SCADA/IACS and Smart Grid Security Standards, Guidelines and Test Centers

International Seminar on:
Critical infrastructure protection in the energy and communications. Energy and Communication sector interdependencies
Critical information infrastructure in the context of new approaches to cyber security
Cooperation between the government, business community and civil society

Date: *10 – 11 October 2013*

Place: *Library of University Politehnica of Bucharest*

Sandro Bologna
s.bologna@infrastrutturecritiche.it

www.InfrastruttureCritiche.it

Information Systems vs. Industrial Control Systems (1/3)

Information Systems	Industrial Control Systems
Non-Hard Realtime	Hard Realtime
Response must be reliable	Response must be reliable and time critical
High throughput demanded	Modest throughput demanded
High delay and jitter accepted	High delay and/or jitter is a serious concern

Different Performance Requirements

Information Systems vs. Industrial Control Systems (2/3)

Information Systems	Industrial Control Systems
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Beta testing in the field acceptable	Thorough testing before installed expected

Different Reliability Requirements

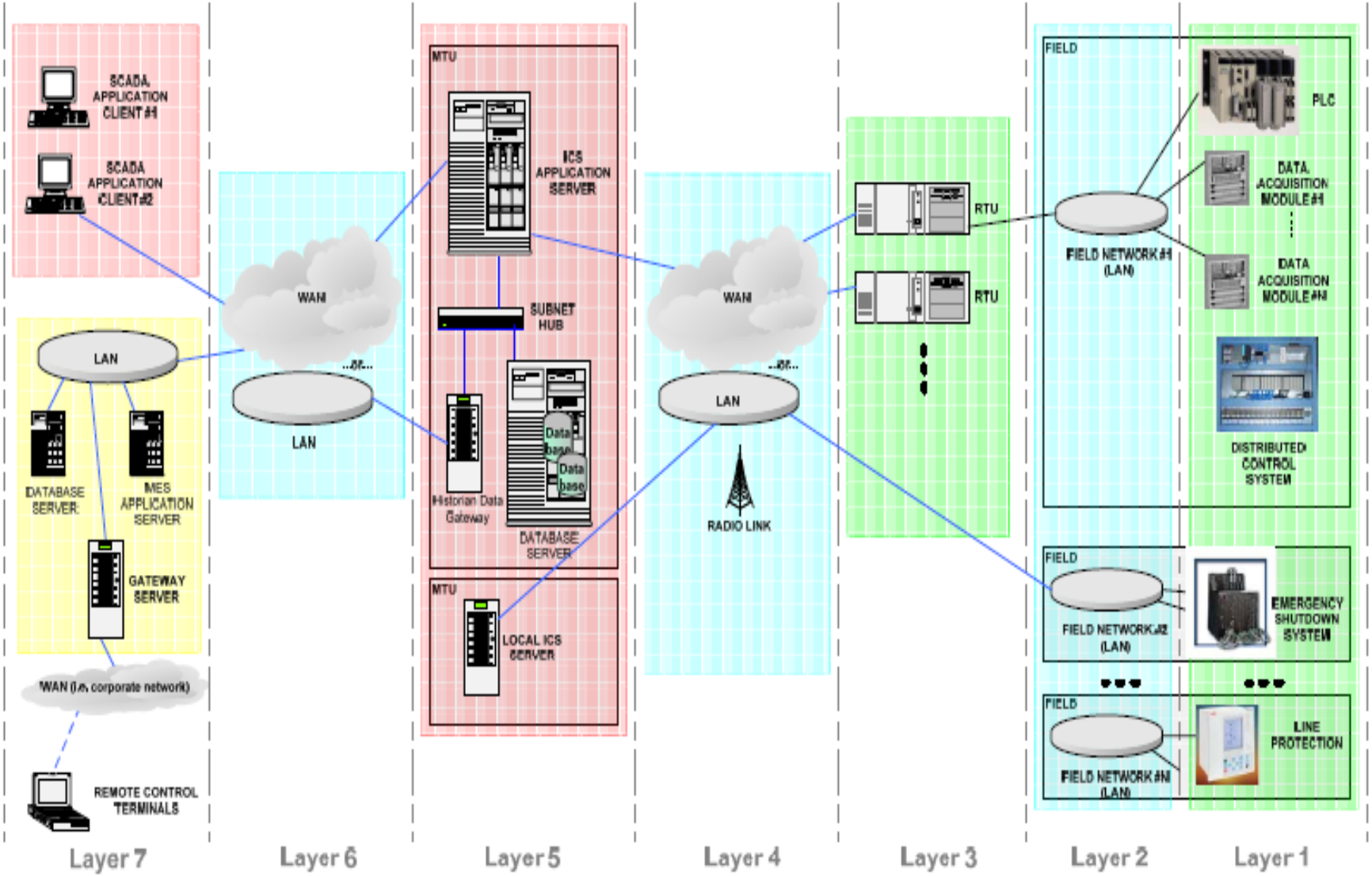
Information Systems vs. Industrial Control Systems (3/3)

Information Systems	Industrial Control Systems
Data integrity paramount	Human safety paramount
Risk impact is loss of data, loss of business operations	Risk Impact is loss of life, equipment or product, environmental damage
Recover by reboot	Fault tolerance essential

