VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Cybersecurity for Wireless Nuclear Applications

Wireless in Nuclear Applications Seminar, Energiforsk, Stockholm 08.03.2018

Reijo Savola, VTT

reijo.savola@vtt.fi

CONTENTS

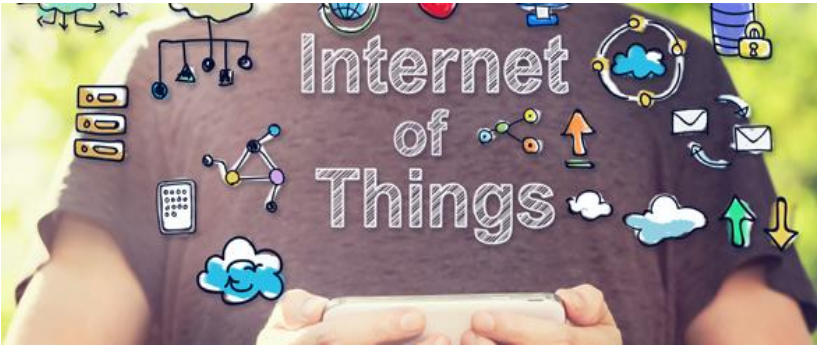
- Trends relevant to cybersecurity
- Cybersecurity considerations in nuclear power plants
- Wireless cybersecurity in nuclear applications
- Cybersecurity risk analysis and measurement
- Conclusions

TRENDS RELEVANT TO CYBERSECURITY

The key asset in the new connected society will be data

- 5G will increase the data volume available to users considerably, with lower latency
- IoT applications become more popular
- Big data analytics can be used
- More applications in the cloud

- The new services will certainly shape our society, but create also new dependency



At the same time, (1) need for <u>efficient and effective</u> cybersecurity solutions becomes more emphasized and the (2) threat landscape becomes more <u>dynamical</u>.

TRENDS RELEVANT TO CYBERSECURITY

- Malware will continue to evolve
- Complexity 5G, IoT, clouds, and their applications lead to security issues and further DDoS attacks
- Applying AI and machine learning to security

Pcworld.com

> Need for <u>efficient and effective</u> cybersecurity solutions becomes more emphasized

