ENISA's work in the area of ICS/SCADA security

10-11th of October, ARPIC, Bucharest, ROMANIA

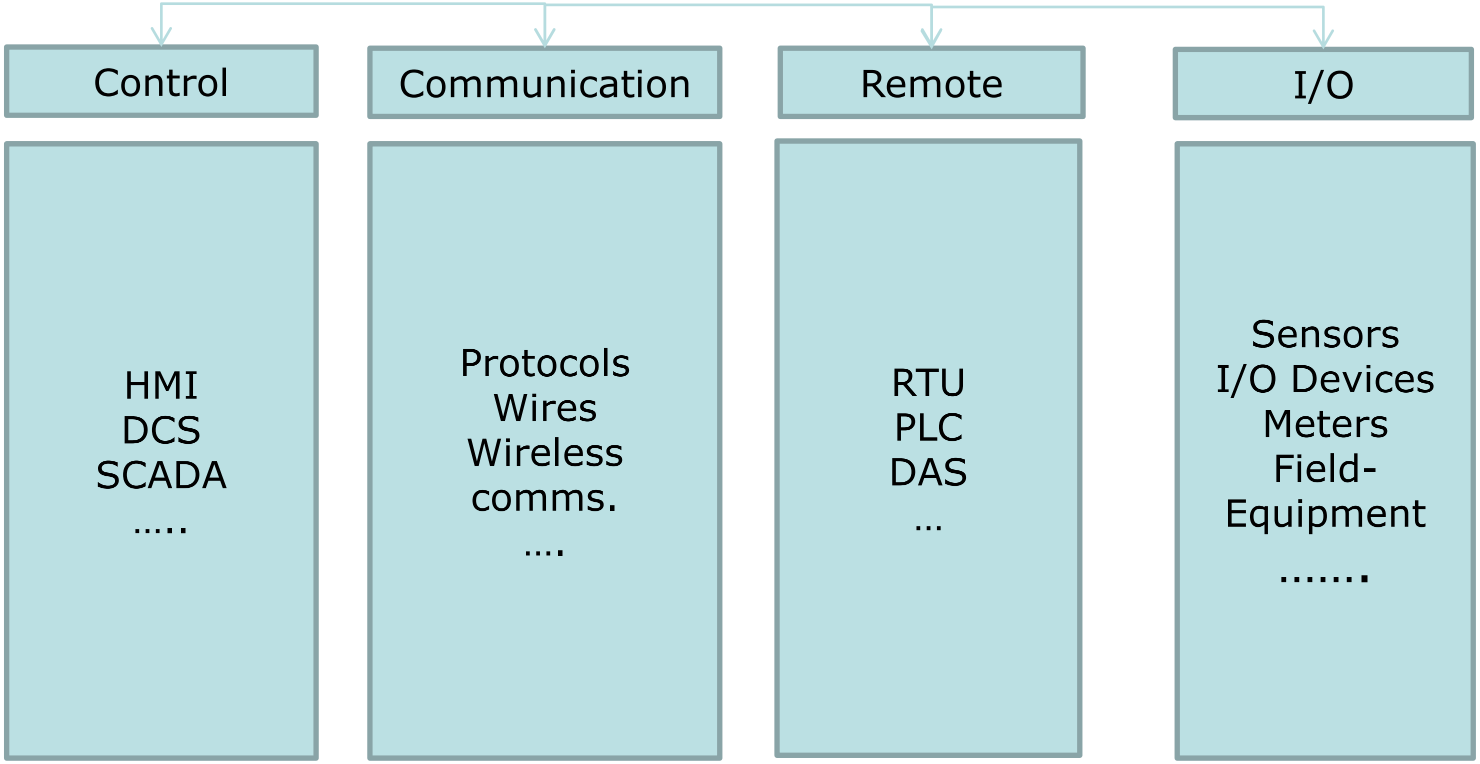
Adrian PĂUNA , NIS Expert
adrian.pauna@enisa.europa.eu

Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații
în contextul noilor abordări privind securitatea cibernetică.

Agenda

- Industrial Control Systems security
- Initiatives in the area of Critical Information Infrastructure
- ENISA’s work in the area

Industrial Control Systems



Control

HMI
DCS
SCADA
…..

Communication

Protocols
Wires
Wireless
comms.
….

Remote

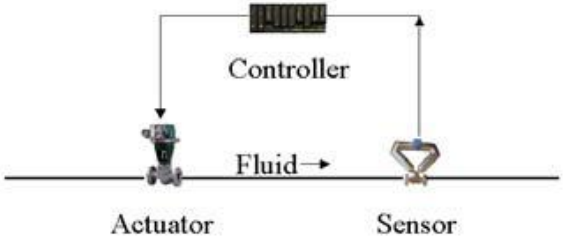
RTU
PLC
DAS
…

I/O

Sensors
I/O Devices
Meters
Field-
Equipment
…….

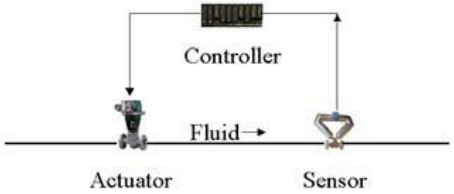
Industrial control systems

The first industrial control systems were simple point-to-point networks connecting a monitoring panel or command device to a remote sensor or actuator.



