# Industrial Automation Control Systems Cybersecurity Certification – Chapter II

**Georgios Theodoridis**
EC DG JRC, Directorate E
**Jose Ruiz**
CTO at jtsec

**The European Commission's science and knowledge service**

Joint Research Centre

European Commission

# Who am I?
## Georgios Theodoridis

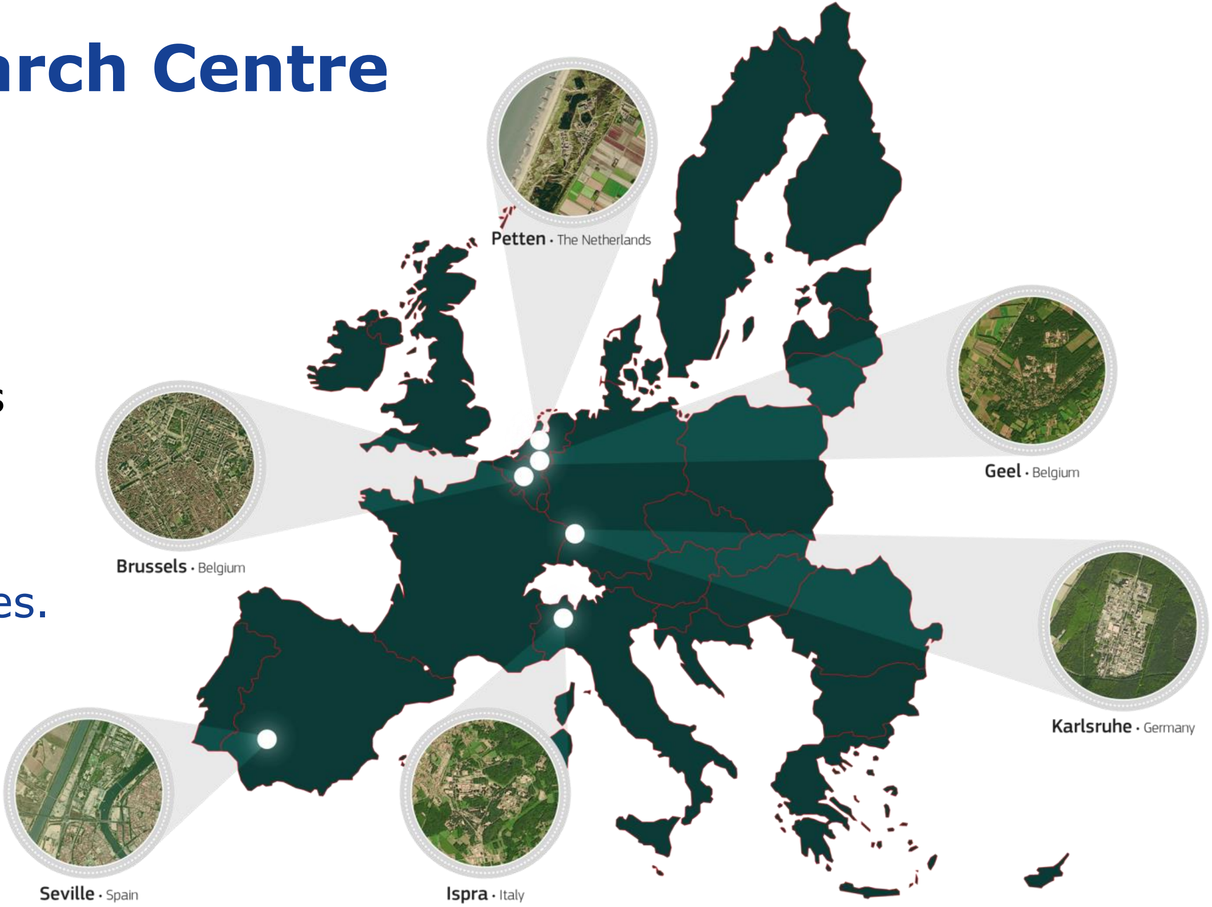
- **Scientific/Technical Project Officer at European Commission DG JRC (Joint Research Centre)**
    - Directorate on Space, Security and Migration
- **Scientific/technological support for EU/MS policy making**
- **Critical Infrastructure Protection**
    - Manager of the ERNCIP IACS TG; Editor of the IACS CCS
    - Review of the NIS and ECI Directives
    - Smart Power Grids resilience and security
    - EU Critical Infrastructures resilience against Hybrid Threats
- **Internet/cyber Security**
    - Internet backbone routing security
    - Data encryption solutions

# Who am I?
## Jose Ruiz

- CTO and founder at jtsec BEYOND IT SECURITY
- Common Criteria & FIPS 140-2 Expert
- EUCA/ICMC/ICCC Program Director
- Editor & Co-leader at ERNCIP TG “IACS Cybersecurity Certification‟
- Editor at JTC13 WG3: “Cybersecurity Evaluation Methodology for ICT products”
- Appointed Member of SCCG (Stakeholder Cybersecurity Certification Group)

# The Joint Research Centre at a glance

**3000 staff**
Almost 75% are scientists and researchers.
Headquarters in Brussels and research facilities located in 5 Member States.