Different Risk Management Requirements: Delivery vs. Safety

These differences create huge differences in acceptable security practice

Possible view of a SCADA/IACS system



Source:ESTEC JLS/2007/D1/22 Final Report

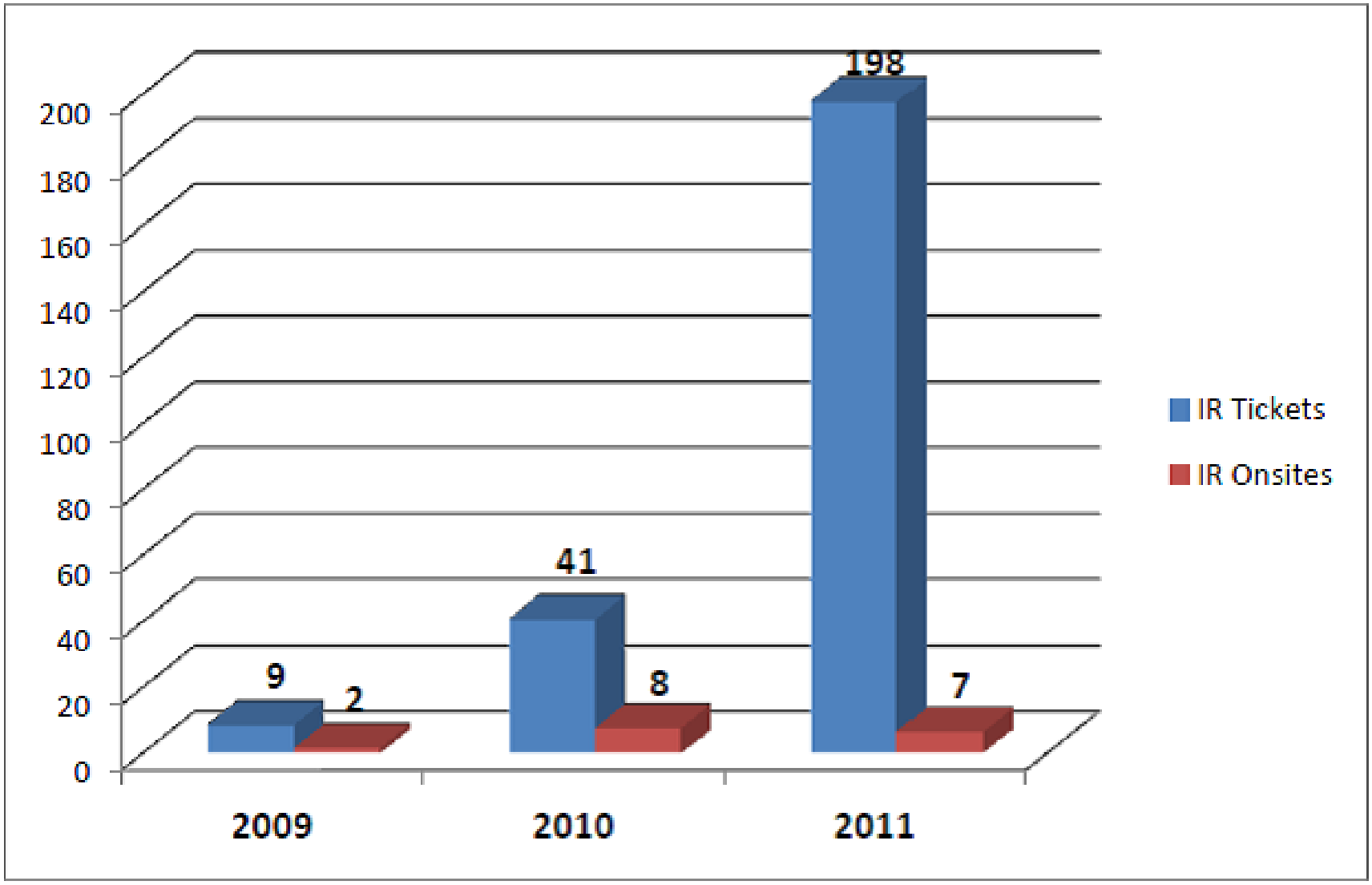
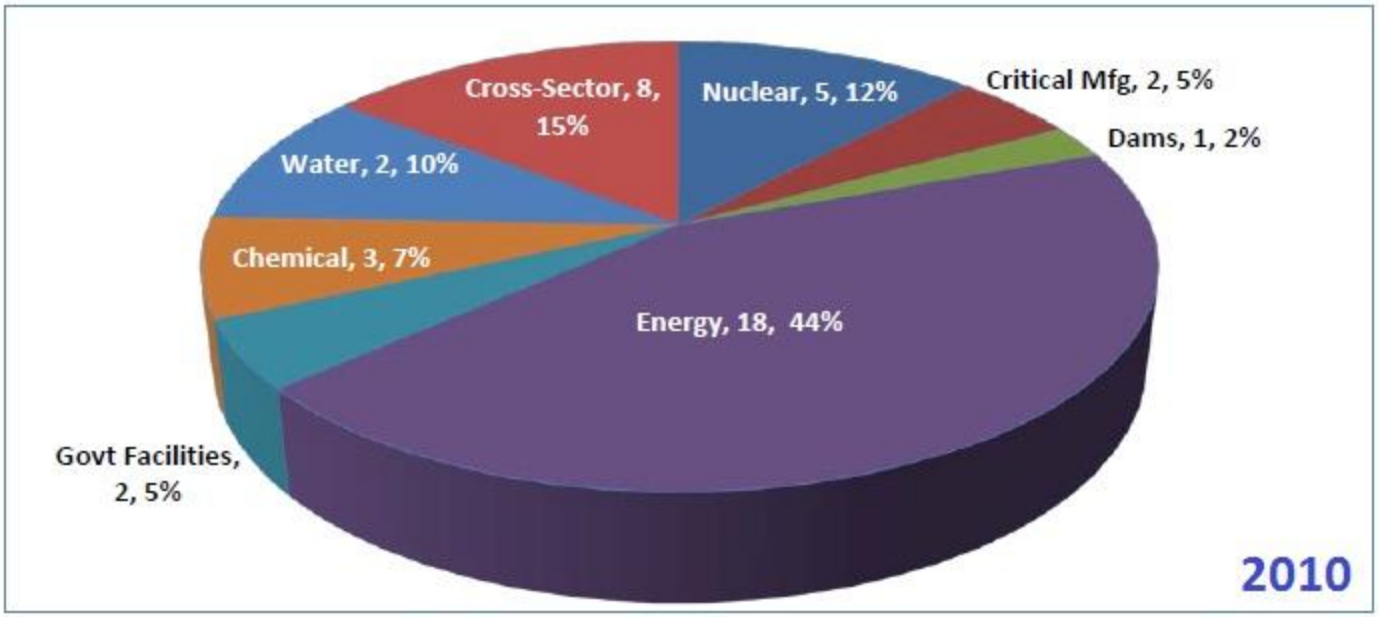
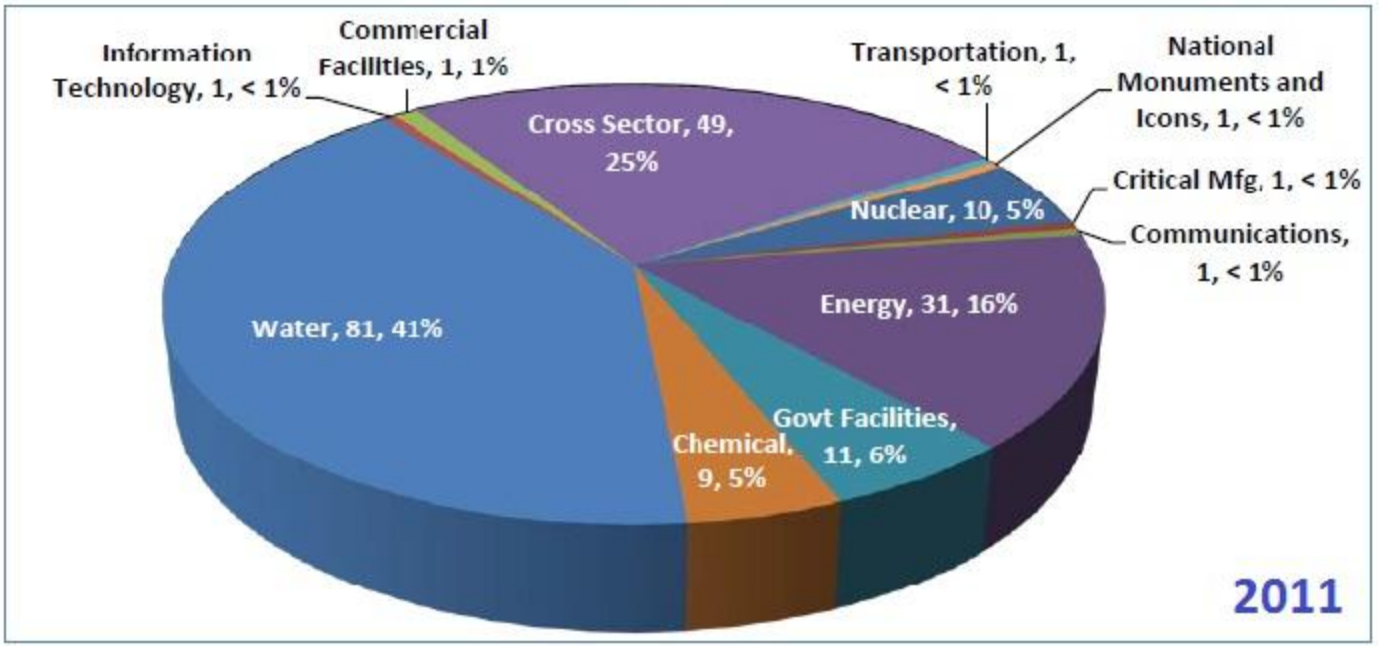