ICS/SCADA – 1st Gen

1964, IBM 1800 data acquisition and control system was described as "a computer that can monitor an assembly line, control a steel-making process or analyze the precise status of a missile during test firing."



ICS/SCADA – 2nd Gen

- In second generation, the controller is replaced with an embedded digital computer that runs desired control in software.
- Analog electrical signals are passed between the controller and the field devices.
- One physical line conveys one signal. It started a trend of truly distributed system in which the operator remotely controls the plant while sitting in the off the field control room.
- The operator works on a computer console connected to the controller.

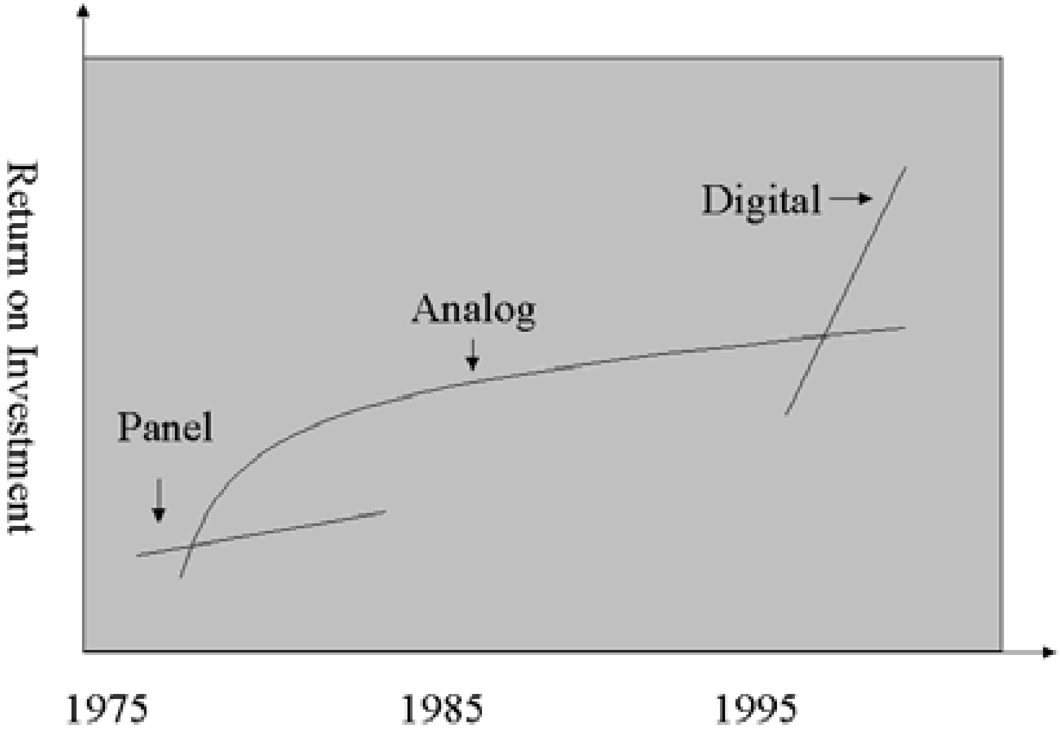
ICS/SCADA – 3rd Gen

- In the 1990's, a third generation system began to emerge. In this new generation, devices are empowered with computers.
- The *smart* device digitally communicates with the controller through field buses.
- One physical line conveys multiple control signals plus diagnostic/maintenance information.
- Personal computers replace expensive mini-computers. Standards are created to provide customers choices.
- Field bus standards include Foundation Fieldbus, Profibus, DeviceNet, etc. OPC was created to pass control information over computer networks.

ICS/SCADA – 4th Gen

What do you think will be the 4 generation?

Direct communication between client and control system?


Return on Investment
Digital
Analog
Panel
1975
1985
1995

Industrial control systems and communication/Process automation protocols

ControlNet – an implementation of CIP, originally by Allen-Bradley

HART Protocol

Modbus RTU or ASCII or TCP

Honeywell SDS – Smart Distributed System – Originally developed by Honeywell. Currently supported by Holjeron.