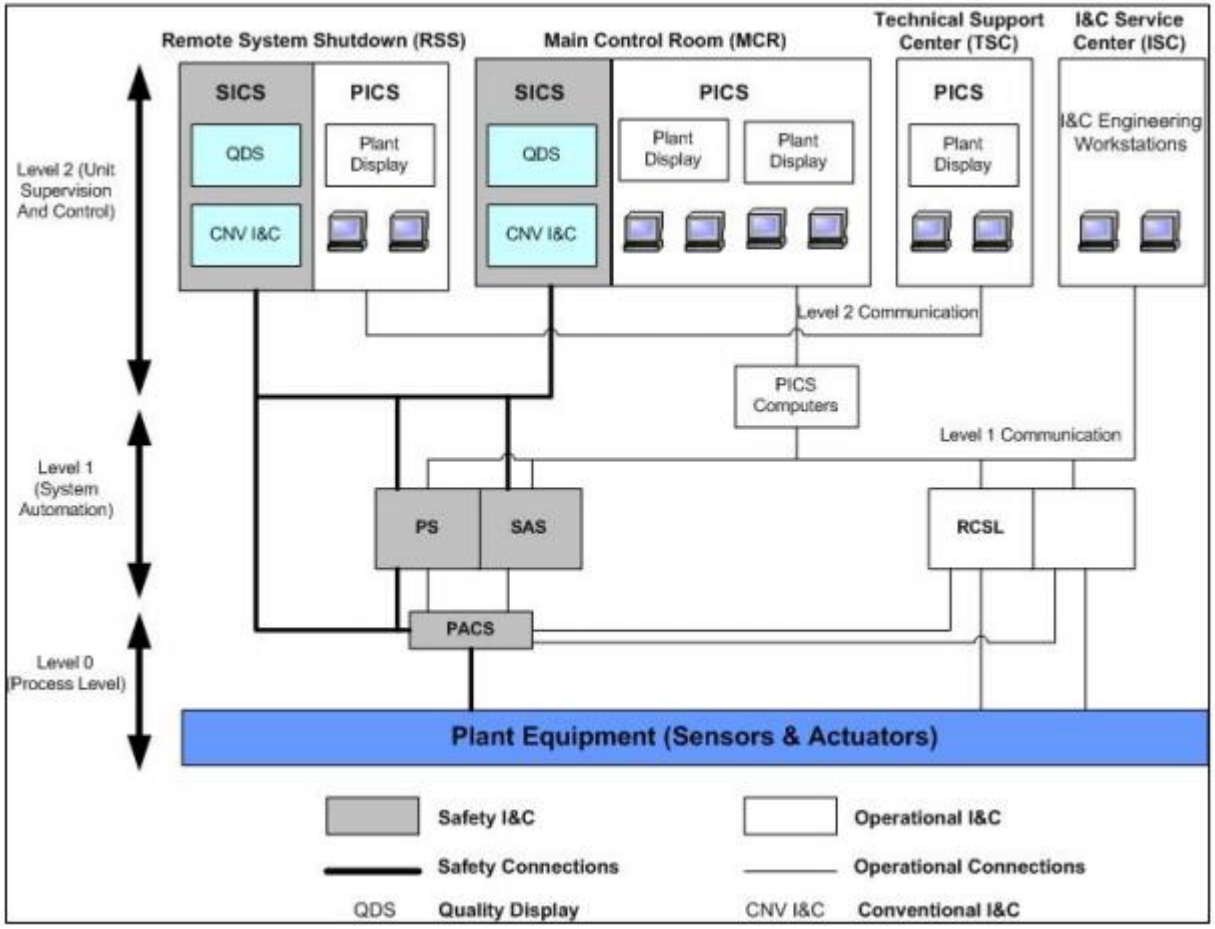
NUCLEAR POWER PLANT CYBERSECURITY CONSIDERATIONS

Architecture of NPP Instrumentation and Control Systems*:

Level 0: Process Interface Level: measurement and sensory capabilities

Level 1: System Automation Level: protection, safety automation, process automation, priority actuation and control, reactor control, surveillance and limitation

Level 2: Unit Supervision and Control Level: interactions between operators and the rest of the plant systems at L0 and L1.



*Korsah et al: Instrumentation and Controls and Nuclear Power Plants: An Emerging Technologies Update. US Nuclear Regulatory Commission, 10/2009.

NUCLEAR POWER PLANT CYBERSECURITY CONSIDERATIONS

The Main Cyber Risk Scenarios by IAEA*:

Cyber attack: corruption of C&C systems and removal of radiactive material. Often sophistication needed, with expertise in vulnerabilities, industrial control systems and malware design and implementation. Nation-states have the best resources for cyber attacks

Cyber sabotage: affects the normal operations of nuclear facility and causes serious damage to nuclear equipment. Sabotage can cause discruptions to equipment, or even nuclear explosion. Stuxnet is an example of cyber sabotage, which caused damage to Iranian centrifuges and SCADA control systems

Cyber espionage: Collection of confidential information from a nuclear facility and its usage for malicious purpose. More common than sabotage. Tools include key loggers and spyware.

*Dudenhoeffer: IAEA Information and Computer Security. Office of Nuclear Cyber Security Programme, International Atomic Energy Agency. May 21, 2013.