Figure 1. ICS-CERT incident response trends data.

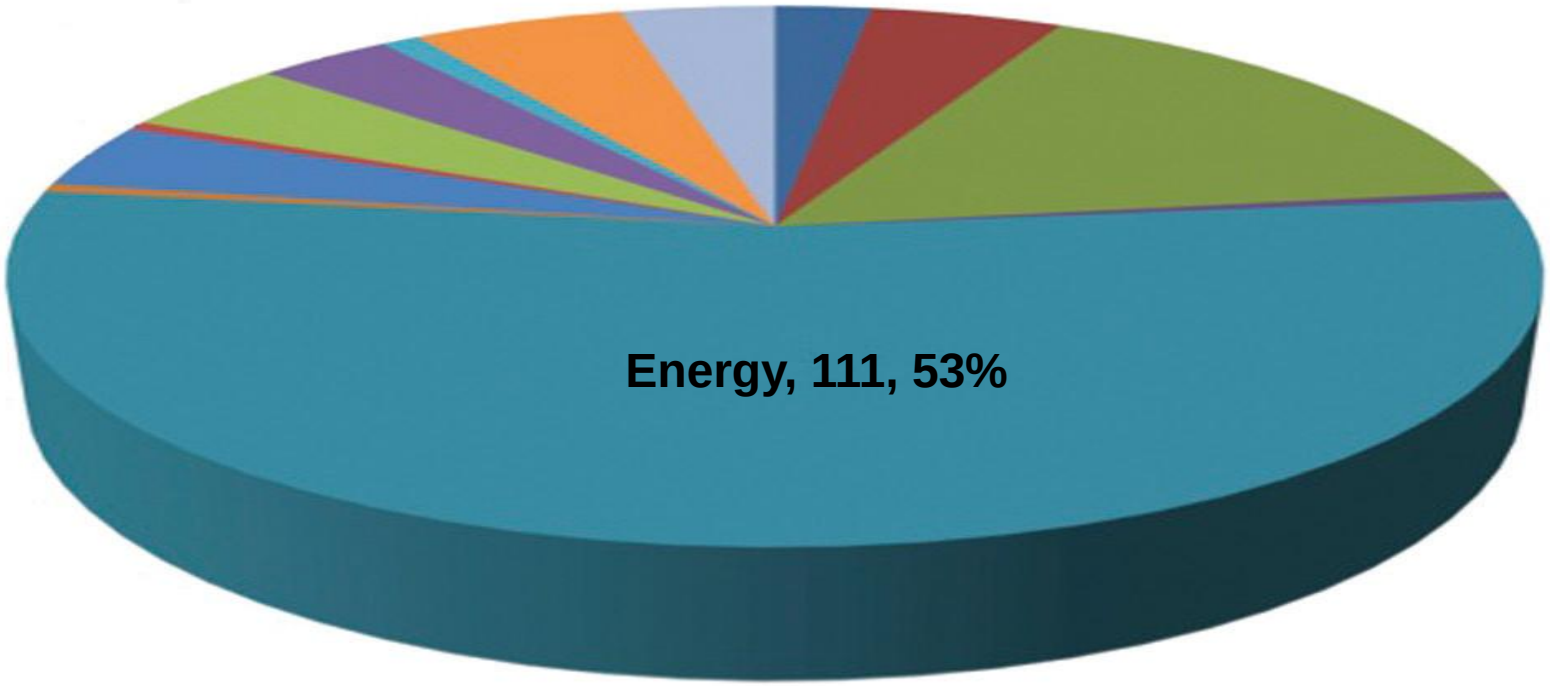
Source: US ICS-CERT Incident Response Summary Report 2009−2011