European Commission

# JRC’s Mission

*As the European Commission's science and knowledge service, the Joint Research Centre (JRC) supports EU policies with independent scientific evidence throughout the whole policy cycle.*

# EU Cybersecurity Certification Framework

## What?

- **Harmonised approach** to Cybersecurity Certification Schemes at EU level
- **Common EU Cybersecurity Certification Schemes**
- **Specific ICT Products, Services and Processes** of common interest

# EU Cybersecurity Certification Framework

## Why?

- **Increase the Cybersecurity within the EU**
- **EU-wide recognised Cybersecurity Certificates**
- Improve the conditions for the **functioning of the internal market**
  - A digital single market for ICT Products, Services and Processes
- Increase the **competitiveness and growth of EU ICT companies**
  - Quality standards for Cybersecurity
  - Minimise the certification cost

# EU Cybersecurity Certification Framework

## How?

- Definition of Common EU CCS for specific ICT **Products** / **Services** / **Processes**
- Evaluation against the common EU CCS
- Attestation of compliance with specified security requirements
- Protection of the
    - **availability**, **authenticity**, **integrity** or **confidentiality** of
    - **stored** / **transmitted** / **processed data** or
    - the **functions** / **services** offered by, or accessible via, those ICT Products / Services / Processes
    - **throughout their life cycle**

# EU Cybersecurity Certification Framework

## CyberSecurity Act

### Union Rolling Work Programme

- **Defined by the EC**
- Multiannual overview of strategic priorities for future CCS
- Specific ICT products/services/processes
- Criteria
  - Related MS CCS or EU/MS legislation/policy
  - Market demand
  - Cyber threat landscape
  - Request by the ECCG
- Input from ECCG and Stakeholders CG

# EU Cybersecurity Certification Framework

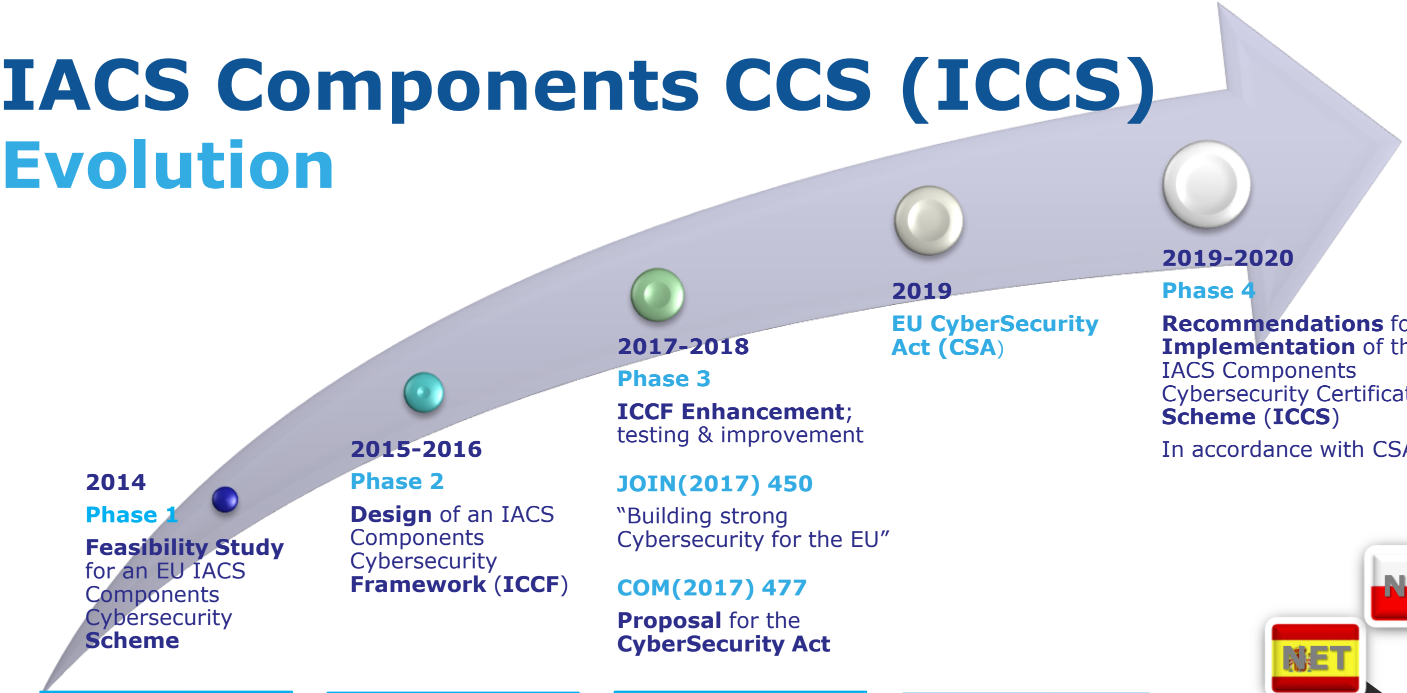
## CyberSecurity Act

- **EC request to ENISA** for preparing a **Candidate CCS**
  - Based on the **Union Rolling Work Programme** priorities
  - Ad-hoc requests also possible
- ENISA
  - Establishment of an ad-hoc Group of Experts
  - Consultations/collaboration with all the **Stakeholders**
  - **Submission of the Candidate CCS**
- **Adoption of the CCS**
  - The Candidate CCS becomes **Effective**

