in the entire EU gCCA.
1451	Req.6770	The validation of an EU gCCA shall be carried out by a CB which has not been involved
1452		in the elaboration of the EU gCCA. The CB shall be chosen by the submitter of the EU
1453		gCCA in agreement with the Home NCCA. For the assessment of the content, the CB
1454		closely works with both the ICCSGG (or its relevant subgroup) and the submitter, to
1455		ensure inconsistencies and ambiguities are resolved. For the formal verification of the
1456		EU gCCA (i.e. the certification) the details depend on the underlying standard chosen
1457		for the EU gCCA and are listed in Annex B.
1458	Req.6780	The validation of an EU gCCA shall be followed by the certification of this EU gCCA, so
1459		as to ensure that CCAs can be successfully based on this EU gCCA.

1460 **Req.6790** After its certification, the EU gCCA shall be published before any Component can be
1461 certified to conform to the EU gCCA. For this, the ICCSGG and ENISA shall agree on a
1462 suitable Internet webpage. The EU gCCA shall be available free of charge.

1463 **Note:** Annex D gives examples of validation of an EU gCCA for the IEC 62443, ISO/IEC 15408
1464 and Lightweight approaches.

ICCSGG- Req.0220	The ICCSGG or the respective ENISA Ad hoc Working Group shall develop the validation procedures for EU gCCAs.
-----------------------------	---

1465 **6.4 Vulnerability Disclosure Management and Vulnerability Database Update and**
1466 **Communication**

ICCSGG- Req.0230	The ICCSGG or the respective ENISA Ad hoc Working Group shall define a procedure for vulnerability disclosure management and vulnerability database update and communication procedure.
-----------------------------	---

1467 **6.5 Certificate issuance – Mutual Recognition – International Validity**

1468 **Note:** Currently the issue of mutual recognition is at an early stage, since the ICCS is not yet
1469 defined.

1470 **6.6 Monitoring, Maintenance, Renewal and Withdrawal of Certificates**

1471 **Req.6800** After issuing Certificates for Components under the ICCS, these Certificates shall be
1472 carefully managed in order to ensure that they still meet their security requirements.

1473 **Note:** Efficient management of issued Certificates will play a crucial role in several aspects,
1474 including the publication, monitoring, maintenance, renewal or withdrawal.

ICCSGG- Req.0240	The ICCSGG or the respective ENISA Ad hoc Working Group shall devise a mechanism to handle continuous updates of Components.
-----------------------------	--

1475

1476 **Note:** It has not been addressed as there is no generally accepted solution available when
1477 writing this proposal.

1478 **Req.6810** The CB shall manage:

1479 [a] The publication of the Certificates in ENISA website;

1480 [b] The maintenance of the available information given in the Certificate
1481 (Applicant's name and legal address, contact person, Applicant's contact email
1482 address);

1483 [c] The renewal of a Certificate (with a re-assessment based on an impact
1484 analysis) in case of a change of the Component;

1485 [d] The withdrawal of a Certificate when the Component does not meet anymore
1486 its security requirements.

1487 **Req.6820** The Applicant shall be responsible for:

1488 [a] The monitoring of vulnerabilities or new threats to the certified Components.

1489 **Note:** The management of the Certificate is not specific to the ICCS and should be aligned
1490 with other European schemes (like the SOG-IS transposition scheme).

1491 **6.7 Monitoring, Maintenance and Renewal of Statements of Conformity**

1492 **6.7.1 Monitoring and maintenance of Statement of Conformity**

1493 **Req.6830** As soon as a Manufacturer issues a Statement of Conformity, the Manufacturer shall
1494 maintain the Component to be compliant with the requirements of the Assurance
1495 Level Basic during the whole availability period of its Component.

1496 **Req.6840** This activity shall include the monitoring of the potential vulnerabilities that are
1497 present in the Component.

1498 **Req.6850** This activity shall also include the provision of up-to-date information concerning the
1499 contact (an e-mail address) to be addressed if any third party finds a vulnerability in
1500 the Component.

1501 **Req.6860** The Manufacturer shall revoke its Statement of Conformity if it is discovered that the
1502 Component is no longer compliant with the requirements of the Assurance Level
1503 Basic.

ICCSGG- Req.0250	The ICCSGG or the respective ENISA Ad hoc Working Group shall define a monitoring mechanism for statements of conformity issued under the ICCS using a sampling method to confirm that the requirements for content and supporting information are being met. It is recognised that this sort of sampling of statements of conformity may be an activity that is defined in a common manner across all European Cybersecurity Certification Schemes.
-----------------------------	--

1504

Example: of recommendations for sampling of ICCS statements of conformity.

Note that in this example a number of threshold values are identified and marked with ‘##’. These thresholds should be elaborated by the respective ENISA Ad hoc Working Group at the extent that the respective parts of the example are adopted for the ICCS.

The example defines two phases: the first phase (phase A) has higher target rates (i.e. more cases are examined) in order to establish a common understanding and consistent approach, since the scheme is still new, and therefore misunderstandings and inconsistencies are more likely to occur as participants are still becoming accustomed to the requirements. The second phase (phase B) has lower target rates (i.e. fewer cases are examined) on the assumption that common and consistent practices have already been established during the initial phase and all the involved entities are familiar with them.

Phase A. During the first 24 months of the implementation of ICCS

- i. Each NCCA should check the content of each Statement of Conformity that is submitted to it, to confirm that it meets the requirements for content of the Statement of Conformity.
- ii. Each NCCA should check each Statement of Conformity that is submitted to it, to confirm that it accurately and precisely identifies a specific CuA that, at the time of the check, can be obtained by a potential customer (e.g. by observing the availability of the identified device on the Manufacturer’s website).
- iii. Each NCCA should check that, for each Statement of Conformity that is submitted to it, the mechanisms for reporting vulnerabilities and identifying updates to address vulnerabilities, as described in the relevant vulnerability management process in the ENA, are available as described (e.g. by observing a working communication mechanism on the Manufacturer’s website, or contacting an identified helpdesk).
- iv. Each NCCA should sample the ENA for ## % of the statements of conformity that are submitted to it, to confirm that all the required inputs have been identified and included.
- v. For each set of ENA that is sampled as above, the NCCA should select several items from the ENA to confirm that the content provides the relevant level of description and evidence to support the Statement of Conformity. The sets sampled in this way should be chosen so that the NCCA has sampled at least two examples of each input type for the statements of conformity that have been submitted to it over a 12-month period.
- vi. For all updates to any Statement of Conformity that has been submitted to it, each NCCA should confirm that the chain length is not greater than 2 and that the ENA has been updated (sampling of the content of the updated information should be included as part of the sampling in iv – v).

Phase B. After the initial 24 months of the implementation of ICCS

- i. Each NCCA should check the content of all statements of conformity that are submitted to it, to confirm that they meet the requirements for content of the Statement of Conformity.
- ii. Each NCCA should regularly sample statements of conformity and their associated ENA to confirm each of the following items, with the associated target levels of sampling:

- Target level: ## % - That the Statement of Conformity accurately and precisely identifies a specific CuA that, at the time of the check, can be obtained by a potential customer (e.g. by observing the availability of the identified device on the Manufacturer's website).
 - Target level: ## % - That the mechanisms for reporting vulnerabilities and identifying updates to address vulnerabilities, as described in the relevant vulnerability management process in the ENA are available as described (e.g. by observing a working communication mechanism on the Manufacturer's website, or contacting an identified helpdesk).
 - Target level: ## % - That all the required inputs have been identified and included in the ENA.
 - Target level: ## % - That the content of the ENA provides the relevant level of description and evidence to support the Statement of Conformity. The sets of ENA items sampled in this way should be chosen so that the NCCA has sampled at least one example of each input type for the statements of conformity that have been submitted to it over a ## period.
- iii. Each NCCA should check all updates to any Statement of Conformity that has been submitted to it, to confirm that the chain length is not greater than 2 and that the ENA has been updated (sampling of the content of the updated information should be included as part of the sampling in ii).

6.7.2 Renewal of Statement of Conformity

Note: When a Manufacturer wishes to update a Statement of Conformity (e.g. for a new CuA version or when the availability period of the Statement of Conformity is expired), then the Manufacturer may either carry out the complete Self-Assessment process for the new CuA version, or else the Manufacturer may identify the changes made to a CuA with respect to a previous Statement of Conformity. In the latter case, the later Statement of Conformity is described as being "chained" to the previous Statement of Conformity, and the later assessment is referred to as a "delta assessment".

Req.6870 A chain of statements of conformity shall be no longer than 2: i.e. the previous Statement of Conformity referred to in a chained Statement of Conformity shall always relate to a full assessment (not a delta assessment) of the Component.

Req.6880 In a delta assessment, the Manufacturer shall perform the following actions:

- [a] The changes to the Component, relative to the version in the previous assessment, shall be identified from the chained Statement of Conformity (e.g. by reference to a publicly available document identifying the changes);
- [b] Any additional security vulnerabilities corrected in the new version of the Component shall be identified from the chained Statement of Conformity (e.g. by reference to a publicly available document identifying the vulnerabilities corrected);

- 1525 [c] The ENA shall be updated to include a description of the impact of the changes
 1526 on the Security Function of the Component, and on the ENA evidence for the
 1527 previous CuA;
 1528 [d] Updates shall be supplied, as part of the new ENA, for all impacted ENA evidence
 1529 for the previous CuA. The updates shall demonstrate that the security
 1530 properties established for the previous version still hold for the new version.
 1531 The updates shall include a statement of the testing carried out on the new
 1532 version and a rationale for why this is sufficient to demonstrate not only the
 1533 intended new functionality, but also the preservation of the previous security
 1534 properties.
 1535 **Req.6890** To register the chained Statement of Conformity for the new version, the
 1536 Manufacturer shall follow the same process as for the initial Statement of Conformity.

1537 **6.8 The ICCS Governance Group: Role and responsibility of the ICCSGG**

1538 The governance group for the Industrial Cybersecurity Certification Scheme (ICCSGG) is the group
 1539 responsible for decisions regarding the scheme after it has been initiated. The requirements for the
 1540 ICCSGG are separately identified throughout this document with the tag 'ICCSGG-Req'. This Section
 1541 contains the top-level requirements for creating the ICCSGG and for its basic composition,
 1542 operation, and responsibilities. The ICCSGG requirements that are identified in the other Sections
 1543 regard the low-level ICCSGG functional responsibilities that are specifically related to some
 1544 individual aspect of ICCS.

