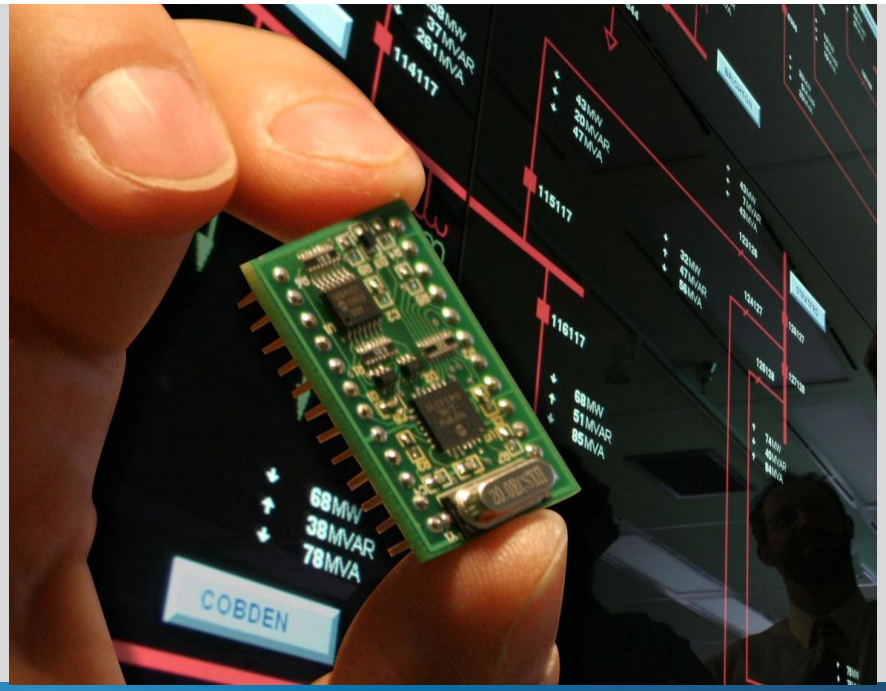
enisa
European Network and Information Security Agency

Methodology used for the project

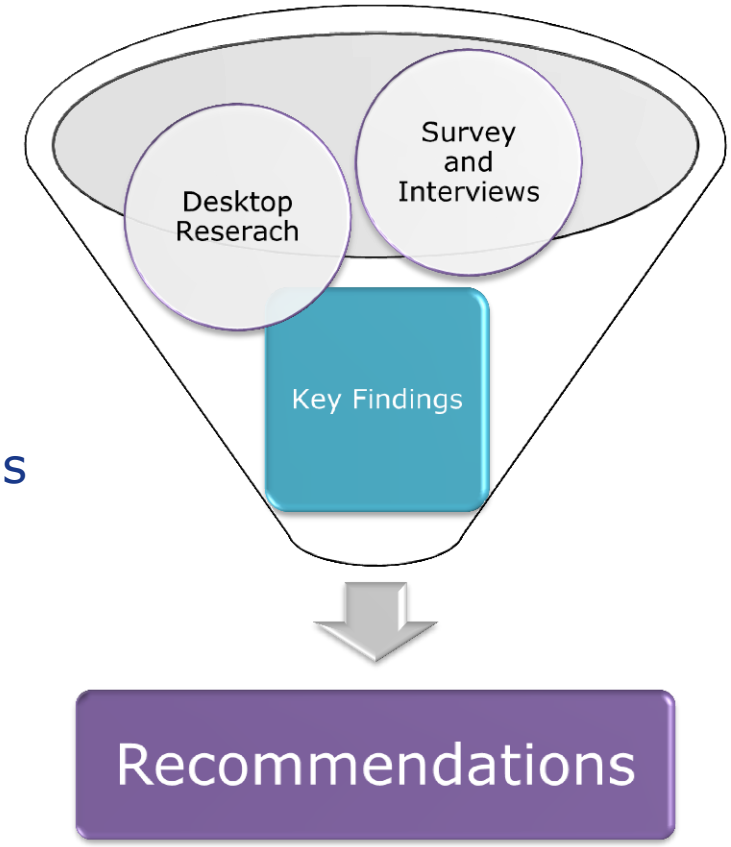
Recommendations for Harmonized ICS Testing Capability in the EU



Methodology used for the project

- Phase I. Stock Taking
  - Desktop research
  - Questionnaire
  - Interviews

- Phase II. Analysis and Good practices
  - Normalise
  - Analysis
  - Extract Key findings
  - Build Recommendations
  - Report improvement



Phase I. Stock Taking

Tasks:

- Desktop research
- Questionnaire
- Interviews

Deliverables:

- Annex I: Desktop Research Results
- Annex II: Key Lessons identified, good testing practices, challenges and gaps
- Annex IV: ICS Security Testing Related Standards, Guidelines and Policy documents.
- Annex V: ICS Security Testing Related Initiatives

Phase I. Stock Taking – Desktop research

- Secondary research based on information from published resources
- High reputation documents:
  - Technical reports
  - Specialised books
  - Good practices
  - Standards
- Developed by relevant organisms, companies, consortiums or research centres
- ICS Test bed initiatives, whitepapers, product/services, sheets, etc.
- Latest news: forums, mailing lists, twitter, blogs, etc.