Source: US ICS-CERT Incident Response Summary Report 2009−2011

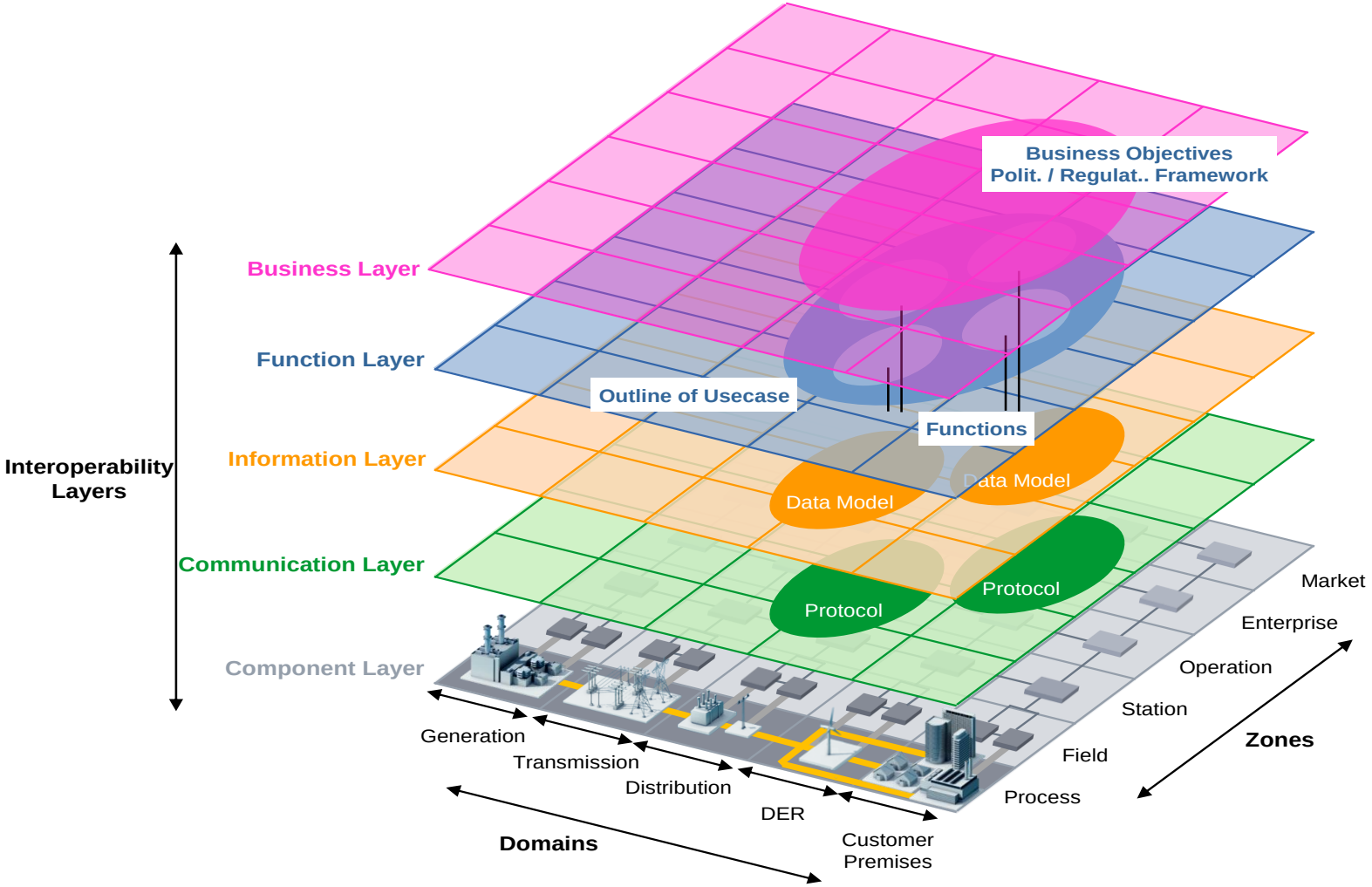
US DHS ICS – CERT MONITOR June 2013



In the first half of fiscal year 2013, (October 1, 2012–May 2013), US-ICS-CERT has responded to over 200 incidents across all critical infrastructure sectors.
The highest percentage of incidents reported to US-ICS-CERT occurred in the energy sector at 53%.