ICCSGG- Req.0260	The ICCS Governance Group (ICCSGG) shall be composed of NCCA representatives, one from each participating NCCA ² .
-----------------------------	---

1545

ICCSGG- Req.0270	<p>The ICCSGG shall set up its Terms of Reference (ToR). These ToR shall be based on the ToR of the ECCG, especially regarding decision making. Particular considerations for the ICCSGG ToR shall cater for:</p> <ul style="list-style-type: none"> [a] Allowing an NCCA that is unable to participate (e.g. because the ICCS is not operational within the concerned Member State) to delegate its representation to another NCCA; [b] Allowing additional experts to participate as observers, after having been confirmed by the ICCSGG (possibly limited to particular activities such as subgroups or individual meetings); [c] Specifying membership and participation in terms of individuals and organisations, i.e. allowing substitution of individuals participating in ICCSGG and its individual activities; [d] Setting up subgroups with their own ToR and membership requirements, e.g. for dealing with technical matters such as the elaboration and validation of
-----------------------------	--

² Participation is open to all NCCAs within the European CyberSecurity Act, but it is recognised that some nations may choose not to participate in the ICCSGG.

European generic Component Context Analysis (EU gCCA). These subgroups should be staffed with experts and national delegates as appropriate for the subject matter, especially including industry representatives, members of standard developing organisations and Conformity Assessment bodies. When selecting the experts should be adequately represented to the possible extent. The subgroups may be temporary or permanent.

1546 6.8.1 Responsibilities of the ICCSGG

ICCSGG- Req.0280	<p>The ICCSGG shall achieve harmonization of the ICCS definition and its operation in terms of aspects that need to be agreed on in order to harmonise individual national practice, therefore making the ICCS results consistent. More specifically it has the following tasks (some tasks may be delegated to subgroups):</p> <ul style="list-style-type: none"> [a] Developing and maintaining ICCS requirements for generic Component Context Analysis, Component Cybersecurity Profiles, Assurance Levels and Component Cybersecurity Requirements (ICR) catalogue; [b] Resolving any disputes/disagreements that may rise during the Peer Assessment of the Peer Review; [c] Harmonizing the procedures to be carried out by a Home NCCA; [d] Developing and maintaining licensing criteria for CBs, including TestLabs (Section 6.2); [e] Developing and maintaining accreditation criteria for CBs (Section 6.2); [f] Managing the Peer Assessment process for NCCAs and CBs (Section 6.2); [g] Defining and maintaining Technical Domains, if any (Section 6.2); [h] Harmonizing categorization and terminology, e.g. the list of recognised ICCS Component families; [i] Elaboration and Approval of EU gCCAs; [j] Publication of information on the ICCS, including listing approved EU gCCAs in cooperation with ENISA; [k] Developing and maintaining evaluation mechanisms for meeting ICCS requirements; [l] Developing and maintaining supporting documents, e.g. regarding attack methods used during evaluation or defining acceptance criteria not explicitly specified in the evaluation standards; [m] Resolve open technical issues related to ICCS; [n] Sampled validation of information supplied in support of statements of conformity (Section 6.7.1); [o] Work to obtain mutual recognition of ICCS ECC with countries outside the EC.
-----------------------------	---

1547

7 ICCS Supporting Documents

7.1 IACS Components Cybersecurity Requirements (ICR) Catalogue

The proposed ICCS scheme is built on top of already available internationally recognized standards, while at the same time it is designed to allow maximum flexibility to the users in terms of which standard is being used as a source of security requirements.

Note: It is seen from the examples of other functional certification schemes (e.g. SOG-IS or IECCE) that in practice it is of high importance that the proposed scheme provides its users with a list of possible security requirements which can be further used, or extended, in evaluations. Moreover, Article 54 of the CSA foresees, among the minimum elements for the definition of EU certification schemes, that a scheme should determine the specific evaluation criteria to be used in order to demonstrate the completeness of the defined Security Objectives.

To this end, in this report, it is proposed to create a catalogue of relevant cybersecurity requirements (IACS Components Cybersecurity Requirements – ICR). This catalogue may serve as a base for conducting evaluations in line with the proposed scheme, as well as a basis for further drafting generic Component Context Analysis for certain types of IACS Components (e.g. PLC devices). The catalogue may be defined by extracting relevant security requirements from internationally recognized sources, such as:

- ENISA – “Indispensable baseline security requirements for the procurement of secure ICT product and services”, December 2016
- IEC 62443-4-2, “Technical security requirements for IACS Components”, February 2019
- ISO/IEC 15408, Part 2, “Security Functional Requirements”, April 2017
- NIST SP 800-82, “Guide to industrial systems security”, May 2015

Further sources may be added. At the same time, it needs to be kept in mind that the abovementioned publications might receive updates, which will lead to necessary updates also to the catalogue of requirements.

Starting from the publications mentioned above, the following process steps should be followed in the creation of the proposed ICR catalogue:

- [a] Extraction of relevant security requirements from the above identified sources
- [b] Grouping of all the requirements into several catalogue categories
- [c] Analysis and overlap of the requirements, in order to avoid duplications and un-clarities
- [d] Addition of possible enhancements on top of the Basic requirements

The catalogue of requirements could be formatted as in the table below. In the catalogue, all the applicable requirements will be clearly presented.

Category	Requirement number	Requirement name	Requirement text	Requirement enhancements	Source publication	Comments and remarks
----------	--------------------	------------------	------------------	--------------------------	--------------------	----------------------

Explanation: Category of requirements, for example Identification and authentication control	Explanation: the number of the requirement, for clear traceability	Explanation: name of the requirement	Explanation: Text of the requirement	Explanation: Possible enhancements to the original requirement	Explanation: Publication from which the requirement is extracted	Explanation: Remarks on the usage and interpretation of the requirement
--	--	--	--	--	--	---

Table 5 – Example of format for the ICR catalogue

Example of catalogue categories

These categories of grouped requirements are defined in line with the Foundational Requirements from IEC 62443-1-1:

- Identification and authentication control;
- Use control;
- System Integrity;
- Data confidentiality;
- Restricted data flow;
- Timely response to events;
- Resource availability

ICCSGG-Req.0290 The ICCSGG or the respective ENISA Ad hoc Working Group shall define an ICR Catalogue.

Note: The ICR catalogue does not aim to provide a mapping of the security requirements to the Assurance Levels defined in the CSA. This mapping would be possible, but it is considered that it will lead to Component specific implementations, as some requirements (and their enhancements) will be more relevant for some types of IACS Components compared to others (between hardware devices and software IACS applications for example). Such mappings may be considered in the drafting of future (generic) Component Cybersecurity Profiles defined under the proposed IACS scheme, which may take the ICR catalogue as a base for the selection of security requirements.

ICCSGG-Req.0300 The ICCS Governance Group (ICCSGG) shall continuously monitor and improve the ICR.

Example of continuous monitoring and improvement actions:

- Monitoring of the considered publications, in order to include in the ICR catalogue new versions of such publications;
- Monitoring of other relevant international publications providing security requirements related to the domain of IACS Components, and possible integration of these requirements into the ICR catalogue;
- Tailoring of the presented requirements, to ensure efficient usage within the ICCS.

1595

1596 7.2 IACS Components Cybersecurity Evaluation Report Table of Contents (ICERT)

1597 **Req.7010** The ICERT shall, at minimum, address the contents given in the table below. It should
1598 be augmented by testing protocols, scripts, configuration of tools or further
1599 information necessary to understand the results.

Title	Expected Content
Introduction	Explanation what this ICERT is for, definition/glossary, references
Identifications	Precise and short identification of all parties (laboratory, Applicant, CB) and CuAs involved
Overview	A description of the CuA under testing, its environment, typical users etc.
Document analysis	Results on the analysis of the CCP and other documents provided for evaluation.
Installation	How the CuA under testing installed and any observations thereof.
Conformity analysis	An overview of what was analysed/tested ("Security Functions") and a description of the results.
Vulnerability analysis	A description of the testing strategy, and, for each test case, the results including a rationale for the verdict.
Cryptography	If applicable for the evaluation method, an overview of the results of the cryptographic evaluation.
Conclusion	The results and the verdict proposed by the CB in the light of the CCP and Article 51 of the Cyber Security Act

1600

Table 6 – Table of contents for the ICERT

1601 **Req.7020** Where the Assessment Team uses self-developed tools, those shall be described in
1602 an annex.

1603 **Req.7030** The ICERT shall contain, for each test case:

1604 [a] Test description with test expectation;

1605		[b] Test preparation;
1606		[c] Testing steps;
1607		[d] The test result
1608	Req.7040	If certain evaluation steps are not relevant for the Assurance Level (e.g. vulnerability
1609		analysis) those parts of the ICERT shall be left off.
1610	Note:	The ICERT forms the basis of the decision of the CB and in case of investigations by
1611		the NCCA Supervision the basis for their findings.
1612		
1613	7.3 IACS Component Cybersecurity Certificates Contents (IC3)	
1614	Req.7050	IC3 shall contain the following information:
1615		[a] The name and contact information of the Applicant;
1616		[b] The name of the CuA;
1617		[c] The type of the CuA;
1618		[d] All relevant version information for the CuA (including, where applicable,
1619		hard-, soft- and firmware versions);
1620		[e] How to uniquely identify the CuA ³ ;
1621		[f] The name and contact information of the TestLab that performed the
1622		evaluation (if applicable);
1623		[g] The name and contact information of the body that issued the Certificate
1624		including the responsible NCCA;
1625		[h] Contact information for security reports;
1626		[i] The applicable Assurance Level according to the CSA (Basic, Substantial or
1627		High);
1628		[j] The identification of the certification report;
1629		[k] The IT security evaluation criteria and methodology used and their version;
1630		[l] The identification of the CCP (title and version) that has been used for the
1631		evaluation of the CuA;
1632		[m] The identification of any gCCA (if applicable) that has been used;
1633		[n] Validity period of the Certificate;
1634		[o] The period during which support shall be offered to end-users, in particular
1635		as regards the availability of cybersecurity related updates;
1636		[p] Any further information required by the applicable Evaluation Methodology ⁴ .
1637	Req.7060	A Certificate shall always be accompanied by an ICERT

³ This is a high level description suitable for the expected users, while in the ICERT might contain a longer and more technical description.