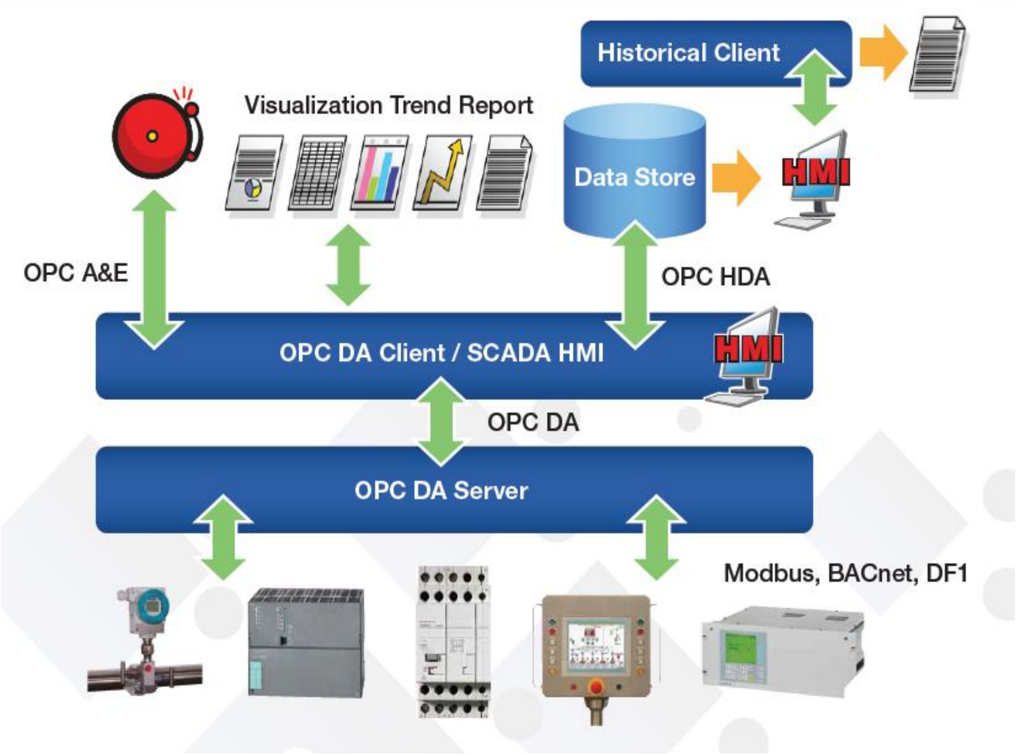
OSGP – The Open Smart Grid Protocol, a widely use protocol for smart grid devices built on ISO/IEC 14908.1

AS-i – Actuator-sensor interface, a low level 2-wire bus establishing power and communications to basic digital and analog devices

DeviceNet – an implementation of CIP, originally by Allen-Bradley

FOUNDATION fieldbus – H1 & HSE

OPC Open Platform Communications



- The **OPC Specification** was based on the OLE, COM, and DCOM technologies developed by Microsoft for the Microsoft Windows operating system family. The specification defined a standard set of objects, interfaces and methods for use in process control and manufacturing automation applications to facilitate interoperability.

EU level Initiatives

- In April 2007, the Council adopted the conclusions of a European programme for critical infrastructure protection (EPCIP)

- Key element of EPCIP is the Directive3 on the identification and designation of European Critical Infrastructures

- Information security issues for vital infrastructures in Europe are addressed by The Digital Agenda for Europe (DAE)4 and the CIIP action plan

International initiatives

- CIGRE, JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems
- International Atomic Energy Agency
- International Electrotechnical Commission (IEC)
- Institute of Electrical and Electronics Engineers
- IFAC stands for International Federation of Automatic Control.
- IFIP stands for International Federation for Information Processing

Initiatives

- ISACA
- International Society of Automation
- MERIDIAN Conference
- SANS
- UCA International Users Group
- Trusted Computing Group (TCG)
- Zigbee Alliance
- Seventh Framework Programme

Initiatives

- European Programme for Critical Infrastructure Protection (EPCIP)
- Action plan on CIIP
- EU-US Working Group (EU-US WG) on Cyber-security and Cybercrime
- European SCADA and Control Systems Information Exchange
- IMG-S
- Sixth Framework Programme

enisa

Initiatives

- European Network for Cyber Security (ENCS), formerly known as Cyber-TEC.
- Bundesverband der Energie- und Wasserwirtschaft BDEW
- NAMUR
- Verband der Großkraftwerks-B (VGB)
- Verein Deutscher Ingenieure (VDI)
- (Centre for the Protection of National Infrastructure) CPNI

Initiatives

- Test bed Framework for Critical Infrastructure Protection Exercise (Cloud CERT)
- North American Electric Reliability Corporation's (NERC)
- (National Institute for Standards and Technology) NIST
- SCADA hacker
- SANS
- ICS-CERT
- And many more

Training

- SANS
- Idaho National Laboratory
- Vendor based training
- Private initiatives at site

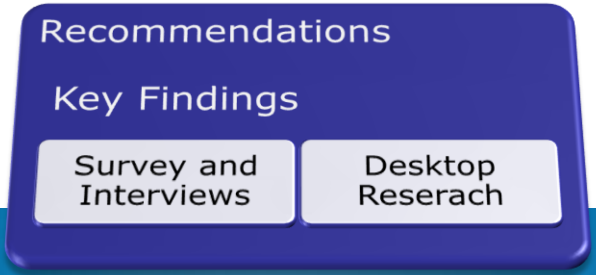
ENISA projects (2013):

1. Previous projects
2. Analyzing the European testing capabilities of ICS-SCADA Systems
3. Recommendations to address ICS-SCADA patching
4. Ex post analysis of security incidents in ICS-SCADA environments

1. ICS Security Study 2011

Aim/Scope of the Study

- ICS Security „panorama”
  - Threats, risks, challenges
  - National and pan-European initiatives
- Identification of gaps
- Recommendations
- Draft Report: *ENISA Recommendations on ICS Security*
- Workshop – 16 Sep, 2011



ENISA Recommendations

- National and Pan-European ICS Security Strategies
- Good Practices Guide for ICS Security
- ICS Security Plan Templates
- Awareness and Training
- Common Test Bed or ICS Security Certification Framework ✓
- National ICS-CERTs ✓
- Research in ICS Security
- The needs of research in the area of Patching and updating equipment without disruption of service and tools ✓

2. Analyzing the European testing capabilities of ICS-SCADA Systems

"Analyzing the European testing capabilities of ICS-SCADA Systems" - Background -

ENISA's document «*Protecting Industrial Control Systems - Recommendations for Europe and Member States* » (2011).