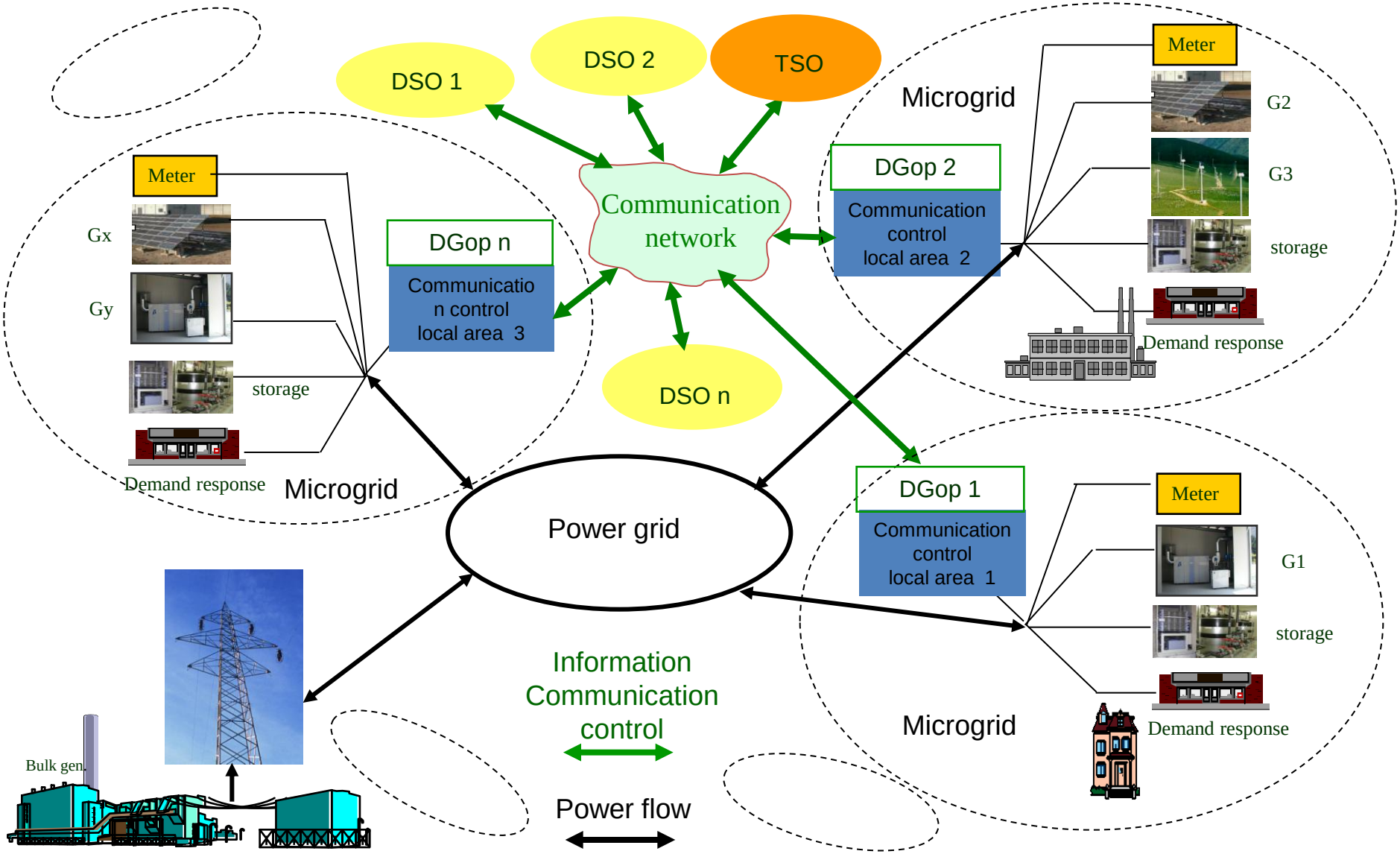
Smart Grid Architecture Model (SGAM)

Integrated approach involving technical, commercial and regulatory issues



Source: CEN-CENELEC-ETSI Smart Grid Coordination Group

Possible view of active network operation (Smart Grid)



Source: Massimo Gallanti RSE
Sandro Bologna ENEA

ERNCIP Project: European Reference Network for Critical Infrastructure Protection

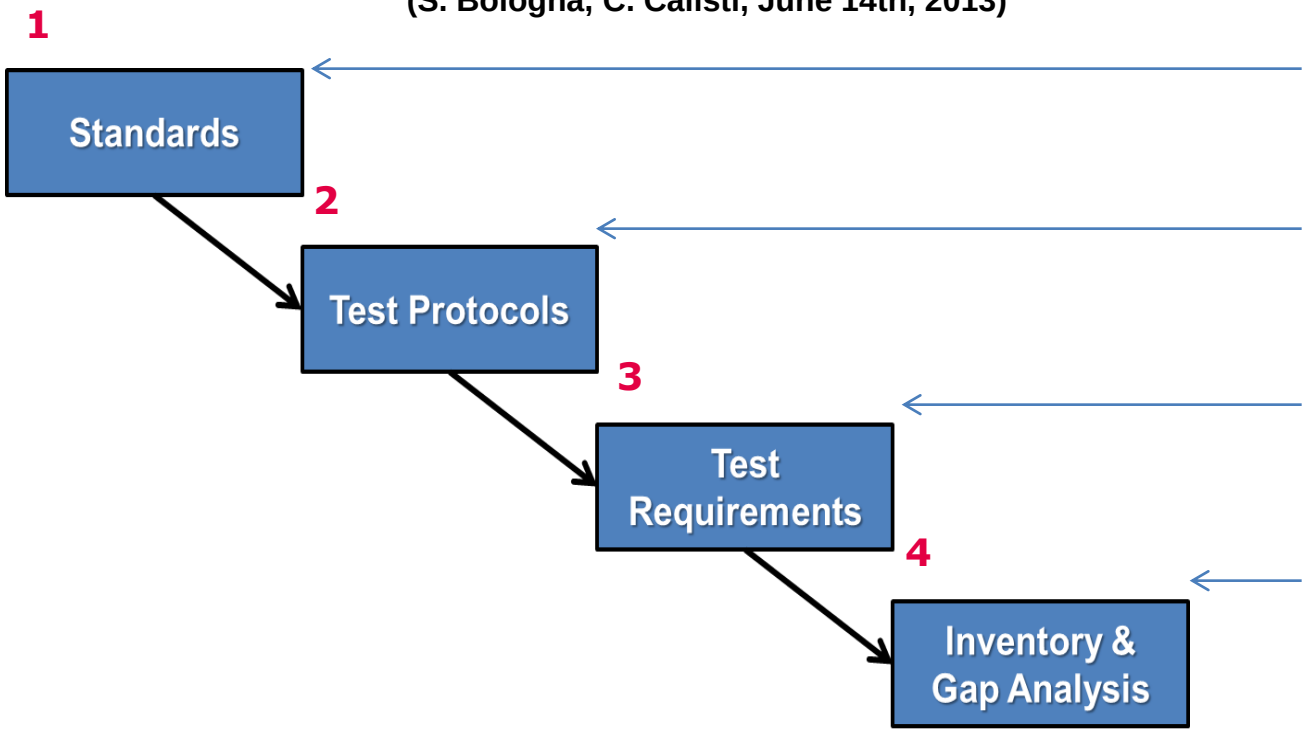
ERNCIP Expert Group Romania Representative <merla.nicolae@mai.gov.ro>