# IACS Components CCS (ICCS)
## ERNCIP

- **ERNCIP**
  - **European Reference Network Critical Infrastructure Protection**
  - Managed and Coordinated by **EC DG JRC**
- **ERNCIP IACS TG**
  - **Industrial Automation & Control Systems Thematic Group**
  - Highly reputable experts
  - All the relevant scientific and technical fields
  - All over the EU
  - All the ICCS stakeholders
    - IACS (Components) manufacturers
    - Cybersecurity certification authorities
    - Cybersecurity industries, cybersecurity assessment laboratories
    - Academia

# IACS Components CCS (ICCS)
## Evolution



**2014**
**Phase 1**
**Feasibility Study** for an EU IACS Components Cybersecurity **Scheme**

**2015-2016**
**Phase 2**
**Design** of an IACS Components Cybersecurity **Framework** (**ICCF**)

**2017-2018**
**Phase 3**
**ICCF Enhancement**; testing & improvement

**JOIN(2017) 450**
“Building strong Cybersecurity for the EU”

**COM(2017) 477**
**Proposal** for the **CyberSecurity Act**

**2019**
**EU CyberSecurity Act (CSA)**

**2019-2020**
**Phase 4**
**Recommendations** for the **Implementation** of the IACS Components Cybersecurity Certification **Scheme** (**ICCS**)

In accordance with CSA

Proposals from the ERNCIP Thematic Group, “Case Studies for the Cyber-security of Industrial Automation and Control Systems”, for a European IACS Components Cyber-security Compliance and Certification Scheme

Thematic Area
Industrial Control Systems and Smart Grids

Paul THERON, Thales
Sandro BOLOGNA, AIIC

November 2014

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

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

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

Paul THERON, Thales

2016

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

The IACS Cybersecurity Certification Framework (ICCF)

*Lessons from the 2017 study of the state of the art*

P. THERON, Thales
A. LAZARI, JRC

April 2018

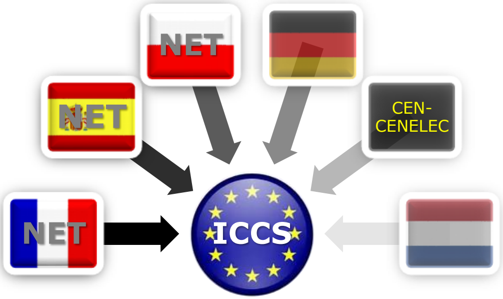
The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure

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; GONZALEZ, Sergio; GORSKI, [illegible]

Editors
THEODORIDIS, Georgios
GIANNOPOULOS, Georgios



European Commission

# IACS Components CCS (ICCS)

## Basic Principles

- **Prescriptive** and **unequivocal**
  - Well structured, concise, clear and precise requirements for all ICCS stakeholders and entities
  - Rigorous and homogeneous evaluation & certification
  - Equivalence and mutual recognition of Certificates
- **Usable** and **self-explanatory**
  - Recommendations, guidelines, information and references for the ICCS implementation
  - Foreseen audience: professionals of products’ cybersecurity engineering, evaluation and certification
- **Agnostic**
  - Technology agnostic
  - Terminology agnostic