More than 100 documents analysed

Phase I. Stock Taking – Questionnaire

- 26 open and closed questions
- Based on Desktop Research and S21sec's experience in ICS SCADA Testing capabilities real projects
- Divided into different categories:
  - Status
  - Objectives
  - Model
  - Resources
  - Constraints
  - External relationships
- Considering the type of Stakeholder:
  - Security Test Lab Experts
  - Manufacturers and Vendors
  - Operators
  - ICS Security Tools and Service Providers
  - Academia and R&D
  - Public Bodies for ICS Protection
  - Standardization Bodies
- On-line Web form that allowed us to easily collect and process the answers (automated tool)

Phase I. Stock Taking – Interviews

- Conducted in a personal basis
- Questions based on the on-line questionnaire
- Audio conferences, either via Skype, WebEx or regular telephone call with experts from three continents.
- Double purpose:
  - Deepen into the details of some of the answers of the survey
  - Exchange of points of view on several hot topics in the field of ICS SCADA Testing Capabilities

23 interviews to 27 experts

Phase II. Analysis and Good practices

Tasks:

- Normalise
- Analysis
- Extract Key findings
- Build Recommendations
- Report improvement

Deliverables:

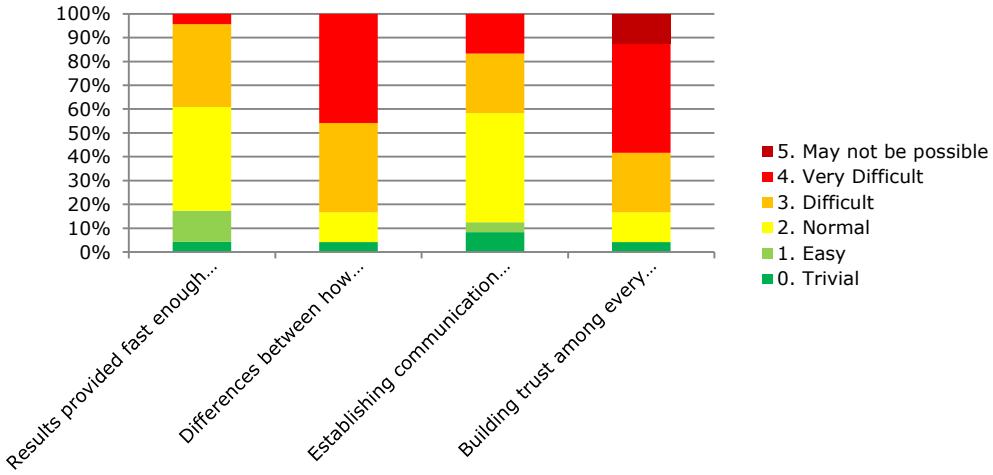
- Annex III: Survey and Interview Analysis
- **Good Practices and Recommendations for a Harmonized ICS-SCADA National Testing Framework**
- Annex VI: Minutes of the Workshop

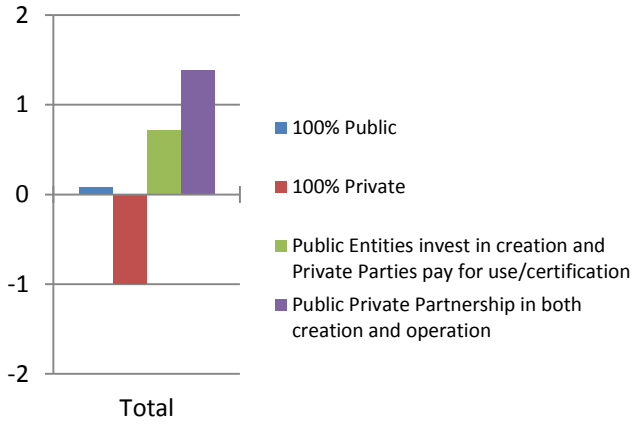
Phase II. Analysis – Normalise

- Complex and unstructured data comes from
  - Open questions in questionnaires
  - Interviews
- Need to normalise this data for a good quality analysis
  - Process the answers
  - Extract the common points
- This is done manually on the raw data

Phase II. Analysis – Analysis

- Dedicated, proprietary tools developed ad-hoc to consolidate and analyse the data have been used.
- A qualitative analysis has been performed on the data to obtain a structured set of information: graphs, tables, statistics, ...