Thematic Area IACS & SG: Industrial Automation and Control Systems & Smart Grids

Task Title: Trusted Test Centres for IACS & SG

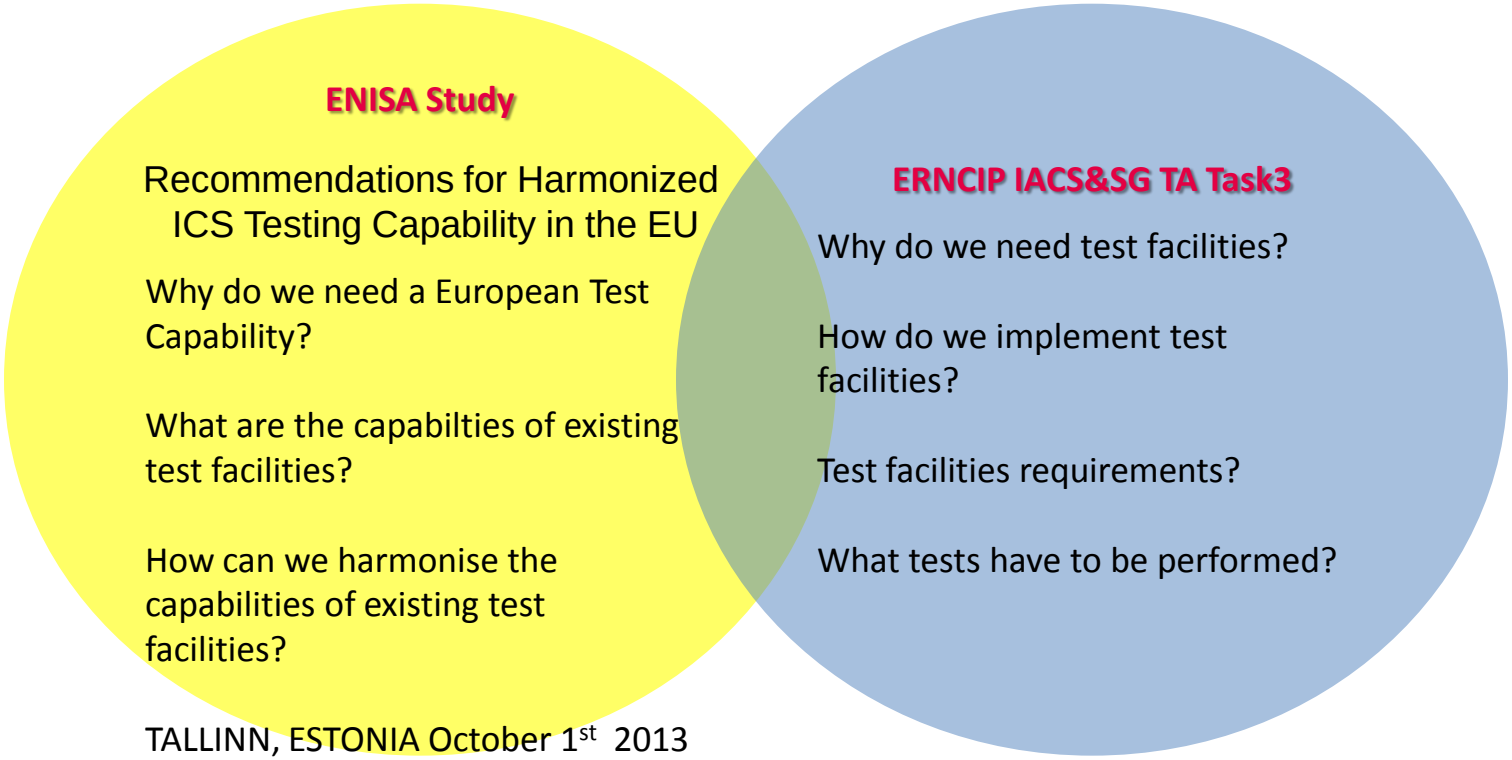
Proposed overall approach to harmonized Test Centers

(S. Bologna, C. Calisti, June 14th, 2013)

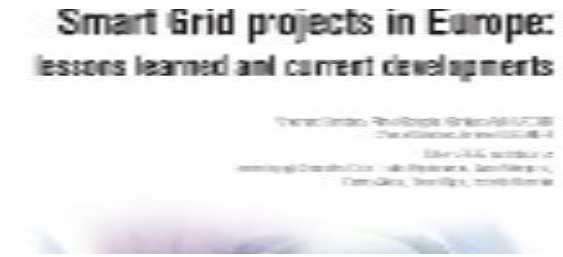


Connections with other initiatives

- ESTEC JLS/2007/D1/22
- ESCoRTS SEC-207-7.0-02
- VIKING http://www.vikingproject.eu
- ESMIG http://www.esmig.eu/
- ENISA study “Recommendations for Harmonized ICS Testing Capability in the EU”



JRC Institute for Energy (2011) : Smart Grid projects in Europe: lessons learned and current developments



First Inventory of Smart Grids in Europe
completed in **2011**

- **219 Smart Grid projects in EU27**

€ 5 billion overall investment

- **Majority of projects in EU15**

while most of EU12 lag behind

EU Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids (DG CONNECT 2011-2012)

(Report in https://ec.europa.eu/digital-agenda/en/news/cybersecurity-smart-grids)

- It is needed to carry out an overall risk assessment to identify the specific well-balanced and effective set of security measures to be adopted by relevant operators

- The need for different levels of security measures adapted to the different architectural layers of the Smart Grid, to keep the Smart Grid infrastructure as robust and as resilient as possible