⁴ For example, the SL level for IEC 62443 or the EAL level for ISO/IEC 15408.

ICCSGG- Req.0310	The ICCSGG or the respective ENISA Ad hoc Working Group shall devise the list of CuA types to be used in the IACS Component Cybersecurity Certificates.
-----------------------------	---

7.4 IACS Component Statement of Conformity Contents

Req.7070 The IACS Component Statement of Conformity shall contain the following information:

- [a] The name and contact information of the Manufacturer;
- [b] The name of the CuA;
- [c] The type of the CuA;
- [d] All relevant version information for the CuA (including, where applicable, hard-, soft- and firmware versions);
- [e] How to uniquely identify the CuA⁵;
- [f] The composition of the Assessment Team that performed the assessment;
- [g] Contact information for security reports;
- [h] The applicable Assurance Level according to the CSA: Basic;
- [i] The IT security evaluation criteria and methodology used and their version;
- [j] The identification of the CCP (title and version) that has been used for the evaluation of the CuA;
- [k] The identification of any gCCA (if applicable) that has been used;
- [l] Validity period of the Statement of Conformity;
- [m] Any further information required by the applicable Evaluation Methodology.

⁵ This is a high level description suitable for the expected users, while in the Statement of Conformity might contain a longer and more technical description.

Annex A

Coverage of CSA by ICCS and Existing Evaluation Approaches

A.1 Mapping Between CSA and ICCS

This Section summarises the ways in which ICCS meets the requirements of the EU CyberSecurity Act.

Title III of the, in Articles 46 to 65, contains the main rules and principles for defining certification schemes. In brief, Articles 46-50 contain general requirements for the operation of the framework, and do not contain requirements for individual schemes, so these are not discussed any further in this report. Articles 51-55 contain the main requirements, and therefore they are mapped in detail in Subsections below. Articles 56-65 describe requirements that are outside the scope of the ICCS itself and therefore are not discussed any further, except for the following notes:

- Article 59 refers to Peer Review above the level of an individual scheme. It is noted that Peer Review processes within the ICCS scheme are covered by Article 54, Paragraph 1.u;
 - Article 60 refers to accreditation of CBs independently of individual schemes, which is assumed for the purposes of this report. Suggested approaches to authorisation and accreditation of CBs for the purposes of ICCS are described in Section 6.2;
 - Article 61 refers to the notification of accredited CBs by NCCAs to the Commission. This is covered for ICCS in Section 6.2;
- Article 63 refers to the right to lodge complaints against issuers of Certificates. This is covered for ICCS in Section 6.1.

A.1.1 Correspondence of ICCS to Article 51 of the EU CyberSecurity Act (Security Objectives of European Cybersecurity Certification Schemes)

Text	Implementation in ICCS
A European Cybersecurity Certification Scheme shall be designed to achieve, as applicable, at least the following Security Objectives:	
a) To protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process	ICCS uses generic Component Context Analysis (gCCA) and Component Cybersecurity Profile (CCP) documents that relate threats and assumptions to assets and thereby deduce required Security Functions and assurance requirements, as described in Section 6.3. This approach will therefore cover appropriate protection of stored and transmitted/processed data. The Evaluation Activities for gCCA and CCP in Section 5.1 ensure that the threats are identified through a risk analysis, taking account of the intended operating conditions.

Text	Implementation in ICCS
(b) To protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process	As for (a)
(c) That authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer	As for (a)
(d) To identify and document known dependencies and vulnerabilities	Known dependencies of a Component are identified in the gCCA and/or CCP as part of the expected operating conditions (Section 4.2). Known vulnerabilities are required to be managed according to an internal vulnerability management procedure which is a required deliverable for all Assurance Levels (Section 4.3). This deliverable is analysed by the Assessment Team to check for continuous monitoring and response by the Manufacturer (Section 5.2). In addition, at higher Assurance Levels, the evaluator vulnerability analysis (Section 5.5) and penetration testing (Section 5.7) check the absence of publicly known vulnerabilities. Vulnerability dependencies monitoring from other parts of the Component are also handled in Section 5.2.
(e) To record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom	As for (a)
(f) To make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom	As for (a)
(g) To verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities	As for (d)
(h) To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident	As for (a)
(i) That ICT products, ICT services and ICT processes are secure by default and by design	ICCS requires that the Manufacturer submits a documented “secure by default and by design strategy” as part of their defence-in-depth

Text	Implementation in ICCS
	protection strategy (Section 4.1), and this is reviewed by the Assessment Team to check that it meets the content requirements (Section 5.2). In addition, it is noted that the general Evaluation Activities will assess that Components are secure by default and by design (Section 5).
(j) That ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates	ICCS includes evaluation of the Manufacturer's vulnerability management process and the Patch and Obsolescence Management procedure from the Basic level, and requires this process to include timely availability of secure updates, and to include security regression testing of updates (Section 5.2.2). For all Assurance Levels, the Assessment Team will review the mechanism implemented by the Component for secure updates at least as part of the documentation analysis (Section 5.2.2). Where secure update functionality is included in the Component Cybersecurity Requirements (CCR) then this will be assessed and tested as part of the evaluated functionality.

Table 7 – Correspondence of ICCS to Article 51

A.1.2 Correspondence of ICCS to Article 52 of the EU CyberSecurity Act (Security Objectives of European Cybersecurity Certification Schemes)

Text	Implementation in ICCS
Paragraph 1. A European Cybersecurity Certification Scheme may specify one or more of the following Assurance Levels for ICT products, ICT services and ICT processes: 'Basic', 'Substantial' or 'High'. The Assurance Level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.	ICCS includes provisions for every Assurance Level based on the consensus of industry experts involved in the definition of the requirements and Evaluation Activities in Section 4 and Section 5. The ICCS is intended to be updated over time, to incorporate expected improvements in the state of the art, as part of the activity of the ICCSGG.
Paragraph 2. European cybersecurity Certificates and EU statements of conformity shall refer to any Assurance Level specified in the European Cybersecurity Certification Scheme under which the European cybersecurity Certificate or EU Statement of Conformity is issued.	The Assurance Levels referenced by Cybersecurity Certificates and EU Statements of Conformity are described in Section 3. These Assurance Levels will be referenced in the ICCS Certificates and EU Statements of Conformity issued as described in Sections 7.3 and 7.4.
Paragraph 3. The security requirements corresponding to each Assurance Level shall be	The requirements for Assurance Levels in ICCS are described in Section 3 and Section 4 (and in

Text	Implementation in ICCS
provided in the relevant European Cybersecurity Certification Scheme, including the corresponding Security Functions and the corresponding rigour and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.	more detail by the Evaluation Activities in Section 5). Functional security requirements for a Component are defined i) generically in a gCCA, and/or ii) specifically for the concerned Component in its CCP (Section 4.2 and Section 6.3), based on the risk analysis for the Component.
Paragraph 4. The Certificate or the EU Statement of Conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.	The ICCS scheme is intended to be based on standardised criteria and methodologies such as ISO/IEC 15408 & 18045 (Common Criteria), IEC 62443-4-1 & 62443-4-2, and the various ‘lite’ methodologies such as CSPN, BSZ, Lince and the emerging “Cybersecurity Evaluation Methodology for ICT products” from CEN-CENELEC JTC13 WG3. However, as noted in Section 5, “at the moment of delivery of this report, there is no single standard that adequately covers the whole set of the Evaluation Activities defined by the ICCS as necessary to evaluate IACS Components”. The choice of specific standards to be referenced will therefore be determined by choices to be made during the preparation of the ICCS. Relevant standards for use in the detailed requirements and Evaluation Activities are described in Annex B Relevant Standards.
Paragraph 5. A European cybersecurity Certificate or EU Statement of Conformity that refers to Assurance Level Basic shall provide assurance that the ICT products, ICT services and ICT processes for which that Certificate or that EU Statement of Conformity is issued meet the corresponding security requirements, including Security Functions, <i>(continues below)</i>	The CCP identifies the Security Function that is covered by the Certificate, as described in Section 6.3.
<i>(continued)</i> and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. <i>(continues below)</i>	The Assurance Levels referenced by Cybersecurity Certificates and EU Statements of Conformity are described in Section 3. It is noted for the overall requirements for assessments in Section 3.1 that the Evaluation Activities (Section 5) for Assurance Level Basic assess whether the Components minimise the known basic risks of cybersecurity incidents and cyberattacks.

Text	Implementation in ICCS
	The minimisation of known basic risks is also achieved by the definition of the ICCS Assurance Levels as described for Article 52, Paragraph 1 above.
<i>(continued)</i> The Evaluation Activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute Evaluation Activities with equivalent effect shall be undertaken.	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. These include a review of technical documentation for the Assurance Level Basic (Section 5.2), either for an EU Statement of Conformity or for a Cybersecurity Certificate.
Paragraph 6. A European cybersecurity Certificate that refers to Assurance Level Substantial shall provide assurance that the ICT products, ICT services and ICT processes for which that Certificate is issued meet the corresponding security requirements, including Security Functions, <i>(continues below)</i>	The CCP identifies the Security Function that is covered by the certification, as described in Section 6.3.
<i>(continued)</i> and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. <i>(continues below)</i>	<p>The Assurance Levels referenced by the Cybersecurity Certificates and EU Statements of Conformity are described in Section 3. These Assurance Levels will be referenced in the ICCS Certificates issued as described in Section 7.3. It is noted for the overall requirements for assessments in Section 3.1 that the Evaluation Activities (Section 5) for Assurance Level Substantial assess whether the Components minimise the known cybersecurity risks and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.</p> <p>The minimisation of known limited risks is also achieved by the definition of the ICCS Assurance Levels as described for Article 52, Paragraph 1 above.</p>
<i>(continued)</i> The Evaluation Activities to be undertaken shall include at least the following: <i>(continues below)</i>	
<i>(continued)</i> a review to demonstrate the absence of publicly known vulnerabilities <i>(continues below)</i>	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. For the Assurance Level Substantial, these include a review to demonstrate the absence of publicly known vulnerabilities (Section 5.5.2.1).