NUCLEAR POWER PLANT CYBERSECURITY CONSIDERATIONS

Vulnerability categories and associated threats in NPPs.*

Vulnerability Category	Attacks	Vulnerable Modules
No or Incorrect Input Validation	Buffer over flow; cross-site scripting; SQL injection; command injection.	Workstations at MCR, RSS; PICS; SICS; HMIs.
Improper Authorization	Data tampering; Escalation of privileges.	Workstations at MCR, RSS; PICS; SICS; HMIs, SAS, PS, PAS.
Improper Authentication	Network eavesdropping; Brute force attacks; Dictionary attacks; Credential theft; Cookie replay; Identity Spoofing.	All I&C systems, sub-systems and components
Unencrypted Sensitive Data	Data exposure; Data tampering; Network Eavesdropping; Credential theft; Man-in-the-Middle.	All I&C systems, sub-systems and components
Improper Software Configurations and Management	Access to default accounts; Exploit unpatched flaws, unprotected files and directories, etc.; Install Malware/Botnets	Workstations at MCR, RSS; PICS; SICS; HMIs, SAS, PS, PAS.
Lack of Backup Facilities	Interrupt plant operations; Shutdown plant; destroy plant equipment.	SAS, PS, PAS, Sensors, Actuators, PICS, SICS.
