Evaluation of ISA 99 in a Real-World Power Plant Security Assessment

Ragnar Schierholz, ABB Corporate Research
Sebastian Obermeier, ABB Corporate Research
Luca Guidi, ENEL
Daniela Pestonesi, ENEL
Giorgio Carpi, ENEL

ICSJWG 2010 Spring Conference

ISA 99 – Brief intro

ANSI/ISA-99: “Security for Industrial Automation and Control Systems”

Broad scope, covering (according to current plans)

- Policies and procedures for secure operations
- System design (e.g. network segregation)
- Technical requirements for systems and products
- Product development lifecycle
- Metrics for measuring security assurance

Partially completed, partially work in progress, partially planned

Plans for co-publishing as IEC 62443 for broader international acceptance

ISA 99 – Work products

ISA99 Common	**ISA-99.01.01** Terminology, Concepts And Models	**ISA-TR99.01.02** Master Glossary of Terms and Abbreviations	**ISA-99.01.03** System Security Compliance Metrics	
Security Program	**ISA-99.02.01** Establishing an IACS Security Program	**ISA-99.02.02** Operating an IACS Security Program	**ISA-TR99.02.03** Patch Management in the IACS Environment	
Technical - System	**ISA-TR99.03.01** Security Technologies for Industrial Automation and Control Systems	**ISA-99.03.02** Security Assurance Levels for Zones and Conduits	**ISA-99.03.03** System Security Requirements and Security Assurance Levels	**ISA-99.03.04** Product Development Requirements
Technical - Component	**ISA-99.04.01** Embedded Devices	**ISA-99.04.02** Host Devices	**ISA-99.04.03** Network Devices	**ISA-99.04.04** Applications, Data And Functions

Published | In Progress | Planned

Background

ESCoRTS – **E**nhanced **S**ecurity for **Co**ntrol and **R**eal-**T**ime **S**ystems is a Coordination and Support Action funded by the European Commission – Framework Programme 7

Main objectives are

- disseminating best practice on security of Supervisory Control and Data Acquisition (SCADA) systems
- Driving and ensuring convergence of SCADA standardisation processes worldwide
- paving the way to establishing cyber security testing facilities in Europe

See more at http://www.escortsproject.eu/

Targeted Experiments

Objectives

- Evaluation of existing standard applicability
- Impact on security methods and actions
- Focus on electricity generation

Standard as reference

- ISA-99

Efforts

- ~ one person week preparation
- 3 days on-site assessment with between 8 and 13 participants from ENEL (asset owner) and ABB (vendor)
- ~ one person week for report generation

Setup

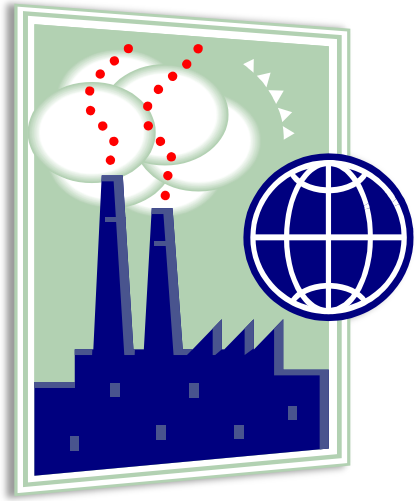
Location: Operating combined cycle power plant in Italy (redesigned in 2003)

Participants: Cross-functional team

- Research organizations (both asset owner & vendor)
- Asset owner's enterprise security organization
- Asset owner's enterprise ICT
- Asset owner's plant operations
- Vendor's product responsible unit
- Vendor's system unit (project engineers)

Three focus areas of the assessments

- ISA-99 applicability, usability and utility
- ENEL plant security in light of ISA-99
- ABB product capability in light of ISA-99