Text	Implementation in ICCS
<i>(continued)</i> and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary Security Functions. Where any such Evaluation Activities are not appropriate, substitute Evaluation Activities with equivalent effect shall be undertaken.	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. For the Assurance Level Substantial, these include testing of the Security Function as well as robustness testing (see Section 5.4 and 5.2.2.2).
Paragraph 7. A European cybersecurity Certificate that refers to Assurance Level High shall provide assurance that the ICT products, ICT services and ICT processes for which that Certificate is issued meet the corresponding security requirements, including Security Functions, <i>(continues below)</i>	The CCP identifies the Security Function that is covered by the certification, as described in Section 6.3.
<i>(continued)</i> and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. <i>(continues below)</i>	<p>The Assurance Levels referenced by Cybersecurity Certificates and EU Statements of Conformity are described in Section 3. It is noted for the overall requirements for assessments in Section 3.1 that the Evaluation Activities (Section 5) for Assurance Level High assess whether the Components minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.</p> <p>The minimisation of significant risks is also achieved by the definition of the ICCS Assurance Levels as described for Article 52, Paragraph 1 above.</p>
<i>(continued)</i> The Evaluation Activities to be undertaken shall include at least the following: <i>(continues below)</i>	
<i>(continued)</i> a review to demonstrate the absence of publicly known vulnerabilities; <i>(continues below)</i>	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. For the Assurance Level High, these include a review to demonstrate the absence of publicly known vulnerabilities (Section 5.5.2.2).
<i>(continued)</i> testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary Security Functions at the state of the art; <i>(continues below)</i>	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. At the High level these include testing of the Security Function (see Section 5.4 and 5.2.2.3 and Section 5.7).

Text	Implementation in ICCS
<i>(continued)</i> and an assessment of their resistance to skilled attackers, using penetration testing. Where any such Evaluation Activities are not appropriate, substitute activities with equivalent effect shall be undertaken.	The ICCS Evaluation Activities are described in Section 5, based on the requirements for the Assurance Levels described in Section 3. For the Assurance Level High, these include extended vulnerability analysis (Section 5.5) and penetration testing (Section 5.7) to assess the resistance to skilled attackers. The ICCSGG shall define precisely how the penetration activity shall be carried out as part of the ICCS.
Paragraph 8. A European Cybersecurity Certification Scheme may specify several evaluation levels depending on the rigour and depth of the Evaluation Methodology used. Each of the evaluation levels shall correspond to one of the Assurance Levels and shall be defined by an appropriate combination of assurance Components.	The ICCS Assurance Levels described in Section 3 correspond directly to the Assurance Levels described in the CyberSecurity Act.

Table 8 – Correspondence of ICCS to Article 52

A.1.3 Correspondence of ICCS to Article 53 of the EU CyberSecurity Act (Conformity Self-Assessment)

Text	Implementation in ICCS
Paragraph 1. A European Cybersecurity Certification Scheme may allow for the conformity Self-Assessment under the sole responsibility of the Manufacturer or provider of ICT products, ICT services or ICT processes. Conformity Self-Assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to Assurance Level 'Basic'.	ICCS allows for conformity Self-Assessment of IACS CuAs, only at the Basic Assurance Level.
Paragraph 2. The Manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU Statement of Conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the Manufacturer or provider of ICT products, ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.	Section 3.1.1 describes the way in which ICCS conformity Self-Assessment works. The ICCS approach is consistent with this requirement.

Text	Implementation in ICCS
Paragraph 3. The Manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU Statement of Conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European Cybersecurity Certification Scheme. A copy of the EU Statement of Conformity shall be submitted to the national cybersecurity certification authority and to ENISA.	Section 3.1.1 describes the way in which ICCS conformity Self-Assessment works. The ICCS approach is consistent with this requirement. The Elements Necessary for Evaluation (ENA) are required to remain available to the National Cybersecurity Certification Authority for the period of validity of the EU Statement of Conformity (Section 4.1). A copy of the EU Statement of Conformity shall be submitted to the National Cybersecurity Certification Authority and to ENISA (Section 3.1.1).
Paragraph 4. The issuing of an EU Statement of Conformity is voluntary, unless otherwise specified in Union law or Member State law.	Issuing an EU Statement of Conformity based on ICCS is a voluntary action.
Paragraph 5. EU statements of conformity shall be recognised in all Member States.	(This is outside the scope of the present report)

Table 9 – Correspondence of ICCS to Article 53

A.1.4 Correspondence of ICCS to Article 54 of the EU CyberSecurity Act (Elements of European Cybersecurity Certification Schemes)

Text	Implementation in ICCS
Paragraph 1. A European Cybersecurity Certification Scheme shall include at least the following elements:	
(a) The subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered	Section 2 describes the function and scope of ICCS.
(b) A clear description of the purpose of the scheme and of how the selected standards, evaluation methods and Assurance Levels correspond to the needs of the intended users of the scheme	Section 2 describes the purpose of ICCS. Refer to the Correspondence of ICCS to Article 52 (A.1.2), Paragraph 1 for discussion regarding the rationale for the standards, evaluation methods and Assurance Levels used in ICCS.
(c) References to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such	Refer to the Correspondence of ICCS to Article 52 (A.1.2), Paragraph 4. Section 5, Annex B and Annex C describe the role of standards applicable to ICCS evaluations. As described, it is part of the role of the ICCS

Text	Implementation in ICCS
specifications are not available, to technical specifications or other cybersecurity requirements defined in the European Cybersecurity Certification Scheme	Governance Group to maintain the list of evaluation approaches, and hence underlying standards, that can be used for ICCS.
(d) Where applicable, one or more Assurance Levels	Section 3 describes the Assurance Levels used in ICCS. These are Basic, Substantial and High as in the CyberSecurity Act.
(e) An indication of whether conformity Self-Assessment is permitted under the scheme	Section 3 describes the use of conformity Self-Assessment for EU Statements of Conformity at the Basic Assurance Level.
(f) Where applicable, specific or additional requirements to which Conformity Assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements	The requirements on CBs for ICCS are described in Section 6.2. Note that in ICCS terminology: certification activities are performed by a 'Certification Body'; Evaluation Activities are performed by 'Assessment Teams' that consist of 'evaluators'.
(g) The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the Security Objectives referred to in Article 51 are achieved	<p>Section 5 describes the Evaluation Activities applicable to ICCS evaluations, including the underlying standards. These define the criteria and methods used.</p> <p>Refer also to the more detailed mapping of Article 51 requirements above (A.1.1), and to the response to Article 52 (A.1.2), Paragraph 4 (related to technical specifications, standards and procedures).</p>
(h) Where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the Conformity Assessment bodies by an Applicant	This information is described in Section 4.1. More details of the relevant information are offered in the description of the Evaluation Activities in Section 5.
(i) Where the scheme provides for marks or labels, the conditions under which such marks or labels may be used	No specific marks or labels are used in ICCS.
(j) Rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity Certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements	Section 6.6 describes the monitoring, maintenance, renewal and withdrawal of ICCS Certificates; Section 6.7 describes the same processes for EU Statements of Conformity.

Text	Implementation in ICCS
(k) Where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity Certificates, as well as the conditions for extending or reducing the scope of certification	<p>Section 6.6 describes the monitoring, maintenance, renewal and withdrawal of ICCS Certificates. Reducing or extending the scope of an existing ICCS Certificates would be dealt with by the maintenance or renewal processes.</p> <p>Extension of Security Functions in a CCP relative to a gCCA is described in Section 6.3.3.</p>
(l) Rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU Statement of Conformity has been issued, but which do not comply with the requirements of the scheme	<p>Section 6.6 describes the monitoring, maintenance, renewal and withdrawal of ICCS Certificates; Section 6.7 describes the same processes for EU Statements of Conformity. A Component that was certified (or issued a Statement of Conformity) under ICCS but was subsequently found not to comply with ICCS requirements would be dealt following the withdrawal process.</p> <p>The specific process for checking EU Statements of Conformity, in order to identify non-compliant cases, is described in Section 6.7.</p>
(m) Rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with	<p>The Manufacturer's vulnerability handling process is included in the scope of the ICCS evaluation for all the three Assurance Levels (Section 4). ICCS expects that a vulnerability disclosure procedure is defined (Section 6.4). The effect of newly discovered vulnerabilities on ICCS Certificates is described in Section 6.7.</p>
(n) Where applicable, rules concerning the retention of records by Conformity Assessment bodies	<p>The ICCS scheme requires Certification Bodies and Assessment Teams to retain records as stated in Section 6.2.2.</p>
(o) The identification of national or international Cybersecurity Certification Schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and Assurance Levels	<p>ICCS is intended to be based on standardised criteria and methodologies. However, as noted in Section 5, "At the moment of delivery of this report, there is no single standard that adequately covers the whole set of the Evaluation Activities defined by the ICCS as necessary to evaluate IACS Components". The choice of specific standards to be referenced will therefore be determined by choices to be made during preparation of the ICCS.</p> <p>Therefore, there is no current overlapping scheme.</p>

Text	Implementation in ICCS
(p) The content and the format of the European cybersecurity Certificates and the EU statements of conformity to be issued	The content of ICCS Certificates and EU Statements of Conformity is described in Sections 7.3 and 7.4. The specific format of the Certificate (or EU Statement of Conformity) is not defined in this document but it is to be included in the implementation activities (under the control of the ICCSGG).
(q) The period of the availability of the EU Statement of Conformity, technical documentation, and all other relevant information to be made available by the Manufacturer or provider of ICT products, ICT services or ICT processes	Section 4.1 contains a requirement that the ENA for an ICCS Certificate or an EU Statement of Conformity needs to be available for the validity period of the respective ICCS Certificate or EU Statement of Conformity. Periods of validity of ICCS Certificates and EU Statements of Conformity are to be defined in the future by the ICCSGG, as required in Section 3.3.
(r) Maximum period of validity of European cybersecurity Certificates issued under the scheme	Periods of validity of ICCS Certificates and EU Statements of Conformity are to be defined in the future by the ICCSGG, as required in Section 3.3.
(s) Disclosure policy for European cybersecurity Certificates issued, amended or withdrawn under the scheme	Section 6.6 describes the publication, monitoring, maintenance, renewal and withdrawal of ICCS Certificates.
(t) Conditions for the mutual recognition of certification schemes with third countries	The use of mutual recognition for ICCS has not yet been defined (Section 6.5), and work on mutual recognition with third countries would be a matter for the ICCSGG.
(u) Where applicable, rules concerning any Peer Assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity Certificates for Assurance Level 'High' pursuant to Article 56(6). Such mechanism shall be without prejudice to the Peer Review provided for in Article 59	Refer to Section 6.2.
(v) Format and procedures to be followed by Manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55	The procedures to be followed for supplying the ENA are described in Section 4. Amendment of information would be covered by the processes for monitoring, maintenance, renewal and withdrawal, as described in Section 6.6 and Section 6.7.
Paragraph 2. The specified requirements of the European Cybersecurity Certification Scheme shall be consistent with any applicable legal	No deviations from applicable legal requirements have been identified.