# IACS Components CCS (ICCS)

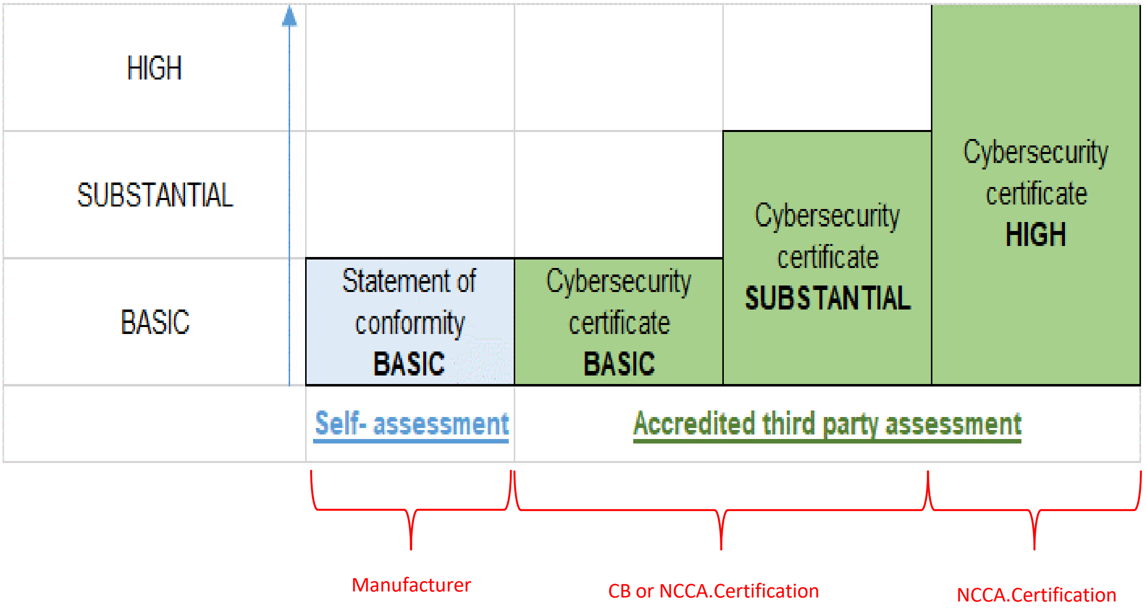
## Focus on Components

- **IACS** are **built as** the **integration** of multiple, disparate hardware/software **Components**
  - Different technologies/solutions
  - Different providers
- Cybersecure IACS by **cybersecuring its Components**
- **Flexibility** and **adaptability**: Different **security requirements and assurance levels per IACS element**
  - System design
  - Intended use
  - Operational environment
  - System-level security measures

# IACS Components CCS (ICCS)

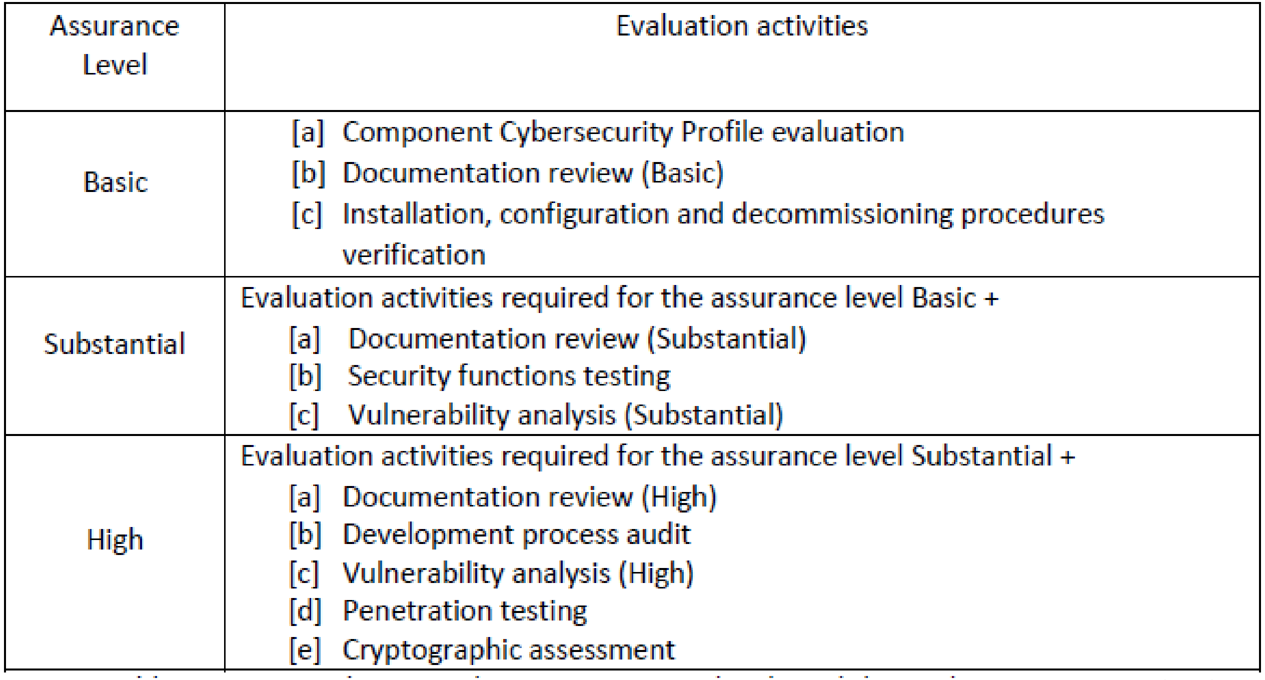
## Assurance Levels

- Three (3) Assurance Levels
- EU Statement of Conformity (Basic)
- In accordance with CSA
- Risk-assessment approach