- Define high level security requirements to enhance the security and resilience of ICT for Smart Grids

- Industrial Control Systems, and not only the smart meters, draw today the primary cyber security focus

- An EU-wide harmonization of security standards is needed

EC DG-ENERGY M/490 Mandate
SGCG – SGIS Working Group

http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

Mandate Scope and Objectives

- *" The objective of this mandate is to **develop or update a set of consistent standards** within a common European framework […] that will achieve interoperability and will enable or facilitate the implementation in Europe of […] Smart Grid services and functionalities […]. "*

- *" It will answer the technical and organizational needs for **sustainable "state of the art" Smart Grid Information Security (SGIS),** Data protection and privacy (DPP), […]. "*

- *" This will enable smart grid services through a Smart Grid information and communication system that is **inherently secure by design** within the critical infrastructure of transmission and distribution networks, as well as within the connected properties (buildings, charging station – to the final nodes).*

ENISA Report Protecting Industrial Control Systems (ICS). Recommendations for Europe and Member States (2011)

The ENISA report evaluates the current state of ICS security and offers seven recommendations for improvement

- ***1: Creation of Pan-European and National ICS Security Strategies***
- ***2: Creation of a Good Practices Guide for ICS Security***
- ***3: Creation of ICS security plan templates***
- ***4: Foster Awareness and Training***
- ***5: Creation of a common test bed, or alternatively, an ICS security certification framework***
- ***6: Creation of national ICS-computer emergency response capabilities***
- ***7: Foster research in ICS security leveraging existing Research Programmes***

ENISA Smart Grid Security Recommendations for Europe and Member States (2012)

This ENISA study makes 10 recommendations to the public and private sector involved in the definition and implementation of smart grids

- ***1: Improve the regulatory and policy framework***
- ***2: Foster the creation of a Public-Private Partnership (PPP) entity to coordinate smart grid cyber security initiatives***
- ***3: Foster awareness raising and training initiatives***
- ***4: Foster dissemination and knowledge sharing initiatives***
- ***5: Develop a minimum set of reference standards and guidelines***
- ***6: Promote the development of security certification schemes for products and organisational security***
- ***7: Foster the creation of test beds and security assessments***
- ***8: Refine strategies to coordinate large scale pan-European cyber incidents affecting power grids***
- ***9: Involve CERTs to play and advisory role in dealing with cyber security issues affecting power grids***
- ***10: Foster research in smart grid cyber security leveraging existing research programmes.***

ENISA study on Appropriate Security Measures for Smart Grids (v. 1.5 2012-1022)

(The report was expected to be released by the end of the year 2012 but it has not yet been officially released)

The Draft of new ENISA study based on the most relevant frameworks and standards generally identified or already used by stakeholders does the following high-level conclusions

- ***1: There is a challenge linked to the proliferation of various security standards and guidances***
- ***2: There is a need for alignment of initiatives, standards, frameworks, etc.***
- ***3: Regulators have an important role in promoting security of the smart grid from the beginning***
- ***4: Importance of a risk assessment activity at started point for the effective and practical implementation of the appropriate security measures for smart grid***
- ***5: Security is not static, on the contrary, it is an everlasting and evolving domain***

ENISA study on Appropriate Security Measures for Smart Grids (2012-12-06)

(The report was expected to be released by the end of the year 2012 but it has not yet been officially released)

The Draft of new ENISA study based on the most relevant frameworks and standards generally identified or already used by stakeholders does a catalogue of security measures in the following domains

1. **Security governance & risk management**
2. **Management of third parties**
3. **Secure lifecycle process for smart grid components/systems and operating procedures**
4. **Personnel security, awareness and training**
5. **Incident response & information knowledge sharing**
6. **Audit and accountability**
7. **Continuity of operations**
8. **Physical security**
9. **Information systems security**
10. **Network security**

ANSI/ISA-99 (2009): Security for Industrial Automation and Control Systems

- A core concept in the ANSI/ISA-99 (now IEC 62443.02.01) security standard is “Zones and Conduits”
- Offers a level of segmentation and traffic control inside the control system
- Control networks divided into layers or zones based on control function
- Multiple separated zones to manage the “***defense in depth***” strategy

INL/EXT-09-15500 (2009): Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues

- Smart Grid design and deployment must take into account the current cyber vulnerabilities in the legacy power grid

- There must be a coordinated and ongoing effort to secure the Smart Grid that includes the full development lifecycle

- The goal of “resistance to attack” is in competition with some of the other desired characteristics of the Smart Grid, e.g. “optimizes assets and operates efficiently”

- The desire to minimize costs and to provide services tend to take priority over the desire for security in the face of a threat that is not well understood

US National SCADA Test Bed Program (NSTB)

http://www.inl.gov/scada/

The National SCADA Test Bed is a national capability to help secure SCADA communications and controls within the energy sector. It combines the expertise and resources of several national laboratories into a multi-lab partnership that helps to identify and correct critical security flaws in control

The NSTB offers the integrated expertise and resources of multiple national laboratories, including Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory, and Oak Ridge National Laboratory.systems and equipment.

NSTB Recommendations for SCADA vendors

The following is a summary of recommendations for SCADA vendors:

- Create a security culture
- Ehnance SCADA test suites
- Create and test patches
- Redesign network protocols for security
- Increase robustness of network parsing code
- Implement and test strong authentication and encryption mechanisms
- Improve security through external software security assessments

Source: INL/EXT-10-18381 Vulnerability Analysisi of Energy Delivery Control Systems

NSTB Recommendations for Owners/operators

Owners/operators are recommended to increase the security of their systems by completing the following recommendations:

- Restrict SCADA user privileges to only those required
- Change all default passwords and require strong passwords
- Test and apply patches
- Protect critical functions with network security zones and layers
- Customize IDS rules for the SCADA and closely monitor logs

Source: INL/EXT-10-18381 Vulnerability Analysisi of Energy Delivery Control Systems

NIST SP 800-82: Guide to Industrial Control Systems Security

- Restricting logical access to the ICS network and network activity (use a network topology that has multiple layers of protection)