Recommendation 5: Creation of a **common test bed**, or alternatively, an **ICS security certification framework**.

The Common ICS security strategy should lead to the creation of a common test bed(s) at European level that **leverages existing initiatives**. This test bed would make use of realistic environments with the appropriate resources for conducting independent verification and validation tests.

An alternative choice to an European common test bed is the definition of a security framework model.

Objectives of the recommendation:

- Help all stakeholders to **detect potential problems** in a controlled environment.
- Provide operators with **independent** security evaluations and a **common security reference**.
- A **security framework model** adapted for ICS could be defined.
- Member State existing **certifying organisms** would be responsible for the certification process based on this security framework.

- Objectives-

The objectives of the work (from ENISAs Tender P/26/12/TCD):

- Assess the need among the Member States for a **national ICS-SCADA testing framework**.
- Identify the **gaps** between different (if any) MSs and the challenges involved in developing ICS-SCADA testing capabilities.
- Produce **guidance** for both the development of new and harmonization of current ICS-SCADA test beds frameworks (if any) among Member States.
- **Research and develop good practices** on developing a European ICS-SCADA test bed program/framework.

– Methodology -

Desktop Research

Questionnaires answered by experts for easy to analyse data

Interviews for deeper understanding

Questions categorized by Topics to Address:

A) Current Status

B) Objectives to Achieve

C) Model

D) Resources

E) Constraints

F) External Relationships

Experts categorised by «Stakeholder Type» and «Sector»

Analysis of the results:

search for Key Findings,

development of Recommendations

Final Workshop and Review 1st October Tallinn, ESTONIA

- Some Key Issues - status of ICS Security Testing

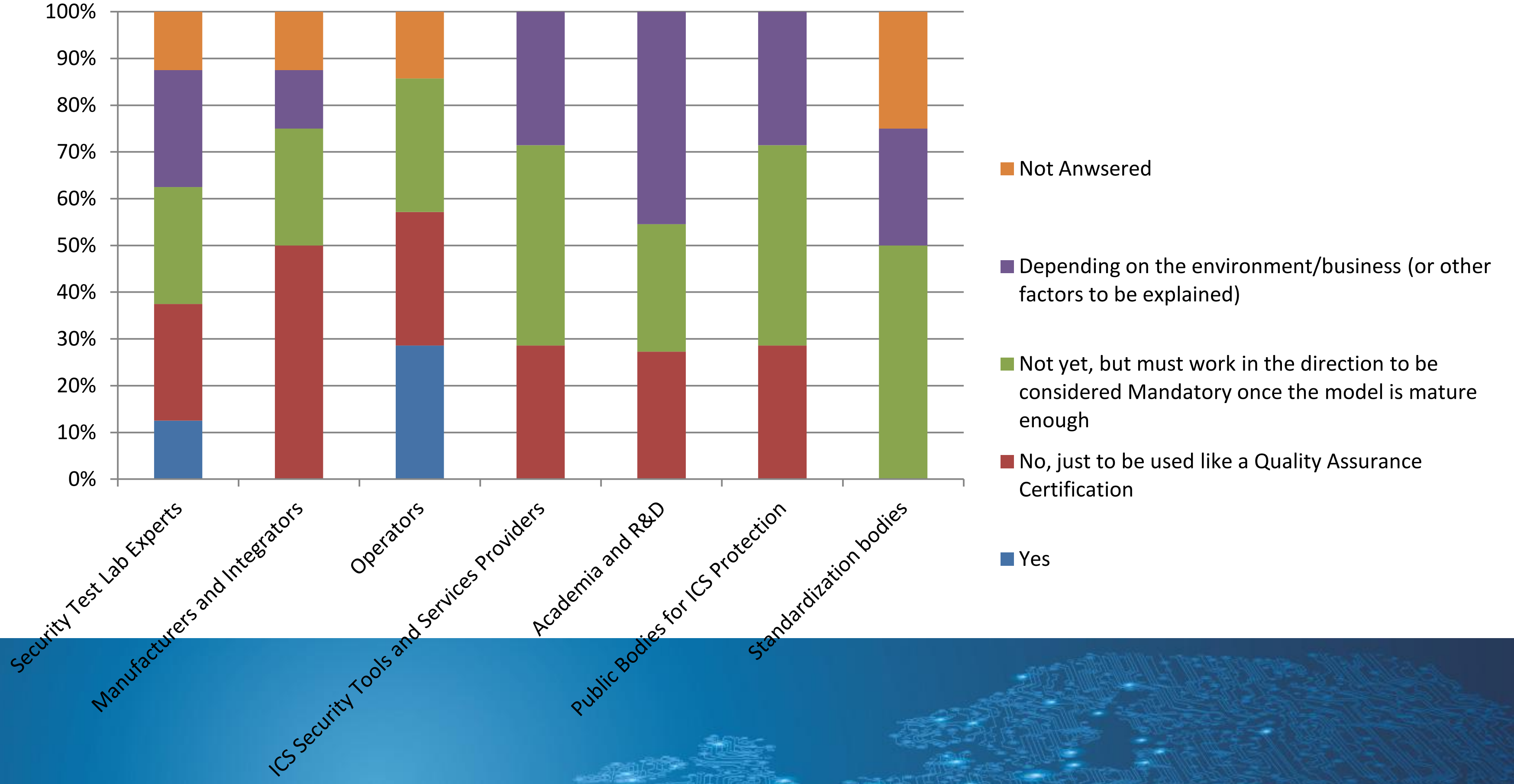
1.- High level of agreement regarding the status of ICS Security Testing in the EU. Most consider that the situation is bad or, at least, remarkably improvable.

