



BME

Budapest University of Technology and Economics



KHJIT

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

Computer Security at Nuclear Facilities

Current Status, Trends and Practice in the field of
Computer Security in the (Nuclear) Industry

I&C System Specifics in Security

Uniqueness, Trends, and Basic Components

NPP I&C system Uniqueness

- Nuclear Control system (NPP) characteristics:
 - Multiple operation modes
 - Power operation
 - Start-up
 - Hot standby/shutdown
 - Cold standby/shutdown
 - Refueling
 - Periodic testing
 - Daily, weekly, monthly, quarterly, yearly
 - Overhaul maintenance
 - Technical Specifications
- Different security aspect comparing with IT environment
 - Striking differences still exist between I&C systems and standard IT systems that must be considered in any security activity.

Information Technologies (IT) vs. Industrial I&C Systems

Topic	IT	I&C systems
Availability	Delays accepted	24x7x365 for ever
Time critical content	Generally delays accepted	Critical
Technology Support Lifetime	2 to 3 years	20+ years
Security upgrades	Regular/scheduled	No common practice
Security awareness	Good in both private and public	Poor except for physical
Antivirus	Very common, easily deployed and updated	Uncommon, and can be difficult to deploy
Outsourcing	Common/widely used	Rare
Incident Response	Well defined and deployed	Uncommon
Security testing/audits	Scheduled and practiced	Not well established

I&C Systems Challenges

I&C Systems:

- Top priority is **reliability** and **availability**, not security
- Traditionally relied on isolation
- Trend: using commercially available hardware and software
- Equipment vendors **often have backdoor** VPN
- Use of default passwords

IT:

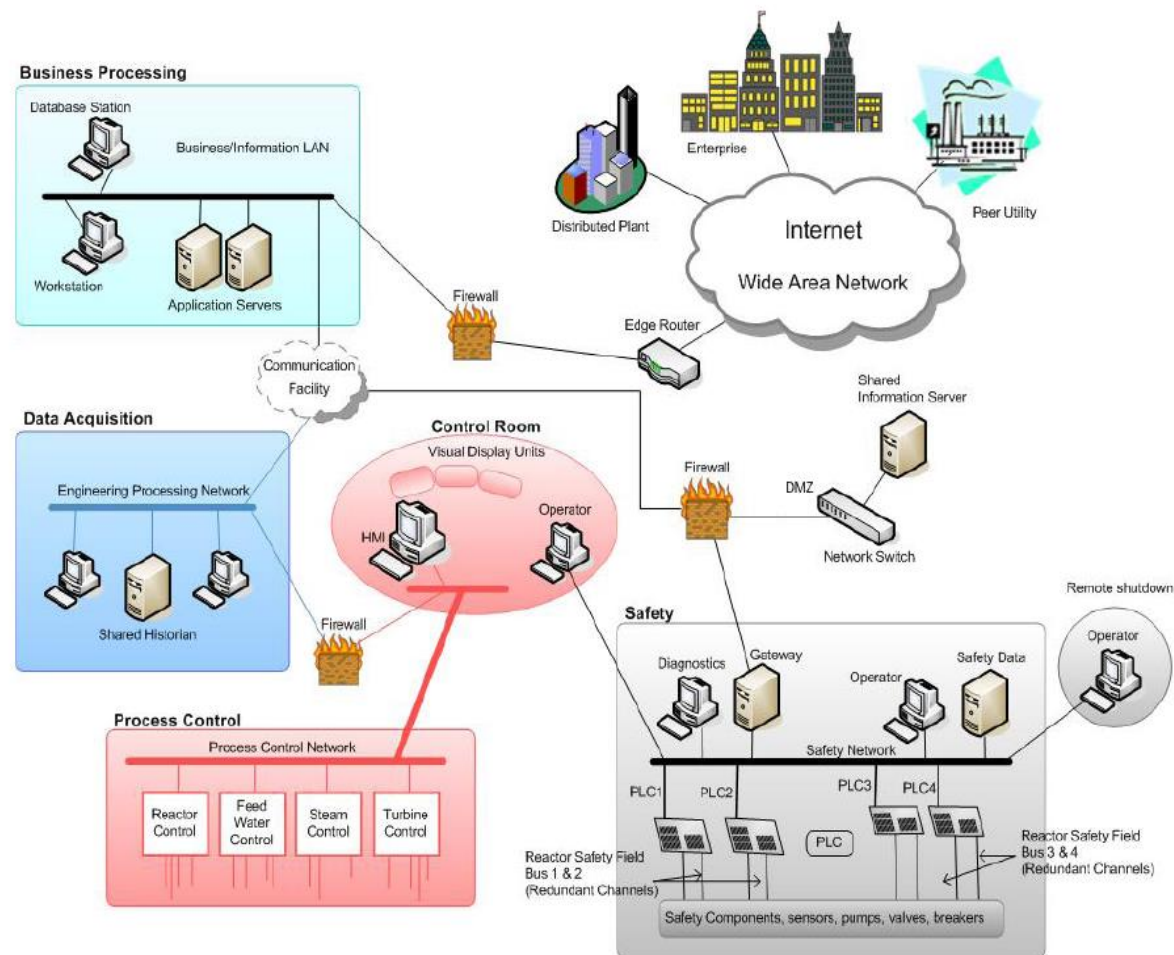
- Traditional security tools may not work for control systems
- IT people do not know control systems
- Enterprise networks are being connected to control systems
- **Control systems are overlooked** because they are not managed by IT

ICS System Trends

- Nearly all I&C is digital now
- Migration toward more non-proprietary systems
- Greater connectivity
- Remote access
- Complexity in control systems is significant and increasing
 - Impossible to test & evaluate all potential application environments
 - Testing of very large, fully integrated systems is extremely difficult

I&C Systems Connectivity

Many connections and access pathways, which must be managed



Hypothetical depiction of the interconnectivity between computing systems at a nuclear power plant.