Lack of Audit and Accountability	Repudiation; No traces of network attack patterns; No traces of installation of malicious software.	All I&C systems, sub-systems and components

*Nelso, Trent and Chaffin: Common Cybersecurity Vulnerabilities in Industrial Control Systems. Department of Homeland Security, May 2011.

WIRELESS CYBERSECURITY IN NUCLEAR APPLICATIONS

Use of wireless technologies in NPPs (for sensors, for ICS)

Advantages

- Decreases measurably the cost of industrial wiring
- Provides an easy way to the installation of temporary instrumentation
- Enables more intelligent monitoring scenarios

Challenges include

- Electrically noisy environment in NPPs
- Security, privacy and reliability
- Electromagnetic compatibility

Historically, the nuclear industry has been slower than others implementing new technologies

WIRELESS CYBERSECURITY IN NUCLEAR APPLICATIONS

Computing.co.uk

Typical Vulnerabilities

Configuration problems

- Default configurations
- Poor configuration management
- Challenges of NPP environment to adequate configuration management

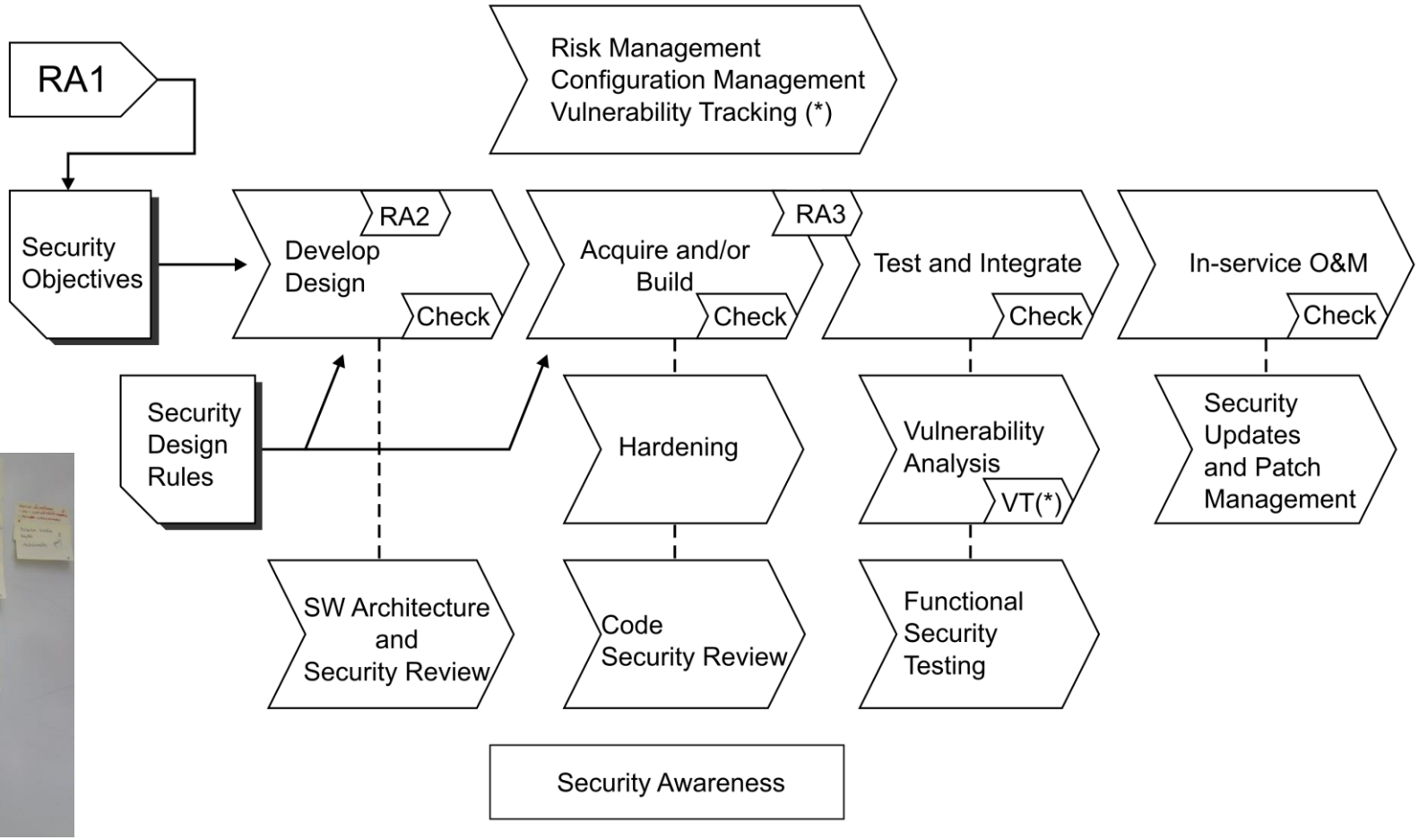
Rogue Access Points or Device Impersonation