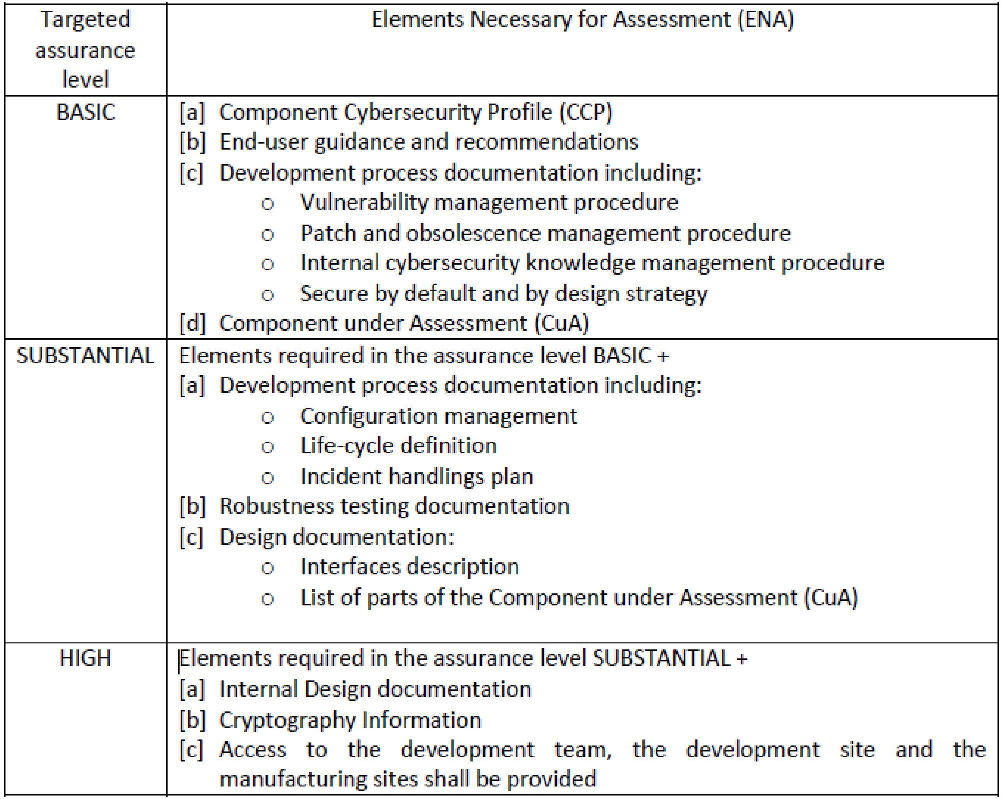
| | | | | |
|---|---|---|---|---|
| HIGH | | | | Cybersecurity certificate **HIGH** |
| SUBSTANTIAL | | | Cybersecurity certificate **SUBSTANTIAL** | |
| BASIC | Statement of conformity **BASIC** | Cybersecurity certificate **BASIC** | | |
| | Self- assessment | Accredited third party assessment | | |
| | Manufacturer | CB or NCCA.Certification | | NCCA.Certification |

# IACS Components CCS (ICCS)
## Assurance Levels



| Assurance Level | Evaluation activities |
|---|---|
| Basic | [a] Component Cybersecurity Profile evaluation<br>[b] Documentation review (Basic)<br>[c] Installation, configuration and decommissioning procedures verification |
| Substantial | Evaluation activities required for the assurance level Basic +<br>[a] Documentation review (Substantial)<br>[b] Security functions testing<br>[c] Vulnerability analysis (Substantial) |
| High | Evaluation activities required for the assurance level Substantial +<br>[a] Documentation review (High)<br>[b] Development process audit<br>[c] Vulnerability analysis (High)<br>[d] Penetration testing<br>[e] Cryptographic assessment |

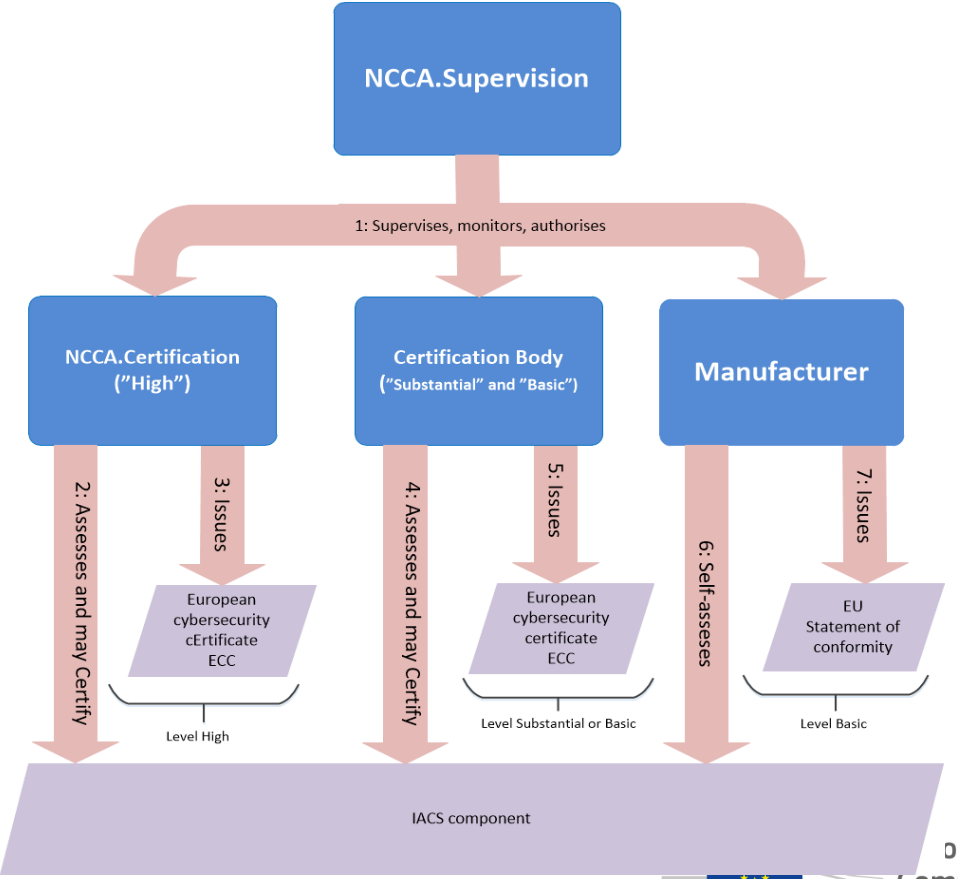
# IACS Components CCS (ICCS)
## Assurance Levels