Synergy of Safety and Security

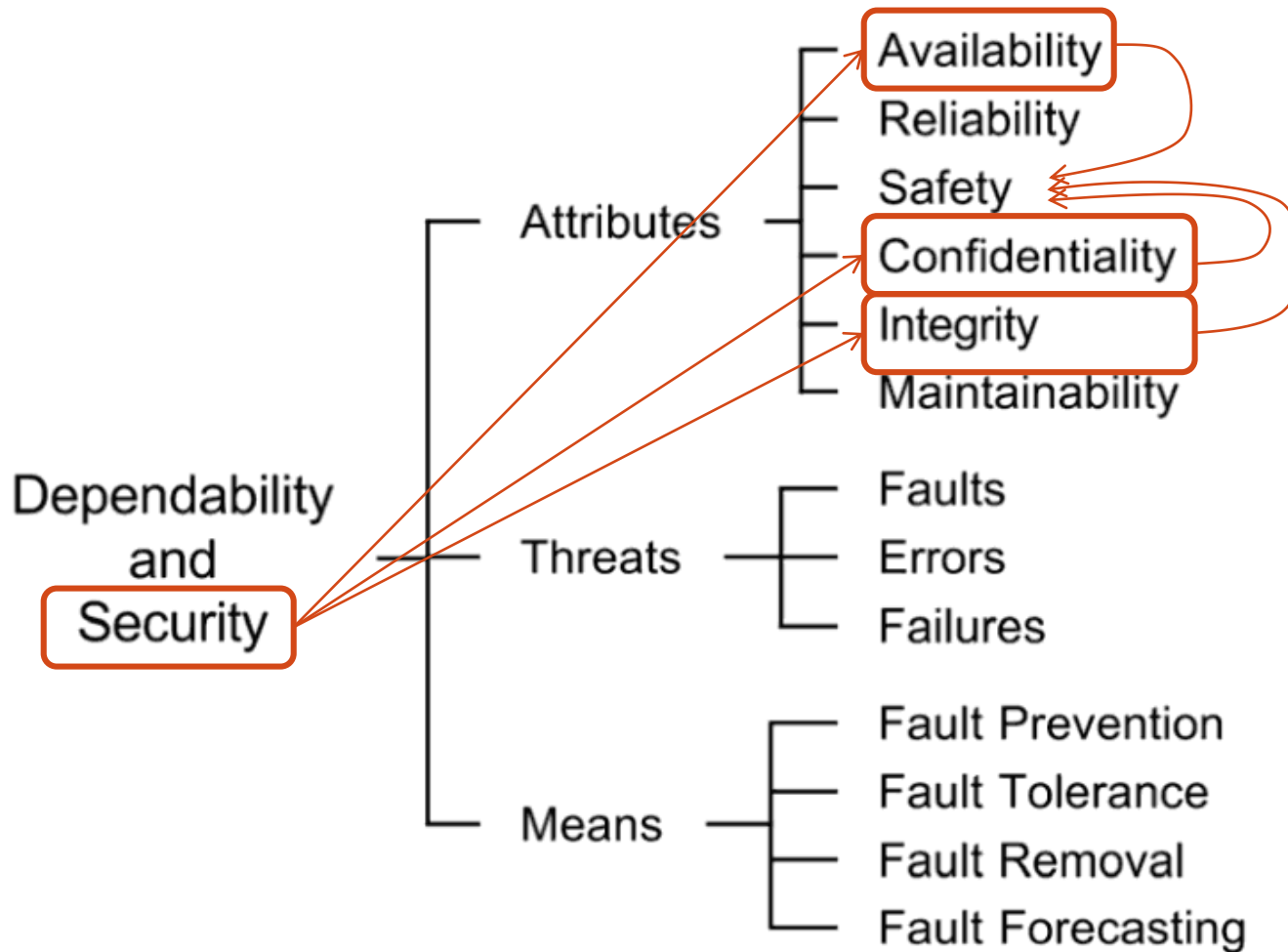
Reference:

Computer Security of Instrumentation And Control Systems At Nuclear Facilities, DRAFT Technical Guidance / Implementing Guide, 2014.

Terminology

- Programmed electronic systems
 - The computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility
- Computer security
 - Security of all programmed electronic systems and all interconnected systems and networks
 - Information security and cyber security are considered synonyms of computer security

Safety relies on Security



What do we need to protect?



- Information Security

- **Confidentiality**: ensuring information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**: ensuring that information including data and executable software held in a system is a proper representation of the information intended and that it has not been modified, created, or deleted by an unauthorized person, entity, or process
- **Availability**: requirement intended to assure that systems work promptly and service is not denied to authorized users

- As well as **Physical Security**

Theoretical basis

NSC (118/2011.), FP (190/2011.)