Text	Implementation in ICCS
requirements, in particular requirements emanating from harmonised Union law.	
Paragraph 3. Where a specific Union legal act so provides, a Certificate or an EU Statement of Conformity issued under a European Cybersecurity Certification Scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.	(This is outside the scope of the present report)
Paragraph 4. In the absence of harmonised Union law, Member State law may also provide that a European Cybersecurity Certification Scheme may be used for establishing the presumption of conformity with legal requirements.	(This is outside the scope of the present report)

1689 Table 10 – Correspondence of ICCS to Article 54

1690 **A.1.5 Correspondence of ICCS to Article 55 of the EU CyberSecurity Act (Supplementary**
1691 **cybersecurity information for certified ICT products, ICT services and ICT processes)**

Text	Implementation in ICCS
1. The Manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU Statement of Conformity has been issued shall make publicly available the following supplementary cybersecurity information:	
(a) end-user documentation to assist end-users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;	Refer to Section 4.2.
(b) the period during which security support will be offered to end-users, in particular as regards the availability of cybersecurity related updates;	Refer to Section 4.2.
(c) contact information of the Manufacturer or provider and accepted methods for receiving vulnerability information from end-users and security researchers;	Refer to Section 4.2.
(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.	Refer to Section 4.2.
2. The information referred to in paragraph 1 shall be available in electronic form and shall	Refer to Section 4.2.

Text	Implementation in ICCS
remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity Certificate or EU Statement of Conformity.	

Table 11 – Correspondence of ICCS to Article 55

A.2 Mapping Between CSA Article 51 and Existing Evaluation Approaches

A.2.1 IEC 62443-4-1 & 62443-4-2

IEC 62443-1-1 defines seven Foundational Requirements (FR) that are used in the mapping table. These Foundational Requirements are:

- FR-1: Identification and authentication control;
- FR-2: Use control;
- FR-3: System Integrity;
- FR-4: Data confidentiality;
- FR-5: Restricted data flow;
- FR-6: Timely response to events;
- FR-7: Resource availability.

The Component Requirements (CR) derived from the seven Foundational Requirements defined in IEC 62443-1-1, and either they can be generic or they can be specialized into four different types of Components: software application, embedded device, host device and network device. When the Component Requirements are specialised, they will be designed as follows:

- Software Application Requirements (SAR);
- Embedded Device Requirements (EDR);
- Host Device Requirements (HDR);
- Network Device Requirements (NDR).

These Components requirements can be enhanced to reach higher Security Levels (as defined in IEC 62443), for example -RE(1) , -RE(2).

The table below gives the detailed mapping of individual requirements of CSA Article 51 to IEC 62443-4-1 and 62443-4-2. This demonstrates that all the relevant requirements can be met using this evaluation approach.

Req. of Article 51	IEC 62443-4-2 Requirement	SL1	SL2	SL3	SL4
To protect stored, transmitted or otherwise processed data against accidental or	CR4.1	X	X	X	X
	CR4.2		X	X	X
	-RE (1)			X	X
	-RE (2)			X	X

Req. of Article 51	IEC 62443-4-2 Requirement	SL1	SL2	SL3	SL4
unauthorized storage, processing, access or disclosure during the entire lifecycle of the ICT product, ICT service or ICT process;	CR4.3	X	X	X	X
To protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire lifecycle of the ICT product, ICT service or ICT process;	CR2.1 -RE(1) -RE(2) -RE(3) -RE(4)	X	X X X	X X X X	X X X X X
	CR3.1 -RE(1)	X	X X	X X	X X
	CR3.4 -RE (1) -RE (2)	X	X X	X X X	X X X
	CR3.8		X	X	X
	CR3.9 -RE(1)		X	X	X X
	SAR3.2	X	X	X	X
	EDR3.2	X	X	X	X
	HDR3.2 -RE (1)	X	X X	X X	X X
	NDR3.2	X	X	X	X
	CR7.1 -RE (1)	X	X X	X X	X X
	CR7.3 -RE (1)	X	X X	X X	X X
That authorized persons, programs or machines are able only to access the data, services or	CR1.1 -RE (1) -RE(2)	X	X X	X X X	X X X
	CR1.2 -RE(1)		X	X X	X X

Req. of Article 51	IEC 62443-4-2 Requirement	SL1	SL2	SL3	SL4
functions to which their access rights refer;	CR1.3	X	X	X	X
	CR1.4	X	X	X	X
	CR1.5 -RE(1)	X	X	X X	X X
	NDR1.6 -RE(1)	X	X X	X X	X X
	CR2.1 -RE(1) -RE(2) -RE(3) -RE(4)	X	X X X	X X X X	X X X X X
To identify and document known Dependencies and vulnerabilities;	Process requirement covered in IEC 62443-4-1	Practice 2 – Specification of security requirements SR-1: Product Security Context SR-2: Threat Model Practice 3 – Security by design SD-1: Secure design principles Practice 5 – Security verification and validation testing SVV-3: Vulnerability testing SVV-4: Penetration testing			
To record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	CR1.1 -RE(1) -RE(2)	X	X X	X X X	X X X
	CR1.2 RE(1)	X	X	X X	X X
	CR1.3	X	X	X	X
	CR2.8	X	X	X	X
	CR2.11 -RE(1) -RE(2)	X	X X	X X	X X X
To make it possible to check which data,	CR6.1 -RE(1)	X	X	X X	X X

Req. of Article 51	IEC 62443-4-2 Requirement	SL1	SL2	SL3	SL4
services or functions have been accessed, used or otherwise processed, at what times and by whom;					
To verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	Process requirement covered in IEC 62443-4-1	Practice 4- Secure implementation SI-1: Security implementation review SI-2: Secure coding standards Practice 5 – Security verification and validation testing SVV-3: Vulnerability testing SVV-4: Penetration testing			
To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	CR7.3 -RE(1)	X	X X	X X	X X
	CR7.4	X	X	X	X
That ICT products, ICT services and ICT processes are secure by default and by design;	Process requirement covered in IEC 62443-4-1	Practice 1 – Security management SM-1: Development process Practice 3 – Secure by design SD-1: Secure design principles SD-2: Defence in depth design SD-3: Security design review SD-4: Secure design best practices Practice 8 – Security guidelines SG-1: Product defence in depth			

Req. of Article 51	IEC 62443-4-2 Requirement	SL1	SL2	SL3	SL4
		SG-2: Defence in depth measures expected in the environment SG-3: Security hardening guidelines SG-4: Secure disposal guidelines SG-5: Secure operation guidelines SG-6: Account management guidelines SG-7: Documentation review			
That ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.	Process Requirement covered in IEC 62443-4-1	Practice 6 – management of security-related issues DM-1: Receiving notifications of security-related issues DM-2: Reviewing security-related issues DM-3: Assessing security-related issues DM-5: Disclosing security-related issues Practice 5 - Security verification and validation testing SVV-3: Vulnerability testing Practice 7 – Security update management SUM-1: Security update qualification SUM-2: Security update documentation SUM-3: Dependent Component or operating system security update SUM-4: Security update delivery SUM-5: Timely delivery of security patches Practice 8 – Security guidelines SG-1: Product defense in depth SG-2: Defense in depth measures expected in the environment SG-3: Security hardening guidelines SG-4: Secure disposal guidelines SG-5: Secure operation guidelines SG-6: Account management guidelines SG-7: Documentation review			

Table 12 – Mapping CyberSecurity Act Article 51 to IEC 62443-4-1 & IEC 62443-4-2

A.2.2 Common Criteria (ISO/IEC 15408)

1719 The following table gives a detailed mapping of individual requirements from CSA Article 51 to
 1720 Security Functional Requirement families from Common Criteria (ISO/IEC 15408-2:2008⁶), and to
 1721 aspects of the Common Evaluation Methodology (ISO/IEC 18045:2008⁷). Common Criteria is
 1722 intended to provide a selection of requirements that can be chosen according to the risk analysis in
 1723 a generic Component Context Analysis (Protection Profile or Security Target as defined in Common
 1724 Criteria), and also allows extension of the catalogue of functional requirements in Common Criteria
 1725 part 2 with user-defined requirements where appropriate. The corresponding requirements
 1726 included in the table below are therefore examples for illustration purposes only (to show that the
 1727 breadth of requirements in the CSA is covered): they do not imply that a Security Target used for
 1728 ICCS would necessarily include these Security Functional Requirements.

Req. of Article 51	Examples of Corresponding Requirements in ISO/IEC 15408
To protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire lifecycle of the ICT product, ICT service or ICT process;	FCS_CKM, FCS_COP, FDP_ACC.1, FDP_ACC.2, FDP_ACF.1, FDP_ETC, FDP_IFF.1, FDP_IFF.3, FDP_IFF.5, FDP_ITT.1, FDP_RIP.2, FIA_UAU, FIA_UID, FIA_USB
To protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire lifecycle of the ICT product, ICT service or ICT process;	FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4, FCS_CKM, FCS_COP, FDP_ACC.1, FDP_ACC.2, FDP_ACF.1, FDP_DAU, FDP_ETC, FDP_ITT.3, FDP_SDI, FIA_UAU, FIA_UID, FIA_USB
That authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	FDP_ACC.1, FDP_ACC.2, FDP_ACF.1, FIA_UAU, FIA_UID, FIA_USB
To identify and document known dependencies and vulnerabilities;	Covered by the AVA_VAN assurance family
To identify and document known dependencies and vulnerabilities; to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.2, FAU_STG.3, FAU_STG.4, FIA_UID
To make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	FAU_GEN.1, FAU_GEN.2 (*), FAU_SAR.1, FAU_STG.1, FAU_STG.2, FAU_STG.3, FAU_STG.4, FIA_UID, FMT_MTD.1
To make it possible to check which data, services or functions have been accessed, used	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.2, FAU_STG.3, FAU_STG.4, FIA_UID, FMT_MTD.1

⁶ ISO/IEC 15408 is currently under revision.