| Targeted assurance level | Elements Necessary for Assessment (ENA) |
|---|---|
| BASIC | [a] Component Cybersecurity Profile (CCP)<br>[b] End-user guidance and recommendations<br>[c] Development process documentation including:<br>o Vulnerability management procedure<br>o Patch and obsolescence management procedure<br>o Internal cybersecurity knowledge management procedure<br>o Secure by default and by design strategy<br>[d] Component under Assessment (CuA) |
| SUBSTANTIAL | Elements required in the assurance level BASIC +<br>[a] Development process documentation including:<br>o Configuration management<br>o Life-cycle definition<br>o Incident handlings plan<br>[b] Robustness testing documentation<br>[c] Design documentation:<br>o Interfaces description<br>o List of parts of the Component under Assessment (CuA) |
| HIGH | Elements required in the assurance level SUBSTANTIAL +<br>[a] Internal Design documentation<br>[b] Cryptography Information<br>[c] Access to the development team, the development site and the manufacturing sites shall be provided |

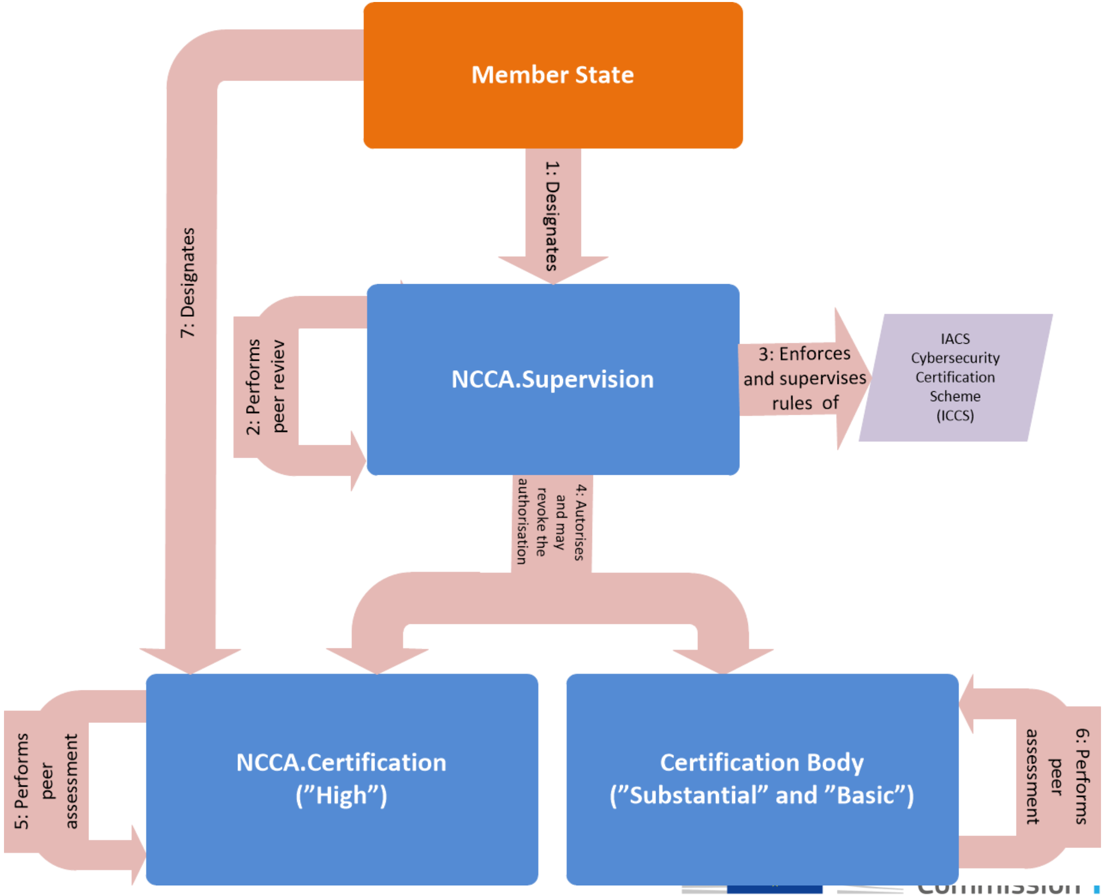
# IACS Components CCS (ICCS)