- HAEA PP-18: Protection requirements for computer systems

IAEA documents

- Nuclear Safety Standards
- Nuclear Security Series
 - IAEA NSS-17 (2011), Computer Security at Nuclear Facilities
 - IAEA NST036: Computer Security of Instrumentation and Control Systems at Nuclear Facilities, DRAFT, 2014.

ISO / IEC / ISA standards

- ISO 27001, ISO 17799
- IEC 61513, IEC 61226
- IEC 60987, IEC 60880, IEC 62138, IEC 61500

ISA standards

- ISA 62443

NERC CIP standards

- CIP-002-3 ... CIP-009-3

NIST standards

- FIPS 199, FIPS 200, SP 800-53
- SP 800-18, SP 800-30
SP 800-60, SP 800-82

NRC regulations

- 10 CFR 73.54, RG 5.71

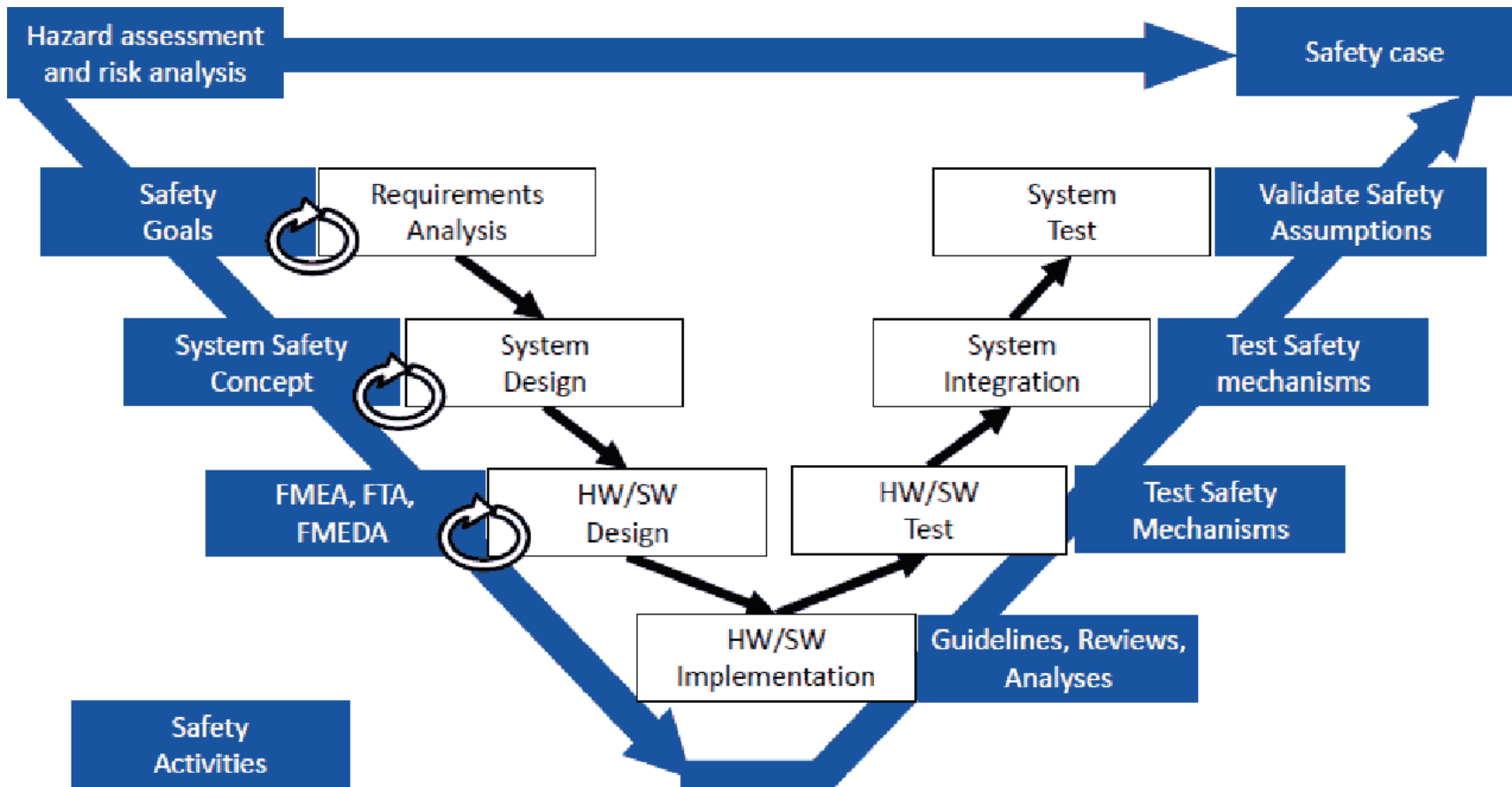
Other

- COBIT 4.1, ITILv3, OCTAVE Allegro

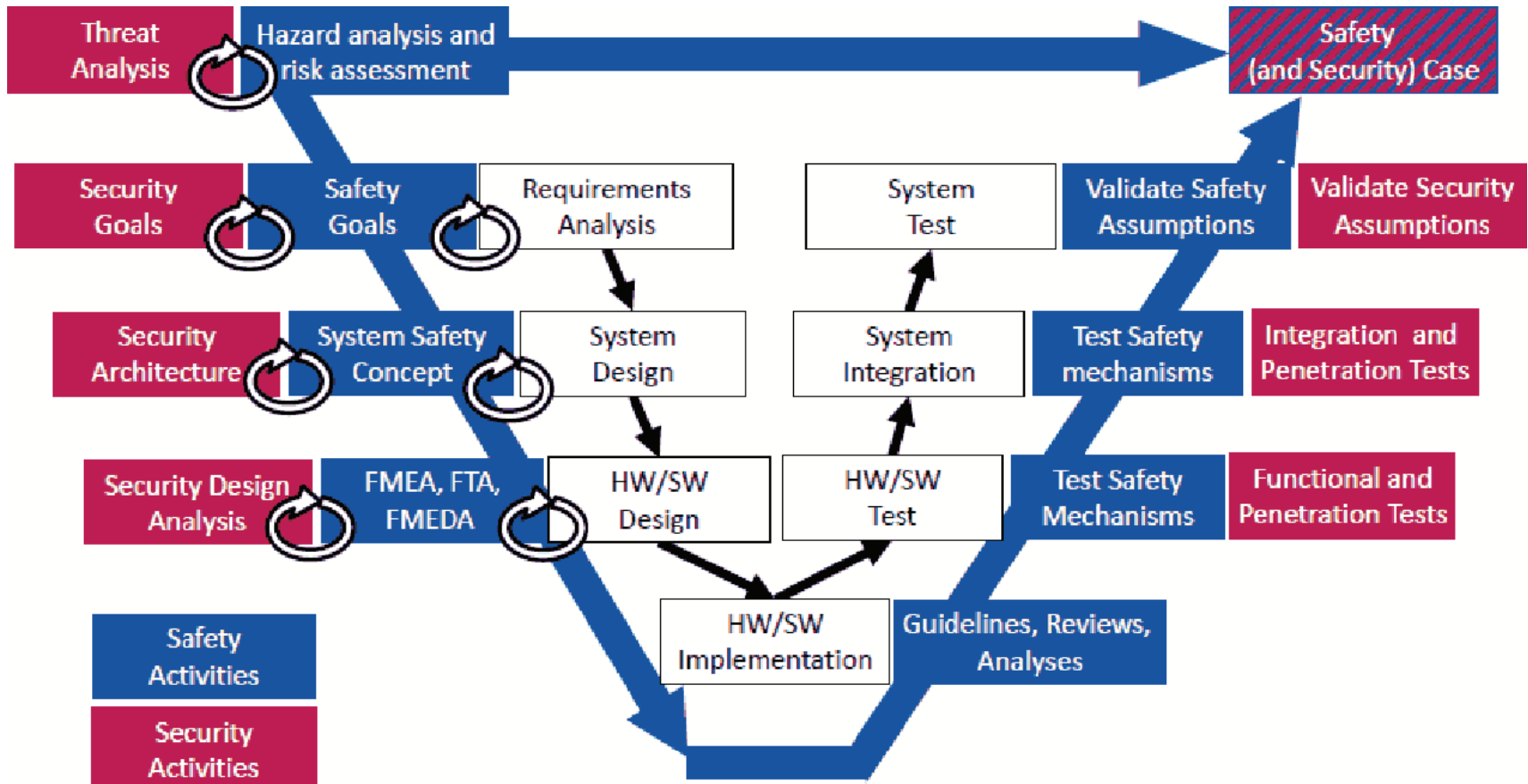
Safety — Security

- Security measures and safety measures are implemented in an integrated manner
- Security measures should not compromise safety and safety measures should not compromise security
- Malicious actions may affect a single I&C system or multiple I&C systems
- Malicious acts might bypass multiple levels of safety defense in depth

Design for Safety Life-Cycle



Safety + Security Integrated Life-Cycle



Safety — Security

- A cyber-attack can cause an initiating event and/or can undermine the performance of a safety function
- Cyber-attacks may potentially cause safety, safety related, and non-safety systems to operate in ways that compromise facility safety
- In some cases cyber-attacks might place the facility in conditions that are not considered by the safety analysis
- A computer attack on the I&C system, its development computers, or its maintenance computers may result in the attacker gathering data that will facilitate a future attack or theft of nuclear material
- Many of design principles applied in practice are effective for both safety and security goals

I&C Security Principles (for safety-security in the draft of IAEA I&C security guide)

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

IAEA NST036: Computer Security of Instrumentation and Control Systems at Nuclear Facilities, DRAFT Technical Guidance / Implementing Guide, April 2014:

1. Principle: The safety hazard posed by computer attacks on I&C systems should be analyzed and documented.
2. Principle: The security controls assigned to an I&C system, subsystem or component should be commensurate with their level of importance.
3. Principle: Computer security controls should be implemented in such a way as to not to adversely impact the required safety functions and performance of the I&C System.