- Restricting physical access to the ICS network and devices (a combination of physical access controls should be used)

- Protecting individual ICS components from exploitation (this includes restricting ICS user privileges to only those that are required for each person's role)

- Maintaining functionality during adverse conditions (this involves designing the ICS so that each critical component has a redundant counterpart)

NIST NISTIR 7628 (2010) : Guidelines for Smart Grid Cyber Security

Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

Vol. 2, Privacy and the Smart Grid

Vol. 3, Supportive Analyses and References

US NERC-CIP Standards (2006)

The intent of the NERC-CIP Cyber Security Standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems.
The standard includes:

- **provisions for identifying critical cyber assets (section 002)**
- **developing security management controls (section 003)**
- **implementing training (section 004)**
- **identifying and implementing perimeter security (section 005)**
- **implementing a physical security program for the protection of critical cyber assets (section 006)**
- **protecting assets and information within the perimeter (section 007)**
- **conducting incident reporting and response planning (section 008)**
- **crafting and implementing recovery plans (section 009)**

NERC (2010) : Reliability considerations from the integration of Smart Grid

- Government initiatives and regulations promoting Smart Grid development and integration must consider bulk power reliability

- Integration of Smart Grid requires development of new tools and analysis techniques to support planning and operations

- Smart Grid technologies will change the character of the distribution system, and they must be incorporated into bulk power system planning and operations

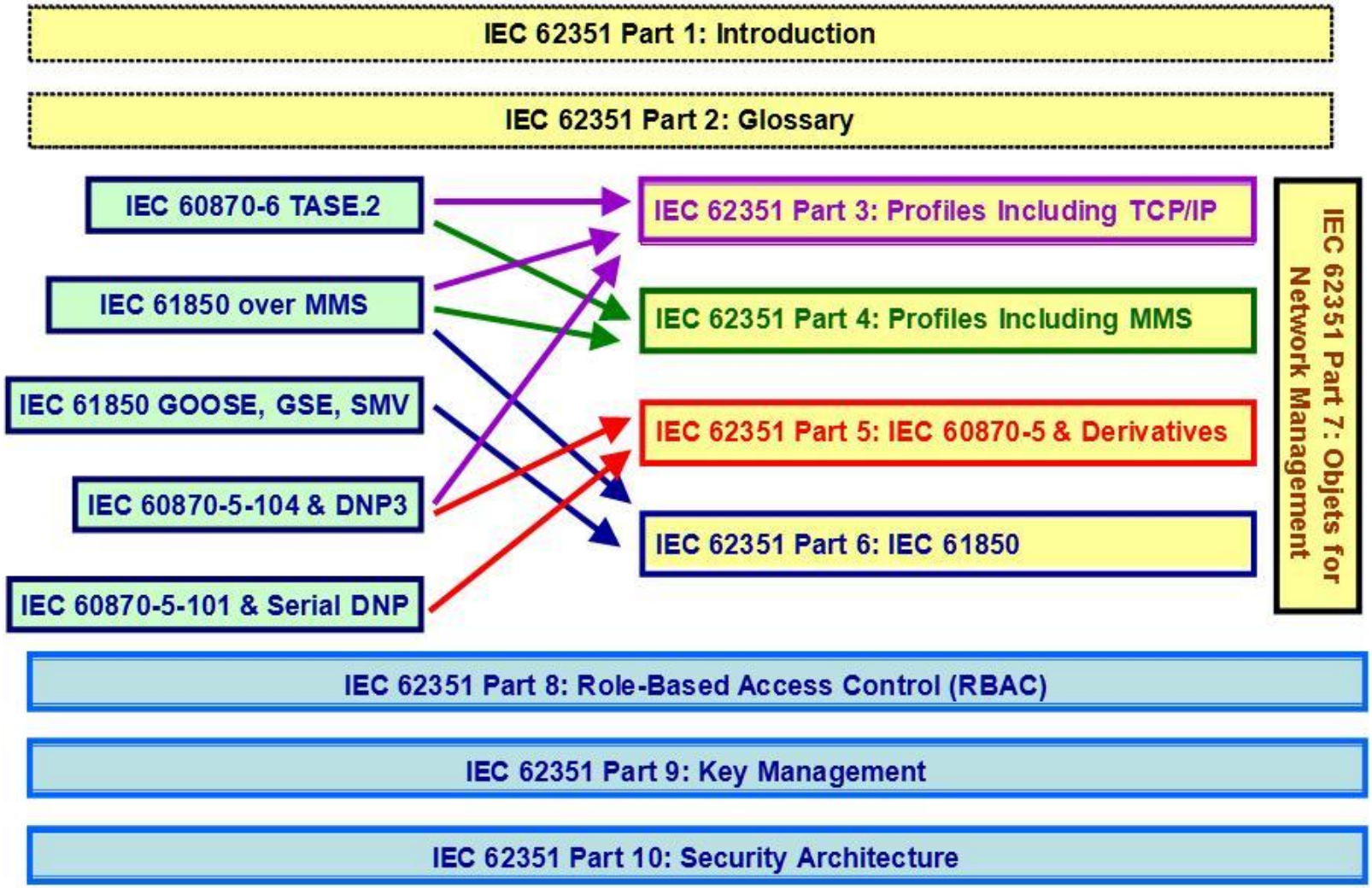
- Cyber security and control systems require enhancement to ensure reliability

- Research and development has a vital role in successful Smart Grid integration

IEC 62351 (2010) : POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY

The scope of the IEC 62351 series is information security for power system control operations. The primary objective is to "*Undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues.*"

Mapping of IEC 61850 and IEC 60870 to IEC 62351



Conclusions

- The situation is rather complex, with a proliferation of initiatives, standards, frameworks, that need to be aligned
- There is the need to promote the development of IACS/SCADA security certification scheme and creation of a network of test bed facilities (ERNCIP Project, ENISA)
- Smart Grid design and deployment must take into account the current cyber vulnerabilities in the IACS/SCADA Systems
- There must be a coordinated and ongoing effort to secure the Smart Grid that includes the full development lifecycle


Thank You!