- Some Key Issues - Making Testing Mandatory

2.- Less reluctance than expected in making testing mandatory

at least, in some cases, there is high agreement: i.e. Critical Infrastructures

Acceptance percentage of mandatory of the framework for any new technology or product by stakeholder type

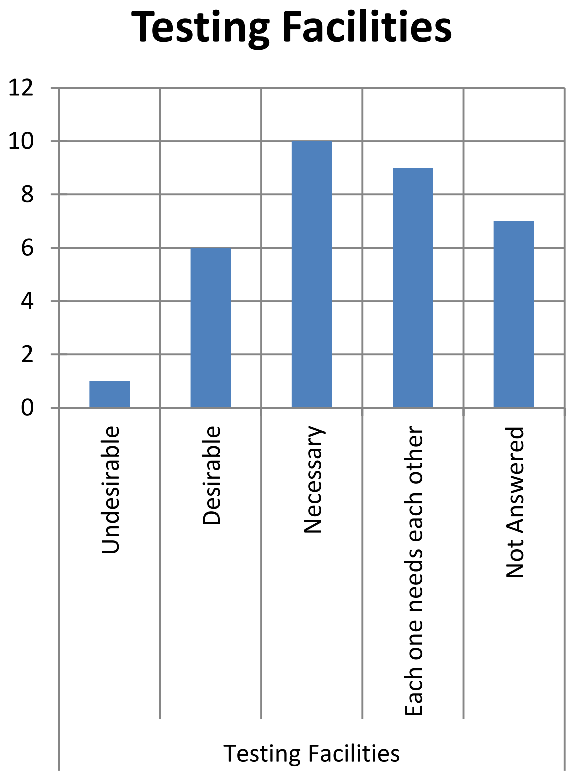


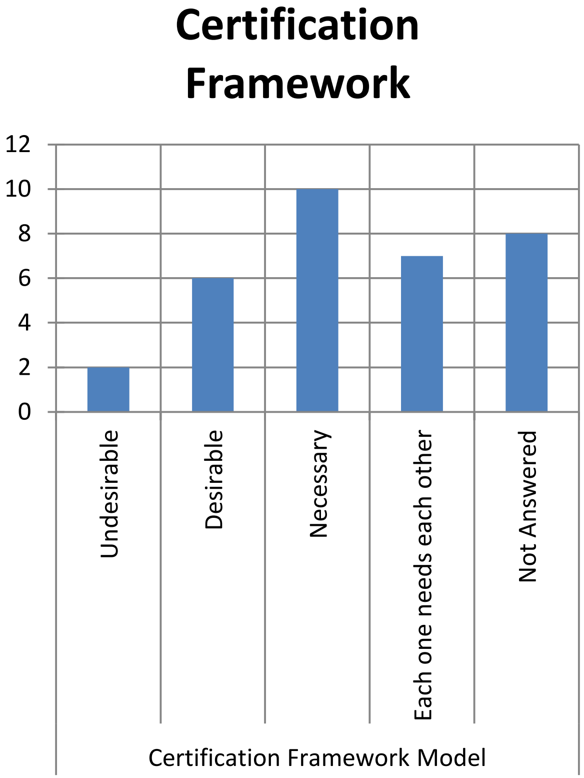
- Some Key Issues - Certification Framework model

3.- There is a big debate about the adequacy of using a Certification Framework model or how should it be applied to:

- devices, security postures by device-type or functionality,
- design and production processes, operations…