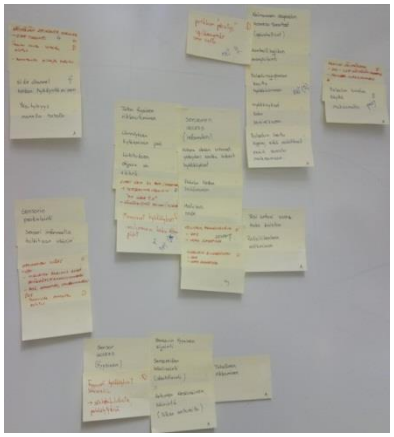
- Ilicitly placed within or on the edges of a WiFi network
- In general, it is also easy to convert a device so that it looks like another device

Encryption problems

- Widely used WPA2 protocol has also been broken

CYBERSECURITY RISK ANALYSIS AND MEASUREMENT





CYBERSECURITY RISK ANALYSIS AND MEASUREMENT

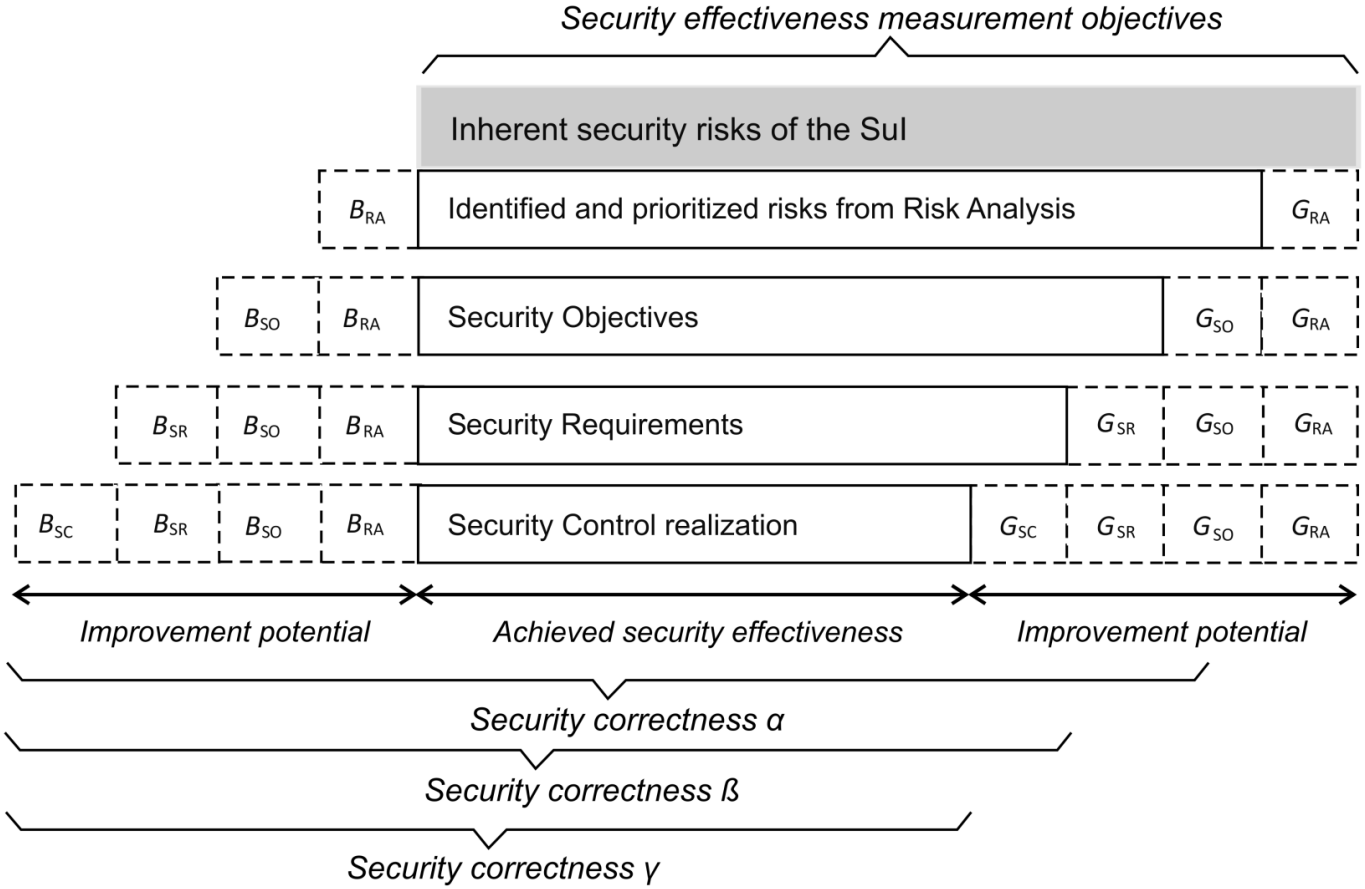
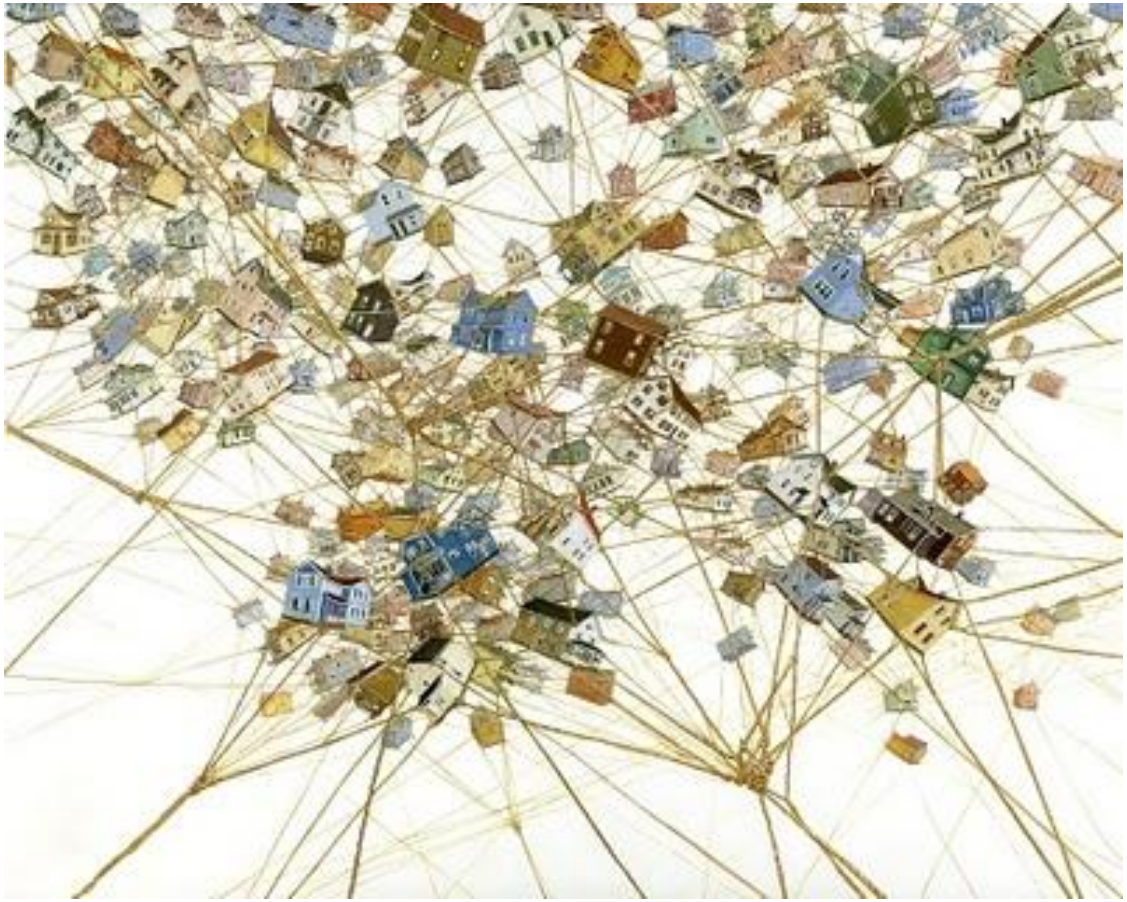