I&C Security Principles

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

1. Principle: The safety hazard posed by cyber-attacks on I&C systems should be analyzed and documented.
2. Principle: The security controls assigned to an I&C system, subsystem or component should be commensurate with their level of importance.
3. Principle: Computer security controls should be implemented in such a way as to not to adversely impact the required safety functions and performance of the I&C System.
4. Principle: The computer security policy for nuclear facilities should include considerations unique to I&C systems.
5. Principle: Each organization that has responsibility for implementing I&C system life cycle activities should have an integrated or separate computer security plan.
6. Principle: A secure environment should be provided for I&C hardware and software development.
7. Principle: Contingency plans and procedures to recover from a potential computer security incident should be prepared and periodically exercised.
8. Principle: Computer security principles and controls should be applied by vendors including support provided on site, at the vendor's workplace, and during any such transit or storage of purchased goods.
9. Principle: Individuals who have physical and/or logical access to digital I&C systems should be trained to support computer security tasks and recognize potential computer security events.
10. Principle: Life cycle activities should be conducted within the framework of a nuclear quality assurance plan.

I&C Security Principles

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

11. Principle: Computer security reviews and audits of I&C systems and computer security activities should be performed on a regular basis to verify compliance with regulations, computer security policy and good practices for I&C system security.
12. Principle: Computer security controls should be managed within the I&C system's configuration management process.
13. Principle: Verification and validation should demonstrate that the I&C system meets the specified system security requirements.
14. Principle: Security assessments should be performed to identify potential security vulnerabilities in each phase of the I&C life cycle.
15. Principle: Documentation should be generated to retain sufficient information of computer security of I&C systems to demonstrate that security controls are designed, implemented and maintained to meet the required levels of importance.
16. Principle: The design basis for the overall I&C architecture and each I&C system should identify the security controls to be implemented.
17. Principle: Physical and logical access to I&C systems should be controlled, logged, and verified such that only authorized personnel have access to or can make changes to the existing configuration, software and hardware.
18. Principle: Security controls should protect confidentiality of information associated with the design, manufacturing, installation, and operations of I&C and associated equipment.
19. Principle: Design basis should specify requirements for monitoring of and indicating the status of the digital system security controls to facilitate the taking of any necessary safety and security actions.
20. Principle: The facility I&C systems should have an overall computer security defensive architecture.

I&C Security Principles

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

21. Principle: I&C systems and related digital components should be designed and operated such that defence in depth against cyber compromise is achieved by the provision of multiple layers of protection.
22. Principle: The security requirements of the overall I&C, individual I&C systems, and I&C components should be established and documented.
23. Principle: Pre-developed components or software should be selected and configured using a security qualification process commensurate with the level of importance of the I&C system.
24. Principle: In the design and implementation phase of the I&C system life cycle, security requirements should be designed and implemented.
25. Principle: During the system integration phase, the integrated security features should be in place and configured as per specification prior to testing.
26. Principle: System validation should confirm the effectiveness of the security controls and check for potential impacts, direct or indirect, on safety functions.
27. Principle: During installation and commissioning, the operator should perform an acceptance review of the correctness of the physical and logical system security features in the target environment.
28. Principle: Computer security controls should be applied to operations and maintenance activities to ensure components and systems are not compromised.
29. Principle: Modifications of an I&C system should include an assessment of the security of the system.
30. Principle: Modifications to I&C systems should be treated as development processes and should be verified and validated.
31. Principle: Controls should be in place to ensure remnant data on discarded components cannot be used to support the development of a computer exploit.

I&C Systems Incidents

Successful Attacks against Industrial I&C Systems

I&C System Possible Incidents

Control systems operation may/might be disrupted by:

1. Delaying or blocking the flow of information through control networks → denying availability of the networks to control system operators
2. Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers → damage to equipment, or shutdown of process
3. False information sent to control system operators → inappropriate actions
4. Malicious software (e.g., virus, worm, Trojan horse) introduced into the system → damage to equipment, employees, ...

I&C — Physical Destruction Possible



A 2007 test conducted by the U.S. government demonstrates the destruction that might be caused by hackers seizing control of a crucial part of the electrical grid.

A large diesel generator spins out of control until it is physically destroyed and power generation is lost. Operational commands were quietly conducted by simulated hackers.

Source: <http://www.youtube.com/watch?v=fJyWngDco3g>

Why is Computer Security important? RISI 2009

- Repository for Industrial Security Incidents
 - collection of industrial computer security incidents
 - compiled by an independent industrial organization
 - it has a large number of member companies all over the world
 - issues quarterly reports based on voluntary but validated data supply and independent audits
- Trends, tendencies
 - the number of security incidents has an **increasing trend**
 - a **sharp increase is expected** in the next years
 - the number of software-based attacks **has doubled during one year**
 - the number of physical attacks is decreasing

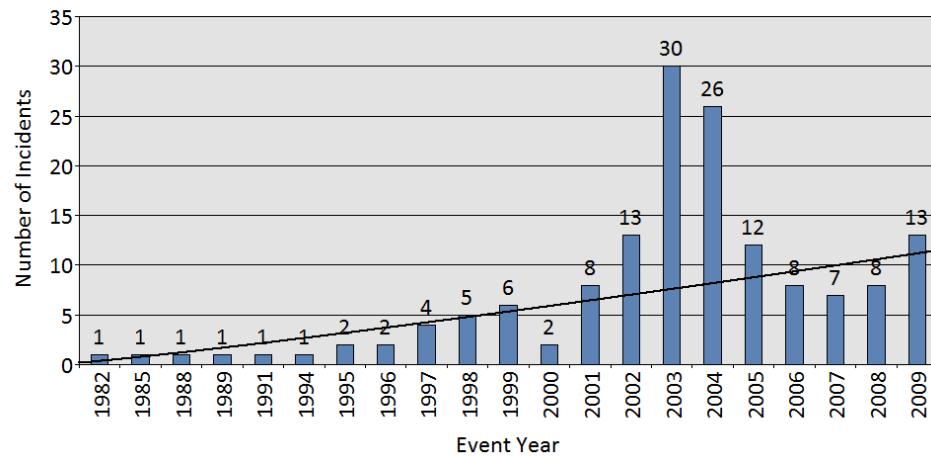
The RISI 2009 report — Trends, tendencies