⁷ ISO/IEC 18045 is also currently under revision, alongside ISO/IEC 15408.

Req. of Article 51	Examples of Corresponding Requirements in ISO/IEC 15408
or otherwise processed, at what times and by whom;	
To verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	This is explicitly covered by the AVA_VAN assurance family and ISO/IEC 18045
To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	FDP_ROL.1, FDP_ROL.2, FMT_SMF
That ICT products, ICT services and ICT processes are secure by default and by design;	This needs to be stated in requirements in a Protection Profile or a Security Target
That ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	ISO/IEC 18045 ensures that at the time the product is certified, no known exploitable vulnerabilities exist. Secure update mechanisms need to be included as functional requirements in a Protection Profile or a Security Target

1729

Table 13 – Mapping CyberSecurity Act Article 51 to Common Criteria (ISO/IEC 15408)

Annex B

Relevant Standards

B.1 The Standardisation Context

Standardisation activities take place in international, national and industry-based fora. Within Europe, the three European Standardisation Bodies, CEN, CENELEC, and ETSI cooperate in order to minimize the duplication of standards. Many technical committees have liaisons and co-operation agreements within all the different technical standardisation committees. However, there are many hundreds of Technical Committees that work on security or have security related work streams and working in parallel. Cooperation has been proven to be difficult due to the different scopes covered by the standardisation bodies and the lack of harmonisation between the terms and definition used. Even the term cybersecurity has different definition and it is often confused with IT security.

The importance of cybersecurity is in fact the protection of the complex environment resulting from the interaction of people, hardware, software and services on the Internet by means of technology devices and networks connected to it. This is the consequence of global digital transformation. All digital systems are concerned: IT of course, but also application domains like healthcare, energy, automotive, cloud computing, IoT (Internet of Things), etc.

For these reasons, cybersecurity is highly transversal. Improving cybersecurity is necessary for all vertical domains.

The scope of cybersecurity is broad and there are a high number of potential domains which are candidates for standardisation:

- **Information security management systems:** To define criteria and methods to guarantee the security of the information by using a management system of a manufacturer, an operator, an end-user. These processes cover the entire lifecycle and not only the development phase;
- **Products, solutions and services design:** To check cybersecurity functions against risks and assess the functions and capabilities of products, solutions, services using technical means like cryptography, public key infrastructures, secure by design principles, secure communications protocols;
- **Cybersecurity and certification:** Evaluation criteria, evaluation methods, hardware module evaluation, side channels attacks evaluation, random bit generators evaluation;
- **Evaluation laboratories evaluation:** People evaluation, development processes evaluation, malware testing, penetration testing, static code analysis and binary analysis;
- **Maintenance and operations of the cybersecurity:** Security operation centre management, Security operation centres indicators, vulnerability management, vulnerabilities format;
- **Standardizing stakeholder security procurement and subcontracting processes:** Contract and subcontract management, product decommissioning and product labelling, supply chain security, fraud and counterfeit management.

B.2 Relevant Standardisation Bodies

Standardisation Bodies have different scopes and governance. We can identify:

- International level Standardisation Bodies: ISO, IEC, ITU, under UN governance are recognized by the standardisation community as international Standardisation Bodies. These organisations are potentially addressing all domains. Their members are registered national bodies and the principle chosen is one member one vote. That is to say that each country has the same weight in vote whatever the size of the country could be. These Standardisation Bodies are mostly working on a consensus basis and voting is an exceptional case. The published standards are generally not free of charge;
- European level Standardisation Bodies: In Europe there are three Standardisation Bodies recognised by the EU: CEN, CENELEC, and ETSI. These European Standardisation Bodies are partly funded by European Union. CEN and CENELEC have similar functioning as ISO and IEC, the membership is also assured through national bodies. CEN and CENELEC have a continuously increasing integrated functioning through CCMC (CEN/CENELEC Management Centre). The published standards are generally not free of charge. ETSI has a different governance organization in comparison with CEN and CENELEC. The membership is assured via individual registration from companies coming from all its member countries. The membership fee is paid on a voluntary basis and the number of votes is proportional to the annual fee cost. There are in place governance regulation mechanisms in order to avoid having the majority shared by only a few members. There is also a national representation for the European matters (like European standards ballots). One important point is that ETSI standards and all technical reports and technical specifications are available free of charge. In order to authorise exchange and transfer of standards between International and European Standardisation Bodies, mechanisms of transposition have been put in place (Dresden, Frankfurt and Vienna agreement), authorising to transpose standards from one Standardisation Bodies to another without having to carry out all the work from scratch;
- Ad hoc Standardisation Bodies: In addition to the official international or European standardization bodies, there are other entities working in specific and focused domains, for example industrial fora like 3GPP, CSA, Fido Alliance, Global platform, IEEE, IETF, AIOTI, one M2M, TCG, Oasis etc. These industrial bodies have different functioning depending on their scope, participation and coverage, but they intend to cover specific requirements from industry and claim to be more efficient than traditional Standardisation Bodies. Nevertheless, they don't have the official recognition of the international/European Standardisation Bodie. However, these Standardisation Bodies have defined specific procedures to import the de facto standards from these organisations, like PAS (Publicly Available Specifications), or so-called fast track mechanisms.

B.3 Standards Relevant to IACS Evaluation

To support IACS cybersecurity certification scheme a certain number of standards have been addressed and referenced in this report. They have been produced by the different Standardisation Bodies already identified and they mainly fall in the following broad categories:

- General standards
- Risk and management systems evaluation standards;
- Security requirements standards;
- Security Evaluation methods.

1811 **B.3.1 General Standards**

1812 The following standards are applicable:

- 1813 • ISO/IEC EN 17065 (pursuant to Regulation (EC) No 765/2008) Conformity Assessment —
- 1814 Requirements for bodies certifying products, processes and services;
- 1815 • ISO/IEC EN 17025 (pursuant to Regulation (EC) No 765/2008) Testing and calibration
- 1816 laboratories;
- 1817 • ISO EN 19011 Auditing Management Systems.
- 1818 • ISO/IEC 27006 Requirements for bodies providing audit and certification of information
- 1819 security management systems
- 1820 • ISO/IEC 27007 Guidelines for information security management systems auditing

1821 **B.3.2 Risk and Management Systems Evaluation Standards**

1822 The following standards are applicable:

- 1823 • ISO/IEC 27001 Information Security Management Systems;
- 1824 • ISO/IEC 27002 Code of practice for information security controls;
- 1825 • ISO/IEC 27005 Information security risk management;
- 1826 • ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 – Requirements;
- 1827 • ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for
- 1828 process control systems specific to the energy utility industry;
- 1829 • ISO/IEC 27031 Guidelines for information and communication technology readiness for
- 1830 business continuity;
- 1831 • ISO/IEC 27035 Information security incident management;
- 1832 • ISO/IEC 27100 Cybersecurity- Overview and concepts;
- 1833 • ISO/IEC 27101 Cybersecurity Framework development guidelines;
- 1834 • IEC 62443-4-1 Security for Industrial Automation & Control Systems - Part 4-1: Secure
- 1835 product development lifecycle requirements.

1836 **B.3.3 Security Requirements Standards**

1837 The following standards are applicable:

- 1838 • ISO/IEC 15408 Evaluation criteria for IT security:
- 1839 ○ Part 1 Introduction and general model;
- 1840 ○ Part 2 Security functional Components;
- 1841 ○ Part 3 Security assurance Components;
- 1842 ○ Part 4 Framework for the specification of evaluation (under development);
- 1843 ○ Part 5 Pre-defined packages of security requirements (under development).
- 1844 • IEC 62443-4-2 Security for Industrial Automation & Control Systems – Part 4-2: Technical
- 1845 security requirements for IACS Components;
- 1846 • EN 303-645 Cybersecurity for consumer IOT: baseline (under development);
- 1847 • ISO/IEC 19790 Security requirements for cryptographic modules.

1848 **B.3.4 Security Evaluation Methods**

1849 The following standards are applicable:

- 1850 • ISO/IEC 18045 Methodology for IT security evaluation;
- 1851 • ISO/IEC 22216 Introductory guidance on evaluation for IT Security;
- 1852 • TS 103 701 Cyber security assessment for consumer IoT products (under development);
- 1853 • JTC13 WG3 Cybersecurity Evaluation Methodology for ICT products (under development).

1854 Other relevant security evaluation standards are:

- 1855 • ISO/IEC 24759 Test Requirements for Cryptographic Modules;
- 1856 • ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing;
- 1857 • ISO/IEC 20543 Test and analysis methods for random bit generators within ISO/IEC 19790
- 1858 and ISO/IEC 15408;
- 1859 • ISO/IEC 29128 Verification of cryptographic protocols.

1860 **B.3.5 Other relevant Standards**

- 1861 • ISO/IEC 29147 Vulnerability disclosure;
- 1862 • ISO/IEC 30111 Vulnerability handling processes;

1863 **Note:** The vulnerability disclosure is a key issue which has also to be considered in particular
1864 in life cycle management.

- 1865 • ISO/IEC 23532 Requirements for the competence of IT security testing and evaluation
1866 laboratories:
 - 1867 ○ Part 1 Evaluation for ISO/IEC 15408;
 - 1868 ○ Part 2 Testing for ISO/IEC 19790.

1869

1870 **B.4 Status of the standards**

1871 From this list numerous standards are already existing or in finalization, covering from the Basic to
1872 the Highest level of evaluation required. There is no clear need to develop additional standards for
1873 IACS but rather to consider the existing set of standards. And it is necessary to encourage the
1874 development and use as much “horizontal” standards as possible in order to avoid as much as
1875 possible domain specific standards.