Phase II. Analysis – Key findings

- The **basic element of knowledge** is called "key finding"
- A "key finding" is the most relevant and influential observation from the desktop research, the survey and the interviews.
- A "key finding" might show an emerging issue, a disagreement among stakeholders, tendencies in answers, etc.
- They are linked to the information sources to assure traceability and good reasoning.
- Key Findings are the **basic element to ultimately derive the recommendations** of the report

51 identified key findings, then consolidated into 36

Phase II. Analysis – Recommendations

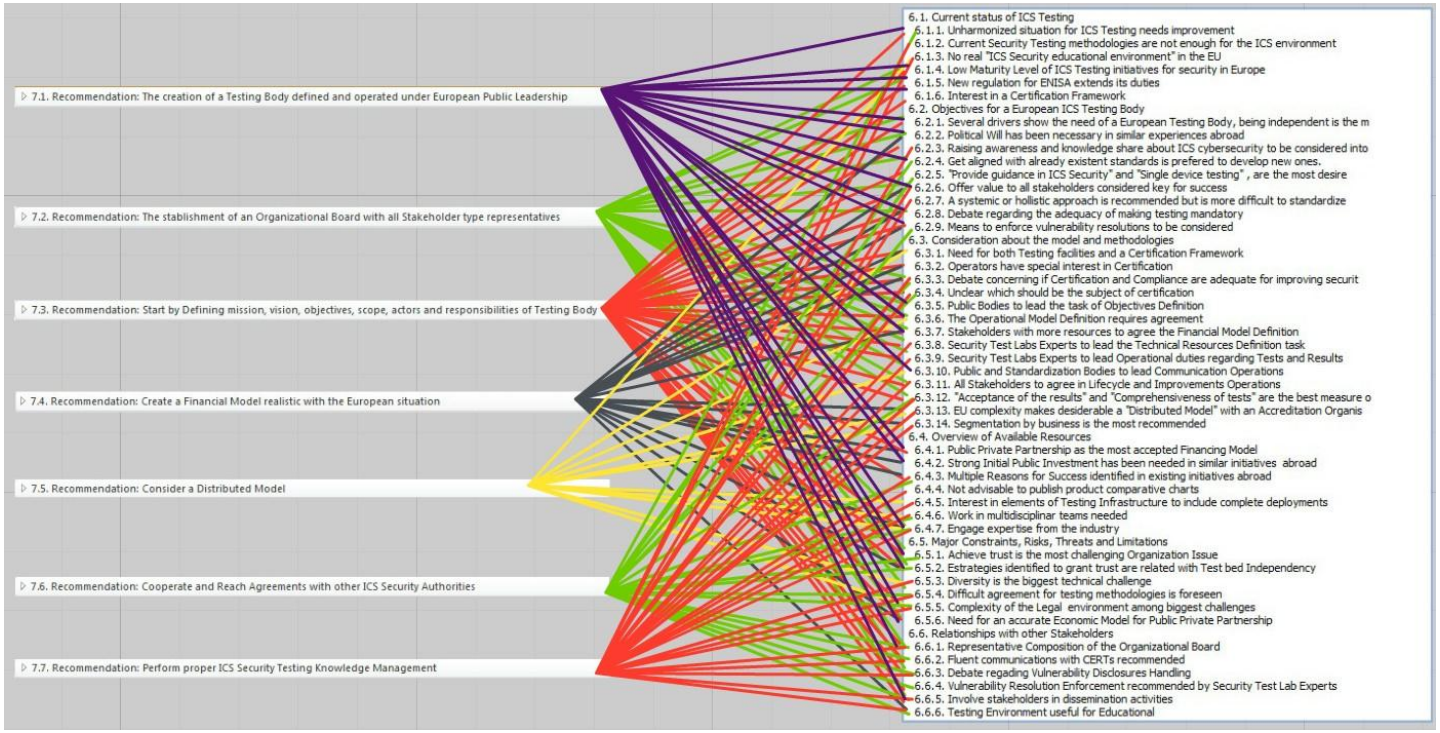
- As conclusion of the analysis of key findings, they have been presented a set of recommendations in order to reach independent ICS security testing capabilities in Europe.

- Each recommendation has been structured as follows:
  - Description.
  - Objective.
  - Steps.
    - Quick Wins
  - Measures of success.
  - Alternative.
  - Stakeholders affected

7 recommendations proposed

Phase II. Analysis – Recommendations

Relation between Key findigns and recommendations



Phase II. Analysis – Report improvement

- Present the results to the experts
  - Key findings
  - Recommendations
- Obtain feedback
  - Debate
- Generate a new version of the final report
- Improve before Publication

To be done today!

Methodology used for the project

Thank you!

For more information on Digital Security Research:

Irene Eguinoa: ieguinoa@s21sec.com

Carlos Monreal: cmoreal@s21sec.com

For ICS/SCADA Cyber Security Services:

Elyoenai Egozcue: eegozcue@s21sec.com