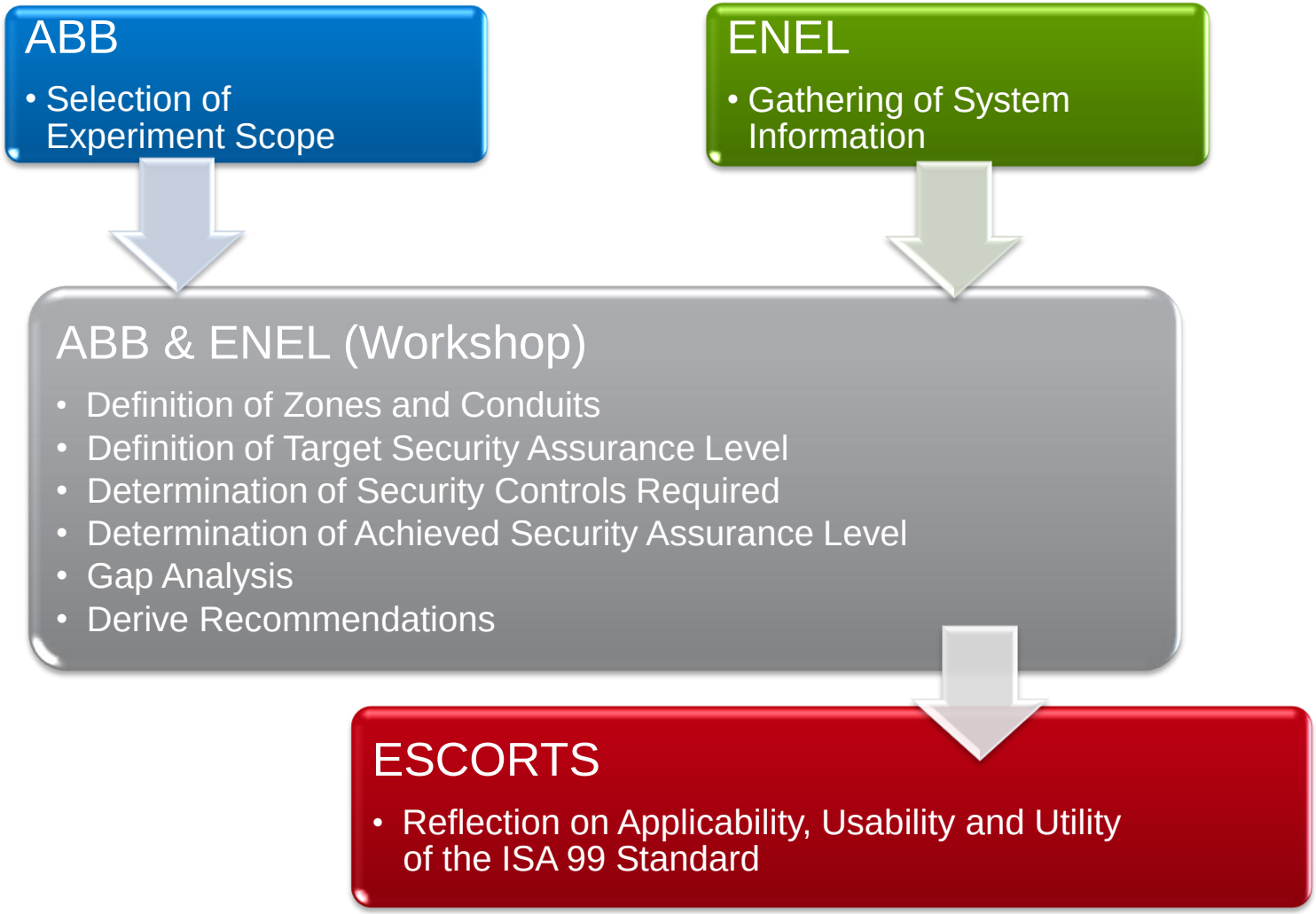


Covered ISA 99 Scope

ISA99 Common	**ISA-99.01.01 Terminology, Concepts And Models**	**ISA-TR99.01.02** Master Glossary of Terms and Abbreviations	**ISA-99.01.03** System Security Compliance Metrics	
Security Program	**ISA-99.02.01** Establishing an IACS Security Program	**ISA-99.02.02** Operating an IACS Security Program	**ISA-TR99.02.03** Patch Management in the IACS Environment	
Technical - System	**ISA-TR99.03.01 Security Technologies for Industrial Automation and Control Systems**	**ISA-99.03.02** Security Assurance Levels for Zones and Conduits	**ISA-99.03.03** System Security Requirements and Security Assurance Levels	**ISA-99.03.04** Product Development Requirements
Technical - Component	**ISA-99.04.01** Embedded Devices	**ISA-99.04.02** Host Devices	**ISA-99.04.03** Network Devices	**ISA-99.04.04** Applications, Data And Functions