Budapest University of Technology and Economics

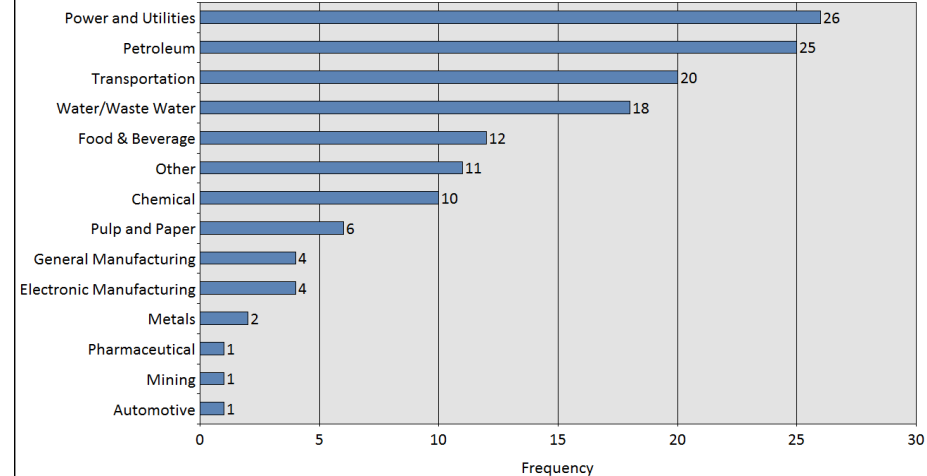
Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

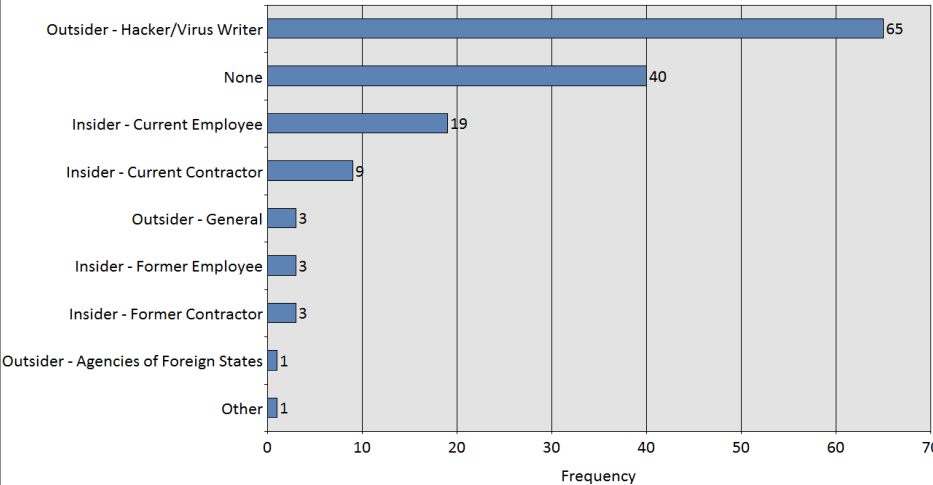
Incidents by Year



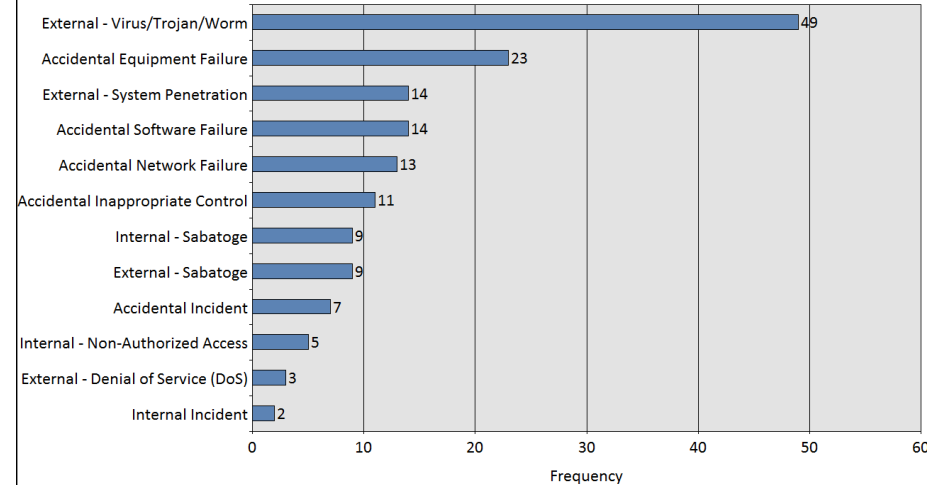
Industry Type (Global)