Consolidated organisation of the ICCS certification and Self-Assessment


NCCA.Supervision
1: Supervises, monitors, authorises
NCCA.Certification ("High")
Certification Body ("Substantial" and "Basic")
Manufacturer
2: Assesses and may Certify
3: Issues
4: Assesses and may Certify
5: Issues
6: Self-asseses
7: Issues
European cybersecurity cErtificate ECC
European cybersecurity certificate ECC
EU Statement of conformity
Level High
Level Substantial or Basic
Level Basic
IACS component

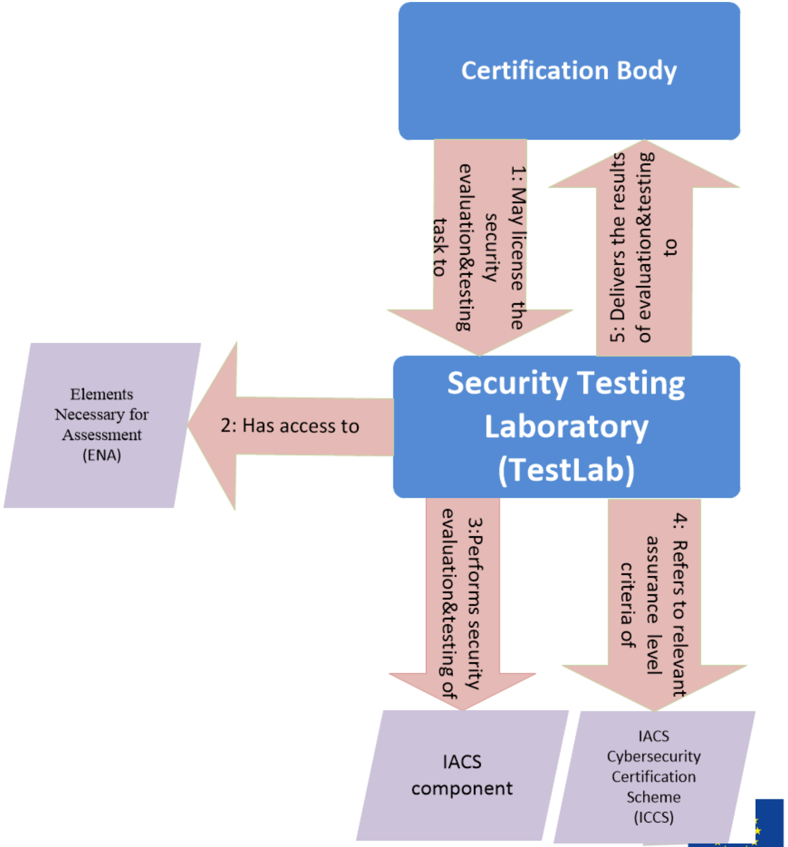
# IACS Components CCS (ICCS)

NCCA.Supervision in context


Member State
1: Designates
NCCA.Supervision
2: Performs peer reviev
3: Enforces and supervises rules of
IACS Cybersecurity Certification Scheme (ICCS)
4: Autorises and may revoke the authorisation
7: Designates
NCCA.Certification ("High")
Certification Body ("Substantial" and "Basic")
5: Performs peer assessment
6: Performs peer assessment

# IACS Components CCS (ICCS)

Security Testing Laboratory (TestLab) in the certification process



Certification Body

1: May license the security evaluation&testing task to

5: Delivers the results of evaluation&testing to

Security Testing Laboratory (TestLab)

2: Has access to

Elements Necessary for Assessment (ENA)

3:Performs security evaluation&testing of

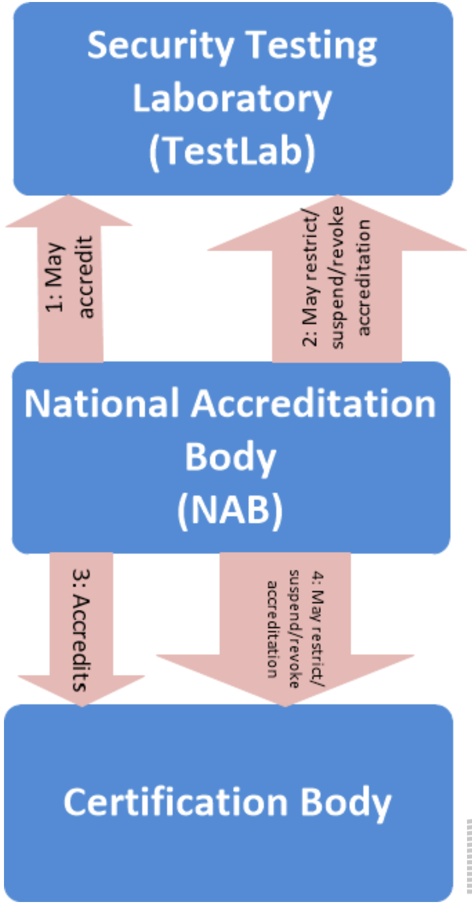
IACS component

4: Refers to relevant assurance level criteria of

IACS Cybersecurity Certification Scheme (ICCS)