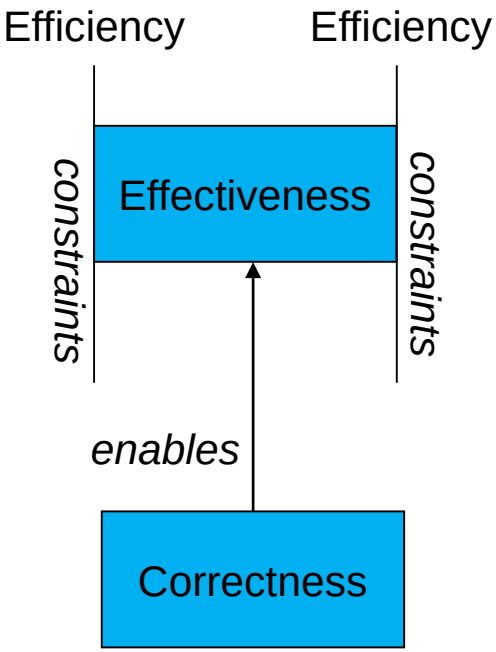
Figure: Savola, R., Frühwirth, C., Pietikäinen A., "Risk-driven security metrics in agile software development – an industrial pilot study". Journal of Universal Computer Science, 2012.

CYBERSECURITY RISK ANALYSIS AND MEASUREMENT

Cybersecurity risks often include a lot of interdependencies



CYBERSECURITY RISK ANALYSIS AND MEASUREMENT



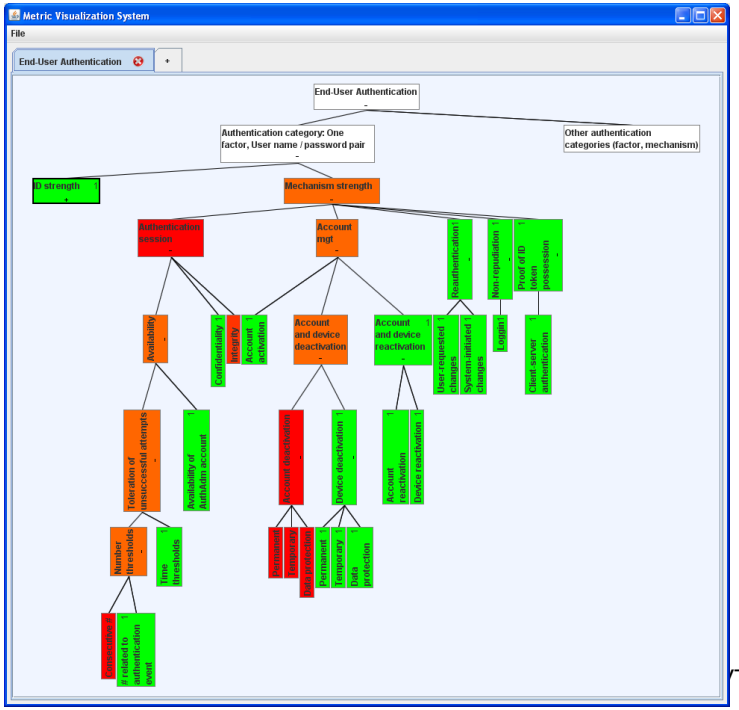
- **SECURITY CONTROL (SC)**
- **Security controls are means of managing privacy risk, which can be administrative, technical, management, or legal in nature** (based on ISO/IEC 27000's security control concept)
- **SECURITY CONTROL CORRECTNESS**
- **Security correctness denotes assurance that privacy controls have been rightly implemented in the SuI, and the system, its components, interfaces and the processed data meet privacy requirements.**
- **SECURITY CONTROL EFFECTIVENESS**
- **Security effectiveness denotes assurance that stated privacy objectives are met in the SuI and expectations for resiliency in the use environment are satisfied, while the SuI does not behave in any other way than what is intended.**
- **SECURITY CONTROL EFFICIENCY**
- **Security efficiency denotes assurance that the adequate privacy quality has been achieved in the SuI meeting resource, time and cost constraints.**