Perpetrator Type (Global)



Incident Type (Global)



The RISI 2009 report — Conclusions

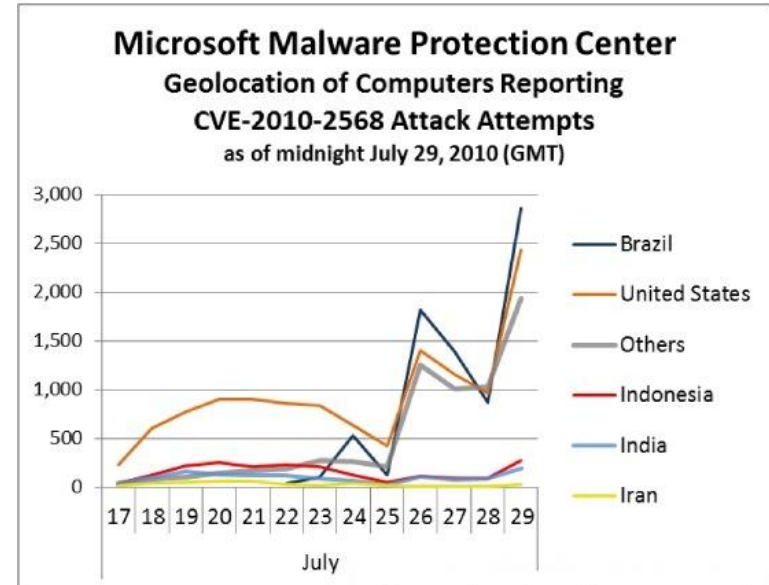
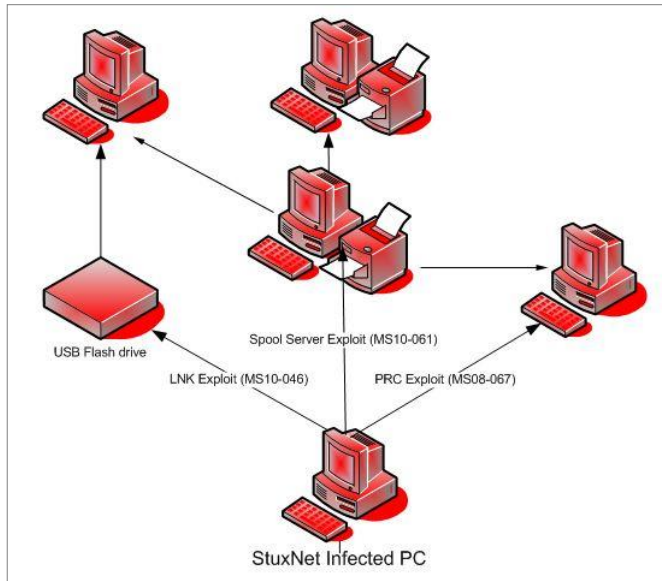
- The most dominant sources of attacks were
 - External attacks by **remote access via computer networks (42%)**
 - Internal software sabotage or failure (28%)
- The most popular target devices of attacks were
 - **Automation (PLC) and control (DCS) systems (31%)**
 - SCADA master systems, industrial computers (19%)
- The industrial sectors most affected by attacks were
 - **The energy industry (18%)** and the oil industry (17%)
- The damage caused by the attacks was **significant**
- The direct financial loss was
 - more than **1 million \$ in 19% of the cases**
- The downtime due to outage caused by the attack was
 - more than 1 hour in 51%, **more than 24 hours in 14% of the cases**

Stuxnet worm (CVE-2010-2568)

Budapest University of Technology and Economics

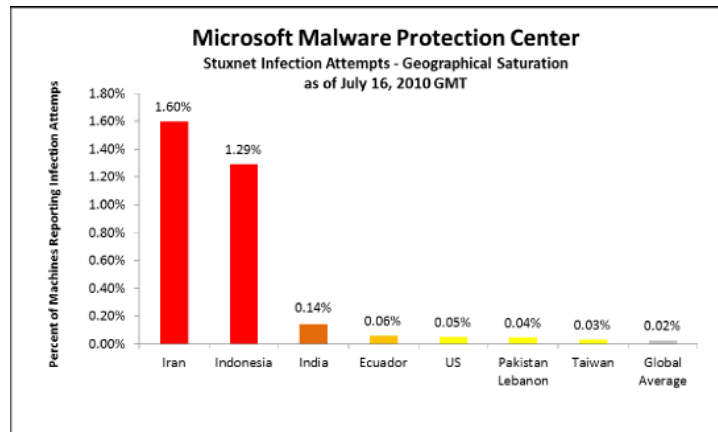
Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems



SIEMENS

F-Secure



Symantec

eset

I&C Systems – Incidents

Stuxnet worm hit industrial systems

“...the worm eats away at a very specific kind of industrial control system: a configuration of the Siemens-manufactured Supervisory Control and Data Acquisition (SCADA) system that commands the centrifuges enriching uranium for Iran’s nuclear program, the key step for an Iranian bomb...”

Iran's president, Mahmoud Ahmadinejad, confirmed on Monday night that a computer worm (Stuxnet), affected centrifuges in the country's uranium enrichment programme.