# IACS Components CCS (ICCS)

Accreditation, Peer Assessment and Peer Review model



Security Testing Laboratory (TestLab)

1: May accredit

2: May restrict/ suspend/revoke accreditation

National Accreditation Body (NAB)

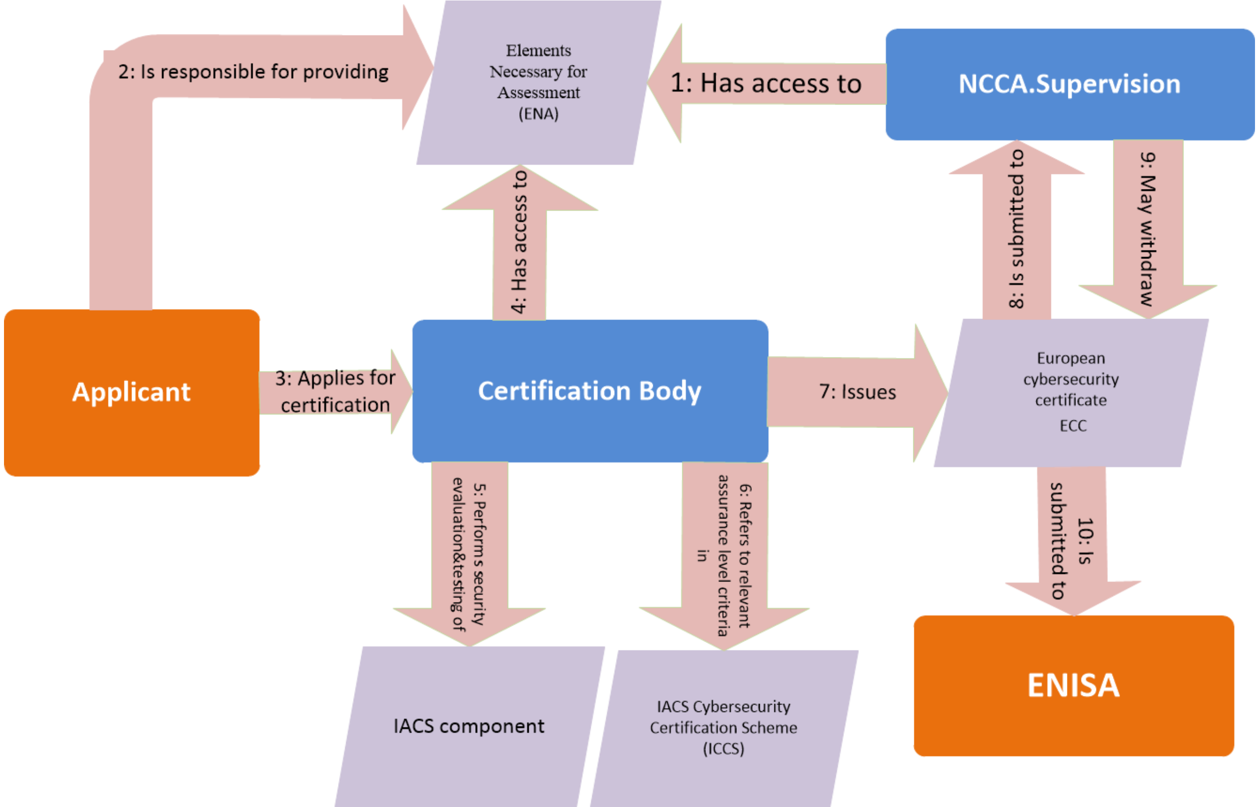
3: Accredits

4: May restrict/ suspend/revoke accreditation

Certification Body

# IACS Components CCS (ICCS)

Issuing a Certificate on the Applicant request



Elements Necessary for Assessment (ENA)

1: Has access to

NCCA.Supervision

2: Is responsible for providing

Applicant

3: Applies for certification

Certification Body

4: Has access to

5: Performs security evaluation&testing of

6: Refers to relevant assurance level criteria in

7: Issues

European cybersecurity certificate ECC

8: Is submitted to

9: May withdraw

10: Is submitted to

IACS component

IACS Cybersecurity Certification Scheme (ICCS)

ENISA

# Conclusions & Next Steps

- **Recommendations for the Implementation of the IACS Components Cybersecurity Certification Scheme (ICCS)**
  - A European and Industry need
  - Good piece of work to be used by the EU Commission and ENISA
- **Work ahead**
  - Define the evaluation(s) methodology(s) to be used in the scheme
  - Analyse and Re-use EUCC applicable work
- **Waiting for Union Rolling Work Programme**

# Thank you for your attention – to stay in touch:

Email: JRC-ERNCIP-OFFICE@ec.europa.eu

ERNCIP IACS TG: ***https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs***

EU Science Hub: ***ec.europa.eu/jrc***

Twitter: ***@EU_ScienceHub***

Facebook: ***EU Science Hub - Joint Research Centre***

LinkedIn: ***Joint Research Centre***

YouTube: ***EU Science Hub***