Certification Framework Model vs. ICS Testing Framework

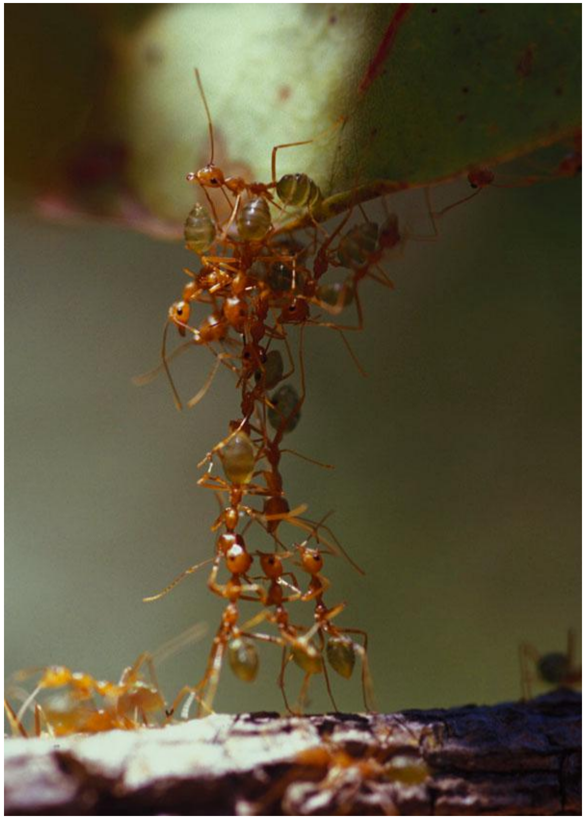




- Some Key Issues - Skills and Background

4.- Wide recognition that a key factors for testing success are the definition of what should be the skills and background knowledge of the involved technicians.

Current experiences show that a mixed profile, including IT Cybersecurity and OT knowledge is necessary for any **team** that aims to envision the complete picture.



- Some Key Issues - Building Trust

5.- Building trust between stakeholders has been signalled out as one of the most critical aspects for the Testing Initiative success.

It has to be taken into account during the definition of:

- the model, strategy, operations, testing criteria,
- vulnerability disclosures and any other potential conflicts.

3. Recommendations to address ICS-SCADA patching

"The need of **research** in the area of Patching and updating equipment without disruption of service and tools"
(ENISA's 2011 report on Protecting Industrial Control Systems)

"In 2011, ICS-CERT saw a **60% failure rate in patches** fixing the reported vulnerability in control system products."
(Kevin Hemsley –ICS-CERT)

"<50% of the 364 public vulnerabilities recorded at ICS-CERT had **patches available** at that time."
(SCADA Security Scientific Symposium (S4) in January 2012, Sean McBride)

A draft of "ISA-TR62443-2-3: Patch Management in the IACS Environment" was released for review. (ISA 99)

Objectives

Assess the challenges involved in:

- developing ICS-SCADA patching good practices.

Provide recommendations to all European Stakeholders on:

- how to meet these challenges.

Deliverable

Desktop research: review existing resources in order to:

- identify the gaps and challenges in existing ICS-SCADA patching practices.

Analysis of the findings and developing a:

- good practice guide with recommendations on patching ICS-SCADA.

Paradigm – EU level

Different approaches for the patching analysis.

Different patching management strategies/methodologies in place.

Existing ICS-SCADA patch management programs used.

Different issues which affect the ICS-SCADA patching process and at least one way to mitigate them.

Legal issues of patching/non-patching an ICS-SCADA system.

ENISA - Expectations

Provide the reader with examples and good practices for key technical aspects;

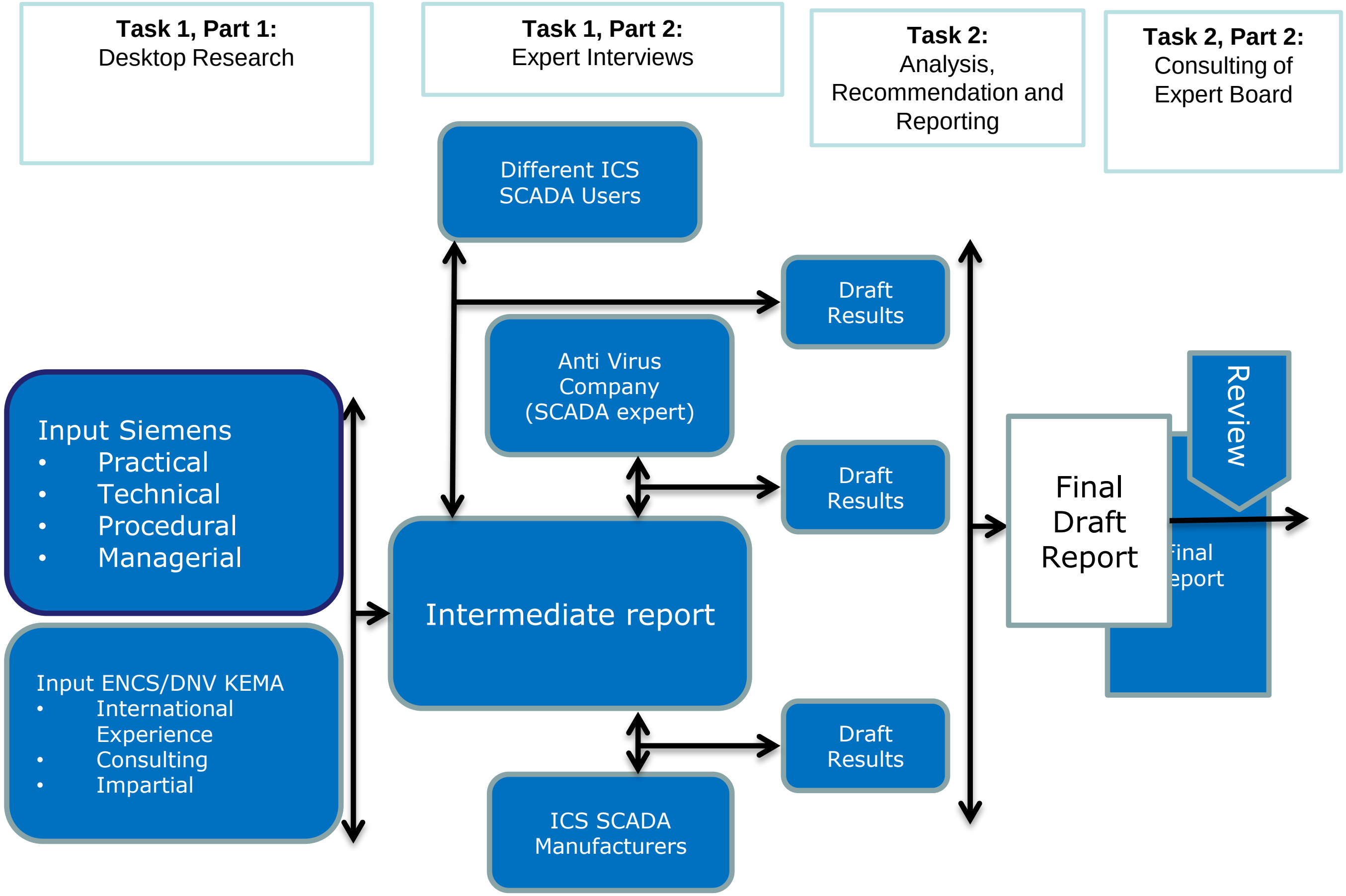
Different patching techniques and standards, relationships between them and gaps;