mostly | partially | not covered

Assessment workflow



Assessment “tools“

Standard does not provide assessment templates

Custom checklist spreadsheet for assessment documentation

67		**Physical and evironmental security**			
78					
79		**Network segmentation**			
80	4.3.3.4.1	Develop the network segmentation architecture			
81	4.3.3.4.2	Employ isolation or segmentation on high-risk IACS			
82	4.3.3.4.3	Block non-essential communications with barrier devices			
83					
84		**Access control: Account administration**			
85	4.3.3.5.1	Access accounts implement authorization security policy	Assessment comments		3 = Fully addressed
86	4.3.3.5.2	Identify individuals		Example Ratings -->	2 = Partially addressed
87	4.3.3.5.3	Authorize account access			1 = In preparation
88	4.3.3.5.4	Record access accounts			0 = Not addressed
89	4.3.3.5.5	Suspend or remove unneed accounts			
90	4.3.3.5.6	Review account permissions			
91	4.3.3.5.7	Change default passwords			
92	4.3.3.5.8	Audit account administration			
93					
94		**Access control: Authentication**			

Assessment findings

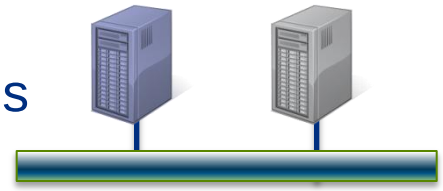
General approach of ISA well targeted to control systems

- Reflects and links risk assessment to security planning
- Operational security requirements (policies, procedures, ...) comprehensive and easy to evaluate

ISA-99 well structured

Identification of “zones” and “conduits” difficult

- ISA-99 imposes several requirements for zone definitions, but leaves a lot of discretion for asset owners
- Detailed requirements in terms of security controls for each zone are present, but difficult to use



Determination of System Security Assurance Levels (SAL) is difficult, as the link between “impact” and “SAL” is missing

Assessment findings

(cont'd)

Suggestion for ISA 99 revision

- SAL definition overly formal, e.g. mandates classifications which are not used later on

More guidance on compensating security controls desirable

- ISA 99.03.02 paragraph 5.2

Detailed fine-tuning of requirements would be helpful. Examples:

- "Expiration of accounts after a period of inactivity"
  (on-site maintenance accounts vs. hardly used supervisor accounts)

Existing mapping of roles and responsibilities (in ISA99 03.02 Annex C) is helpful and important. It should also be included in other parts, but content of matrix is not yet mature.

Assessment findings

(cont'd)

To implement, maintain and document ISA99 compliance requires significant effort for a power generation utility:

- several devices/systems, complex infrastructure, many people involved
- different organization units must cooperate, creation of new organization units could be necessary, entire life cycle requires continuous effort, etc.

To implement, maintain and document ISA99 compliance requires significant effort for an IACS vendor:

- embed security in the design of the IACS system
- IACS integration in a customer owned infrastructure challenging

Assessment findings

(cont'd)

Cross-Function teams are necessary:

- Experts for several domains were present

Time for discussions should not be underestimated - only a part of ISA 99 could be considered in the experiment

- Impact analysis ("what happens if…") is time consuming
- Complete ISA 99 assessment expensive and time-consuming

Additional effort in creating templates and reporting tools

Compliance metrics monitoring (ISA-99.01.03) is important for auditing, but the value of certification is considered controversial. Risk assessment guidelines and vulnerability tests seem to be necessary, too.

Thank you!

Dr. Ragnar Schierholz

Principal Scientist
Industrial Software Systems

ABB Switzerland
Corporate Research
Segelhofstr. 1K
CH-5405 Baden 5 Dättwil
Phone +41 58 586 82 97
Mobile +41 79 733 67 47
E-Mail ragnar.schierholz@ch.abb.com