1876 In support to this action CEN/CENELEC JTC13 has started the transposition of many of them in EN to
1877 make it usable for Cyber act implementation. The standards under transposition are currently:

1878

1879 [a] Standards already transposed and published

- 1880 ○ EN ISO/IEC 15408-1
- 1881 ○ EN ISO/IEC 15408-2
- 1882 ○ EN ISO/IEC 15408-3
- 1883 ○ EN ISO/IEC 18045
- 1884 ○ EN ISO/IEC 19790

1885 ○ EN ISO/IEC 27001

1886 ○ EN ISO/IEC 27002

1887 ○ EN ISO/IEC 27007

1888 ○ EN ISO/IEC 27019

1889 [b] Standards under enquiry for transposition

1890 ○ EN ISO/IEC 27006

1891 ○ EN ISO/IEC 30111

1892 In addition, CEN/CENELEC JTC13 has started the work on Lightweight certification and is discussing
1893 a new work item on IACS certification in order to identify the gaps in security requirements and
1894 evaluation methods.

1895

Annex C

Standards vs Evaluation Activities Mapping

The following table provides a mapping between the Evaluation Activities defined in Section 5 - Evaluation Activities for Assessment Team and the relevant standards.

Evaluation Activity	Relevant standards
Section 5.1 - Component Cybersecurity Profile Evaluation	[CEM] ASE Activity [JTC13WG3EVAL]
Section 5.2 - Documentation Review	[CEM] [TeleTrust] Step 1 Intended Use Verification [TeleTrust] Step 2 Documentation (Design) [TeleTrust] Step 3 Documentation (User) [JTC13WG3EVAL] [ISO/IEC 15408-4]
Section 5.3 - Installation, Configuration and Decommissioning Procedures Review	[CEM] AGD Activity [TeleTrust] Step 3 Documentation (User) [JTC13WG3EVAL] [62443-4-1] Practice 8 (Security guidelines)
Section 5.4 - Security Functions Testing	[CEM] ATE Activity [TeleTrust] Step 4 Conformity Assessment [JTC13WG3EVAL]
Section 5.5 - Vulnerability Analysis	[CEM] AVA Activity [TeleTrust] Step 5 Vulnerability Analysis (+ Appendix D) [JTC13WG3EVAL]
Section 5.6 - Development Process Audit	[62443-4-1] [ISO/IEC 27001] [ISO/IEC 27006] [ISO/IEC 27007] [CEM] ALC Activity & [MSSR] [TeleTrust] Crossreference in Appendix E "Overview of Reuse of Deliverables from IEC 62443-4-1 Development Process"
Section 5.7 - Penetration Testing	[CEM] AVA Activity [JTC13WG3EVAL]
Section 5.8 - Cryptographic Assessment	[ISO/IEC 19790] [ISO/IEC 24759] [SOG-IS Crypto]

Table 14 – Annex C Standards vs Evaluation Activities mapping

Annex D

Correspondence of the Agnostic Terminology with IEC 62443 4-2, Lightweight and Common Criteria Certification Paths

In order ICCS to be “agnostic”, i.e. to bridge differences between existing Cybersecurity Certification Schemes and standards, it has been consciously decided not to select a specific standard as a reference for ICCS. The Component Cybersecurity Profile (CCP) proposed in ICCS, which is based on the separation of the Cybersecurity Context Analysis (CCA) and the Component Cybersecurity Requirements (CCR) allows:

- An independent description of the Security Objectives of a product without being locked in a specific standard;
- The possibility to use a template approach (generic CCA) for a family of IACS Components;
- The shift to a specific certification standard or reference with a minimum of complexity and workload.

Below, the relationship of the agnostic CCP and gCCA principles with the IEC 62443-4-2, Lightweight and Common Criteria certification paths and their instantiation on these paths are explained:

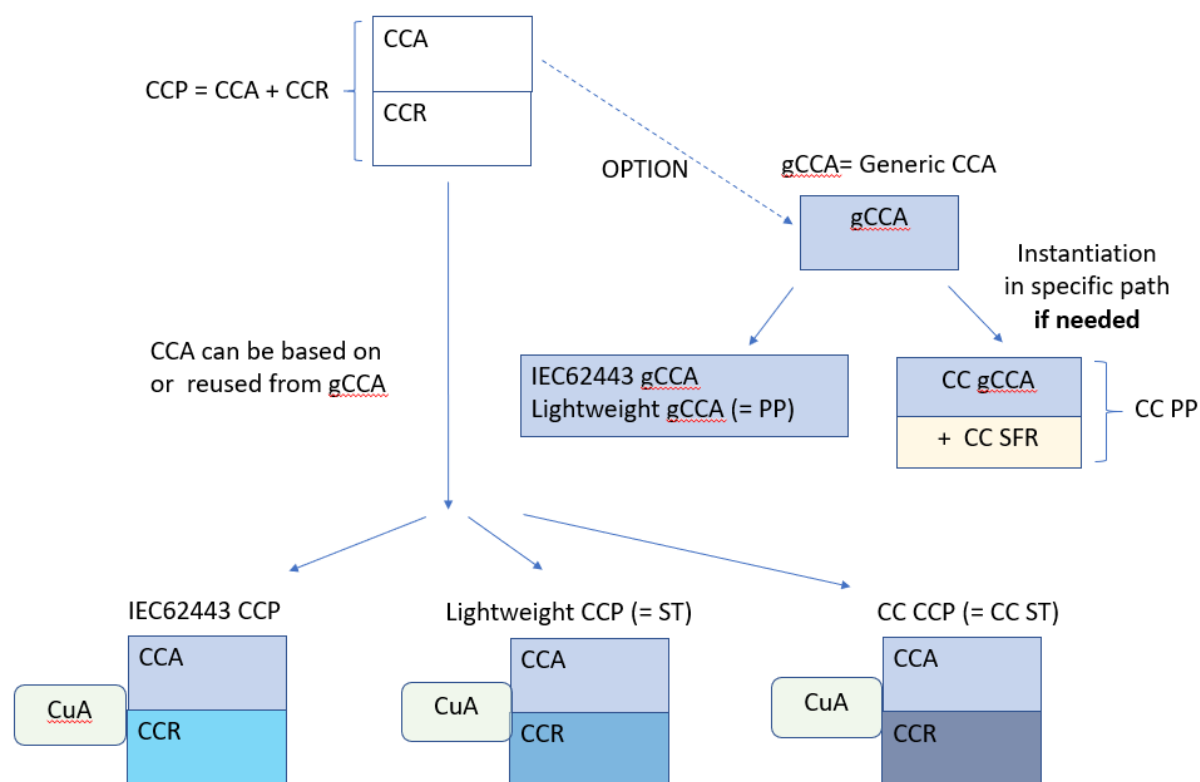


Figure 9 - Relationship of the agnostic CCP/gCCA principles to certification approaches

Below, the correspondence of the agnostic CCP, CCA/gCCA and CCR principles in each certification approach is explained, with the detailed description of the elements required in the CCP, and based on a clear separation between the CCA/gCCA and the CCR:

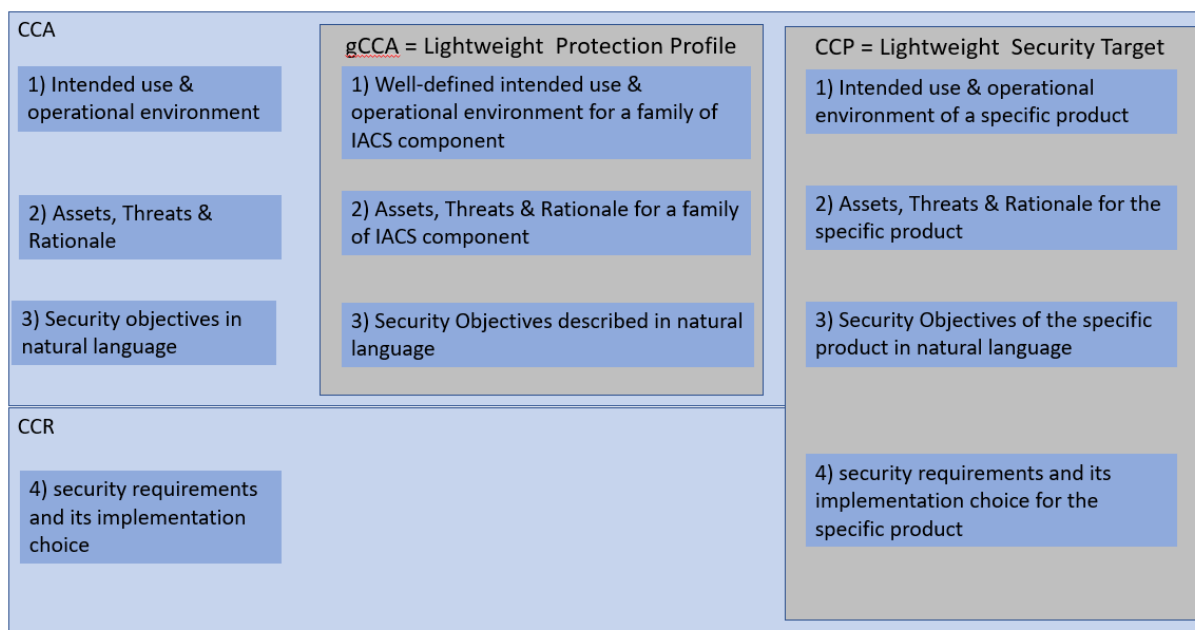


Figure 10 - Relation of agnostic CCP/gCCA principles to the Lightweight certification approach

Note that the principles of the CCP and gCCA are fully compliant with current Lightweight certification schemes.

Note also that the French CSPN, German BSZ, Dutch BSPA and Spanish LINCE certification schemes are examples of a Lightweight methodology.