The role of virtualization in the patching process,

Key elements of an ICS-SCADA patching management methodology;

Good practice on developing a patching management methodology for ICS and SCADA systems;

The validation of the results will be based on the feedback taken by the experts who participated in the consultation



Task 1, Part 1:
Desktop Research

Task 1, Part 2:
Expert Interviews

Task 2:
Analysis, Recommendation and Reporting

Task 2, Part 2:
Consulting of Expert Board

Input Siemens
- Practical
- Technical
- Procedural
- Managerial

Input ENCS/DNV KEMA
- International Experience
- Consulting
- Impartial

Different ICS SCADA Users

Anti Virus Company (SCADA expert)

Intermediate report

ICS SCADA Manufacturers

Draft Results

Draft Results

Draft Results

Final Draft Report

Review

inal
eport

4. Ex-post analysis of security incidents in ICS-SCADA environments

Ex-post incident analysis aims primarily at investigating a security incident.

This report attempts to cover some basic ground by providing recommendations towards the implementation of a proactive environment that will facilitate agile and integrated response to incidents and their ex post analysis.

Ex post analysis

Scope

Good practices on analysing security incidents in ICS-SCADA environments

Forensic analysis is NOT part of the project.

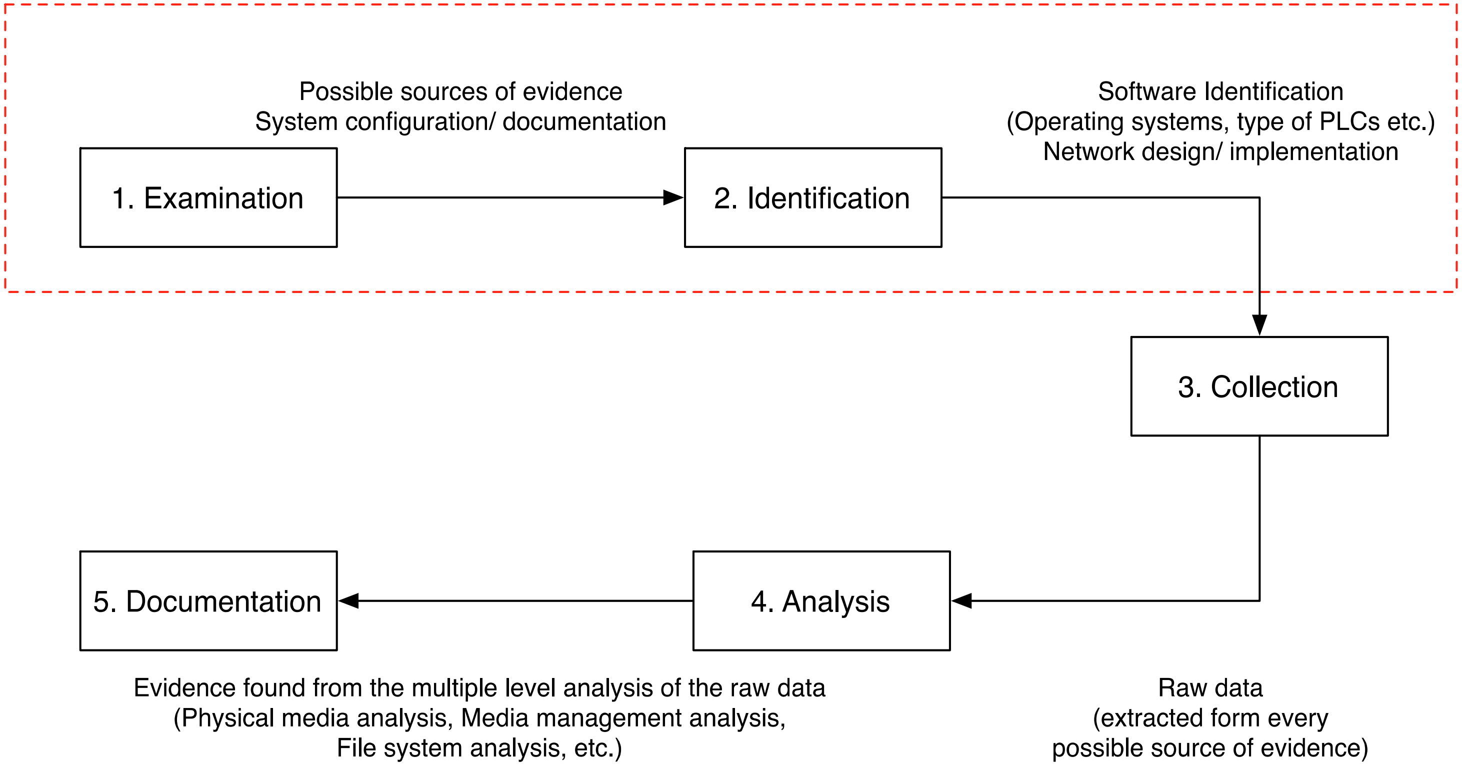
Objectives

Provide organizations with insight in the area of collecting and analysing information related to security incidents.

Provide the ICS-SCADA security experts with recommendations on good practices

- auditing and
- logging capability of the relevant infrastructure.

Ex post incident analysis process



Possible sources of evidence
System configuration/ documentation

Software Identification
(Operating systems, type of PLCs etc.)
Network design/ implementation

1. Examination

2. Identification

3. Collection

4. Analysis

5. Documentation

Evidence found from the multiple level analysis of the raw data
(Physical media analysis, Media management analysis,
File system analysis, etc.)

Raw data
(extracted form every
possible source of evidence)

Organisational structures & procedures for cyber incident response & investigation

The core components of cyber incident response with an embedded investigative component would be modified as :

- Detection
- Response Initiation
- Incident Response Action/ **Evidence Collection**
- Incident Recovery/ **Evidence Analysis**
- Incident Closure/ **Process Reporting**

	Control Centre	Field Devices
Modern/ Common Control Systems Technologies	- Contemporary ex post incident analysis tools can be used. - Network traffic capture. - Contact system administrator in case of modified OS on HMIs.	- Network logs. - Control centre's logs regarding field devices. • Device is off: Examination device for possible evidence • Device is on: Date and time, current active & running processes.