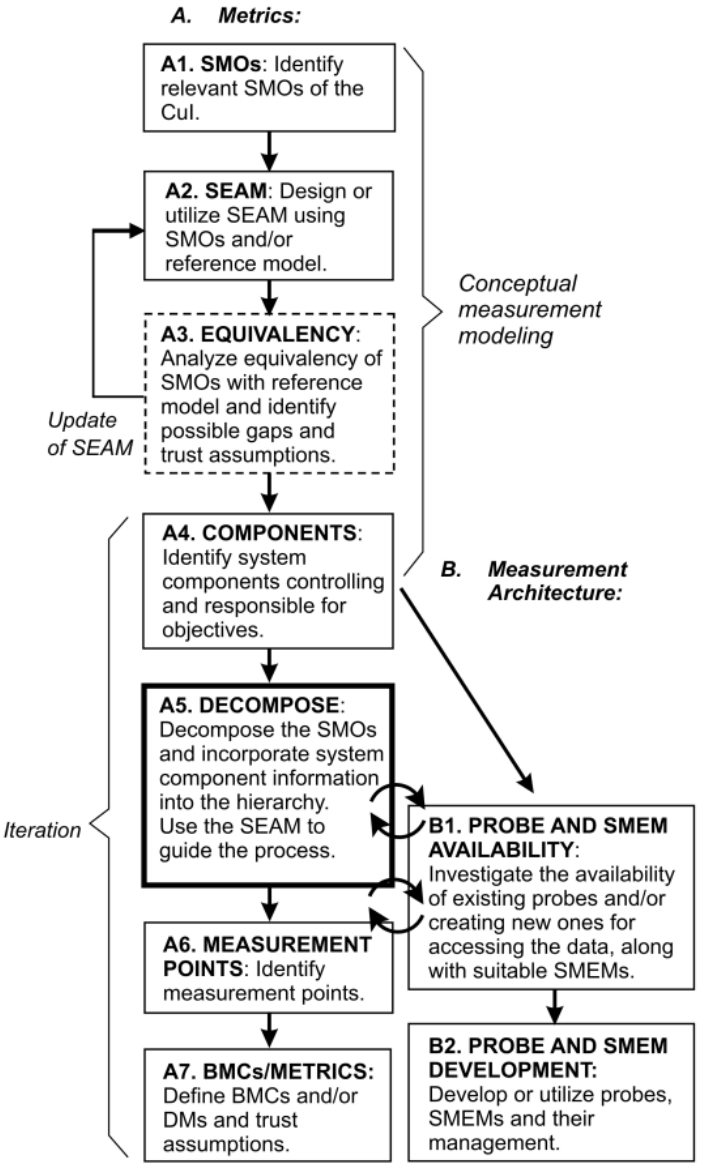
The main SOs and SCs should mitigate the top-ranked risks

CYBERSECURITY RISK ANALYSIS AND MEASUREMENT

- Security metrics development by security objective decomposition

- Management of metrics: hierarchical approach
- Visualisation needed





CYBERSECURITY RISK ANALYSIS AND MEASUREMENT

Systematic Security Assurance in Focus

WAR ROOM

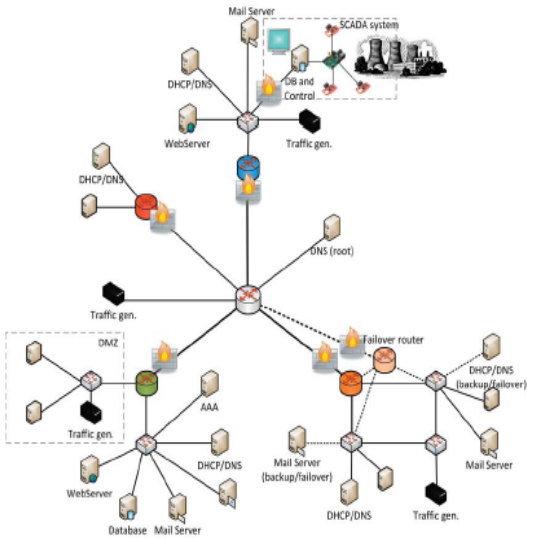
cybersecurity

WHAT IS WAR ROOM?

- Isolated, controlled, safe and secure environment
- Includes a personnel of more than 30 researchers, with extensive experience and knowhow on cyber security
- Equipped with cutting edge technologies & devices

WAR ROOM enables

- Simulation of cyber attacks, countermeasures and defence
- Identification of cyber attacks, threats and vulnerabilities
- Network traffic monitoring and analysis
- Simulating devices in artificially created contexts and conditions
- In-depth cyber analysis from log information
- Security testing of products and services
- SW security auditing
- Professional training/learning
- Enables the use of potentially harmful SW/HW in a controlled, safe and isolated environment



CONCLUSIONS

- Technological trends affecting to cybersecurity concerns include 5G, IoT, big data and use of cloud services. **They shape many services and applications**
- The typical vulnerabilities in wireless technologies include **configuration problems**, **rogue access points** and **encryption problems**
- Cybersecurity risk analysis is not yet developed as a widely understood activity. Iterative RA is needed, and metrics enable implementation of **effective and efficient risk-driven security controls**
- **Systematic security assurance** is needed

TECHNOLOGY FOR BUSINESS