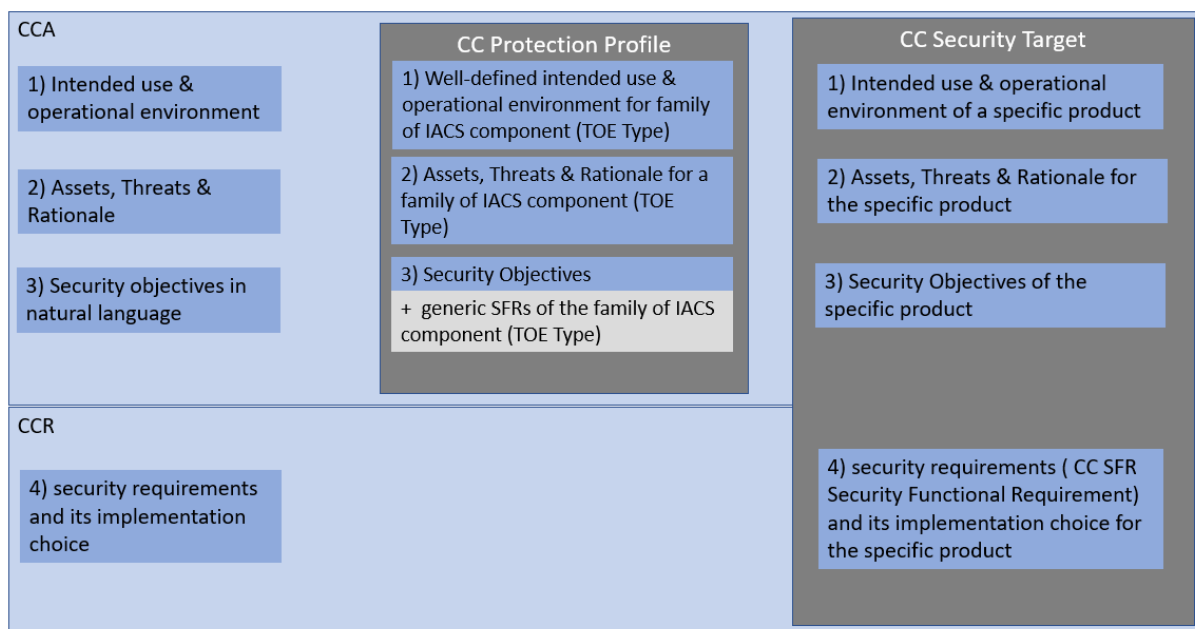


Figure 11 - Relation of agnostic CCP/gCCA principles to the Common Criteria certification approach

Note that the principle of an agnostic gCCA is 100% compliant with the Common Criteria protection profile if the optional set of generic security requirements for the family of IACS Components is included, by reference to ISO/IEC 15408 Security Functional Requirements which are required in Common Criteria certification path. Nonetheless, if the optional set of requirements is included (as

1934 required by ISO/IEC 15408 Security Functional Requirement), the gCCA compatibility to the
1935 different paths/alternative identified by the ICCS scheme may not be maintained.

CCA	IEC62443 gCCA	IEC62443 CCP
1) Intended use & operational environment	1) Well-defined intended use & op environment for a family of IACS component	1) Intended use & operational environment description of the specific product, based on IEC 62443-4-1 SDL practices (<i>SR-1/Product Security Context, SG,...</i>)
2) Assets, Threats & Rationale	2) Assets, Threats & Rationale for a family of IACS component	2) Assets, Threats & Rationale description based IEC 62443-4-1 SDL practices (<i>SM, SR, SG-1/Product Defense in Depth of the specific product ...</i>)
3) Security objectives	3) Security Objectives described in natural language	3) Security Objectives of the specific product, described in natural language
CCR		4) security requirements and its implementation choice for the specific product <ul style="list-style-type: none">• IEC 62443-4-1: <i>SR-3 & SR-4 (Product Security Requirements & Context)</i>• IEC 62443-4-2 : <i>Component Requirements</i>• <i>Implementation choice</i>

1936
1937 Figure 12 - Relation of agnostic CCP/gCCA principles to the IEC 62443 4-2 certification approach

1938 Note that the principles of the CCP/gCCA are fully compliant and can be used with the IEC 62443-
1939 based certification.

1940 Below there are given different examples of the process for validating CCPs/gCCAs based on
1941 different certification approaches:

1942 **D.1 Validation of CCPs/gCCAs based on IEC 62443-4-2**

Example of Validation of CCPs/gCCAs based on IEC 62443-4-2:

Req.XXXX For EU gCCA, the validation shall contain the following additional steps:

- [a] The Assessment Team shall validate that all operations (refinements, selections, assignments) in the EU gCCA are clearly marked, possible choices are given and are consistent amongst each other. For example, if a certain technological decision is left open it shall not be indirectly imposed by other parts of the EU gCCA.
- [b] The CB shall determine a fictious CuA for which it instantiates the EU gCCA to derive a CCP (for this fictious CuA). The validation shall then be done as for CCPs on the derived CCP.
- [c] Additionally, the Assessment Team shall verify that the technical contents are technically valid (“sound”) and applicable to a wide range of possible CuAs, i.e. does not limit implementations by for example specifying unnecessary technical details.

Req.XXXX The certification report shall mention the parameters chosen for the operations of the EU gCCA during the validation.

1943 **D.2 Validation of CCPs/gCCAs based on Lightweight Methodologies**

Example of Validation of CCPs/gCCAs based on Lightweight methodologies:

Req.XXXX The validation of gCCA/CCP shall follow the requirements of the CEN/CENELCT JTC13 methodology for the validation of generic Component Context Analysis (for EU gCCAs) respective Security Targets (CCPs) with the following constraints. At the time of the writing of this scheme proposal, no suitable stable draft was available to complete this Subsection. This needs to be done in the final group working on the ICCS.

Note: CSPN (and BSZ, BSPA, LINCE) certification are examples for a Lightweight methodology

1944 **D.3 Validation of CCPs/gCCAs based on ISO/IEC 15408**

Example of Validation of CCPs/gCCAs based on ISO/IEC 15408:

Req.XXXX The validation of gCCA/CCPs shall happen according to the rules established for the European Common Criteria Scheme, i.e. using the methodology established in ISO/IEC 18045 within the procedural framework of that scheme for the validation of generic Component Context Analysis (for EU gCCAs) respective Security Targets (for CCPs).

Req.XXXX Additionally Assessment Team shall verify that the EU gCCA is technically valid (“sound”) and applicable to a wide range of possible CuAs, i.e. does not limit implementations by for example specifying unnecessary technical details.

Annex E

CCP and gCCA Examples

E.1 Example for a CCP

Example:

A Manufacturer is required to ensure communications' integrity and authentication for a PLC. This functionality will be implemented using a specific protocol. A different PLC Manufacturer may implement the communications' integrity and authentication using a different protocol. Such choices are based on a Security Mechanism Rationale.

Note: Security functions correspond to Components Security Requirements.

Example of a part of a mapping in the case of IEC 62443-4-2:

Protection Profile PLC Short term v1.1: Security Objectives (Claim)	62443-4-2 Requirements (details of the claim)	
Malformed input management: The Family of CuAs (FoP) has been developed in order to handle correctly malformed input, in particular malformed network traffic.	CR-3.5	Input validation
	CR-7.1	Denial of service protection
	CR-7.1 RE 1	Manage communication loads
	CR-7.2	Resource management
Secure storage of secrets: User secrets are securely stored in the FoP. In particular, the compromise of a file is not sufficient for retrieving them.	CR-4.1	Information confidentiality
	CR-4.3	Use of cryptography

E.2 Example gCCA

The following example provides some illustration of the terms of a generic Component Context Analysis:

Example of a gCCA for a Programmable Logic Computer (PLC)

CuAs Family

Programmable Logic Controller.

This kind of devices allows to monitor and/or to actuate a field instrument, an automation device.

Part

A 'user program' ran by the PLC is a (digital) part of this kind of CuAs.

Critical asset

'The integrity of the user program' is a critical asset of the CuA (combination of the part 'user program' and the security criterion 'integrity').

Threat

User program alteration: The attacker manages to modify, temporarily or permanently, the user program

Operating Conditions (Users)

An administrator is a user of the CuA who has maximum privileges (modification of the user program, firmware updates, etc.).

Assumption(s)

'The PLC stands in an open area fully accessible to users. Not only administrators have access to PLC's user programs. Administrators are competent and trustworthy. But other users such as hired, external staff are competent but may be untrustworthy'.

Residual Threat(s)

Hired staff may be a threat to the integrity of a PLC.

Security function

Integrity and authenticity of the user program. Only authorized users can modify it. To do so, the CuA shall at least implement the following CRs:

- CR 1-1 Human user identification and authentication
- CR 1-2 Software process and device identification and authentication
- CR 3-4 Software and information integrity
- CR 4-3 Cryptography

Rationale of the Security Function

The following table is given as an example. It allows for checking the completeness of the coverage of threats by Security Functions. The justification for each cross is expected to be given under the table.

	Denial of service	Firmware alteration	Execution mode alteration	User program compromise	User program alteration	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration	Parameters or command injection	Flows alteration	Flows compromise
Malformed input management	X														
Secure storage of secrets								X							
Secure authentication on administration interface						X	X	X	X						
Access control policy										X					
Firmware signature		X													
Configuration confidentiality and integrity						X	X								
Integrity and authenticity of the user program					X										
Confidentiality of the user program				X											
Integrity and authenticity of commands and PLC mode			X												
Secure communication													X	X	X
Logs integrity											X				
Alarms integrity												X			

1954 **References**

CEM	Common Methodology for Information Technology Security Evaluation. Evaluation Methodology. April 2017. Version 3.1. Revision 5
CCPart1	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. April 2017. Version 3.1. Revision 5
CCPart2	Common Criteria for Information Technology Security Evaluation. Part 2: Security functional Components. April 2017. Version 3.1. Revision 5
CCPart3	Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance Components. April 2017. Version 3.1. Revision 5
TeleTrust	TeleTrust Evaluation Methodology for IEC 62443-4-2 - Security for Industrial Automation & Control Systems
JTC13WG3EVAL	JTC13 WG3 Cybersecurity Evaluation Methodology for ICT products
MDF_PP	U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals Version 3.1
SOG-IS Crypto	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.1
OPENSAMM	Software assurance maturity model (www.opensamm.org)

1955

1956

GETTING IN TOUCH WITH THE EU**In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU**Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub

ec.europa.eu/jrc



@EU_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub



Publications Office
of the European Union