Modern/ Proprietary Control Systems Technologies	- Contemporary ex post incident analysis tools may be applicable. - Network traffic capture. - Interaction between the investigator and the vendor is mandatory.	- Network logs. - Control centre's logs regarding field devices. - Mandatory Interaction between investigator & vendor. - May involve embedded vendor-specific security mechanisms.
Legacy/ Proprietary Control Systems Technologies	- Traditional post-mortem anal. methods can't be applied. - No logging functionality - No longer supported by the vendor. - Interaction with the owner of the equipment may provide some information. - Serial-based communications; network traffic cannot be captured.	- Serial-based communication; network traffic cannot be captured. - Rapid rate of sampling and data override - Rapid rate of sampling and data override. - Interaction with the vendor is imperative. - An experienced engineer should be made available to support the investigation

Challenges /Recommendations

Challenges of data collection:

- **Inadequate logging mechanisms**:
- **High volatility of data**
- **Customised operating system kernels**
- **Extensive lower layer data**
- **Low computational power**

Challenges of data analysis:

- **Ex post analysis tools**
- **Data analytics and correlation**

Facilitate integration with existing structures for reporting and analysis:

- Understand where evidence may be found
- Understand the impact of data retention
- Manage obsolescence and the IT/Ops interface

Safeguard systems & configurations:

- Deploy adequate security controls that also perform logging, firewalls and intrusion detection systems
- Design systems with evidence protection in mind
- Enable logging of common events across the system as a minimum:

Challenges /Recommendations

Operational challenges:

- **The apparent culture gap** between Information Technology (IT) specialists and Operations personnel
- **The absence of dedicated scientific studies**
- **Management of obsolescence** and the availability of skills to handle legacy systems
- **The fundamentally different lifecycles** of the infrastructures

Review key roles and responsibilities:

- Identify gaps in digital investigation skills
- Identify physical and cyber response interfaces and overlaps

Pursue inter-organisational and interstate cooperation:

- A coordinated approach at inter-state level (e.g. pan European)
- Experience sharing and multi-party collaboration may enhance the chances of delivering a solution that is comprehensive and applies more

Thank you for your attention!

Follow ENISA: f in You Tube