Telegraph – Nov, 29th 2010



I&C Systems – Incidents (Spanair Flight 5022)

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

Event: Central computer infected with malware. (8/20/2008)

Impact: Computer failed to detect 3 technical problems, potentially preventing takeoff.

Specifics: Plane crashed just after takeoff. Flaps and slats were retracted.



Killed 154, leaving 18 survivors

Virus: Trojan Horse

- Lessons learned:
- Virus check all external storage devices
- Monitor all Virtual Private Network connections



Ref: http://www.msnbc.msn.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.UH6uNW-39Bk

I&C Systems Threats

Trends and Tendencies that Increase the Vulnerability of
Industrial I&C Systems

I&C Systems – Threats 2005

- SCADA hackers declare themselves (SCADA hacks becoming more common topics at conferences)
- Direct evidence of attackers on a control network knowing what they had hacked into
- Direct evidence of attackers interacting with a controller using its native control protocols
- Vendor software is for sale on the black market¹
- Black Hat communities offering SCADA defense strategies for protecting critical infrastructure²
- Cyber tools:
 - Proliferating
 - More capabilities
 - Easier to use – anyone can download an exploit

1. Niceware, August 12, 2007, *Re: How to BoostUp Tomcat's Performance*, http://www.theserverside.com/discussions/thread.tss?thread_id=43664, web page visited March 6, 2008.

2. Black Hat, 2008, *SCADA Defense: Protecting Critical Infrastructure*, <https://www.blackhat.com/html/bh-dc-08/train-bh-dc-08-ioa-sd.html>, web page visited February 27, 2008.

I&C Systems – Adversary Opportunities

Re: Terrorists hacking power systems [was RE: Genset from AT&T site

[Topic List](#) < [Prev Topic](#) | [Next Topic](#) >

[Reply](#) | [Forward](#)

< [Prev Message](#)

Hello All:
I need to weigh in here. Address a couple points, sorry this is not so much comms related.
Somehow I missed "the" video, could someone point me to it.
-I am a Chief Powerplant Operator at a mainstem Columbia River dam, in the northwest.
I have worked in hydro powerplants, and high voltage switchyards for 27 years.

Sat Mar 1, 2008 6:40 pm

[▶ Show Message Info](#)

- As far as comms go, I do know our "computer engineers" both for the security system, and the plant control system, and power system control computers, can get in from home, over the public network, and that access is "deeper" than my access running the plant. Not sure of the security but, there is also a modem that can be called over a public phone line, so the manufacturer can get in if needed. I feel we are lacking on security, and it would be easy to get in if you wanted to.

Online blog discussing ICS vulnerabilities

-Plant physical security is better than before 9-11, but it is still horrible, you can "tag in" or follow someone in through a security gate, and we have so many contractors working on site, that anyone could walk in or out, and no one would notice, how could we?

Yahoo Groups, February 2008.

I&C Systems – Adversary Opportunities

- Remote login – no borders
- Physical security weaknesses – field devices
- Open source – Example - Military base administration area development plan posted
 - Heating and cooling plant upgrades
 - Electrical service details
- Outside (Internet) facing control systems
- Proliferation of wireless communications
 - World wireless market is expected to grow exponentially
- Outdated software (no patching)
- Implicit trust for all who communicate
- Increasing industrial control system protocols that are IP based
 - More protocols, more vulnerabilities

I&C Systems – Emerging Threats

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

- Mobile computing
 - Outage management
 - Work orders – Maintenance
 - BYOD – Bring Your Own Device – tough to manage
 - Smartphones
 - Tablets
- Blended attacks – cyber/physical
- Increased social media opportunities
 - Increased wireless - reduced cable installation costs
- Increase of zero day malware – immune to anti-virus

I&C Systems – Emerging Threats

- Addition of other networks (Law Enforcement) to the ICS network
- Web servers built into control devices – multiple vulnerabilities
- Supply chain interdiction
- Embedded (firmware) malware
- GPS manipulation (spoofing of GPS signals, ICS use GPS for position and timing signals)
- Cloud computing – storage of non critical information
- Accepting operations on a compromised (non-safety) system (inability to remove all malware from a system)

I&C Systems Vulnerabilities

Potential Weaknesses and Specific Features of I&C Systems
that Attackers Can Use

I&C Systems General Vulnerabilities

- Default vendor accounts and passwords still in use
 - Some systems unable to be changed (proprietary, physically unable to modify)
- Guest accounts still available
- Unused software and services still on systems
- No security-level agreement with peer sites or vendors
- Poor patch management (or patch programs)
- Extensive auto-logon capability

I&C Systems General Vulnerabilities

- Typical IT protections not widely used (firewalls, IDS, etc.)
- Little emphasis on reviewing security logs (Change management)
- Control system use of enterprise services (DNS, etc.)
- Shared passwords
- Writeable shares between hosts
 - User permissions allow for admin level access
- Direct VPN from offsite to control systems

Policy and Procedure Vulnerabilities

Vulnerabilities	Description
Inadequate security policy for the ICS	Vulnerabilities are often introduced into ICS due to inadequate policies or the lack of policies specifically for control system security.
No formal ICS security training and awareness program	A documented formal security training and awareness program is designed to keep staff up to date on organizational security policies and procedures as well as industry cyber security standards and recommended practices. Without training on specific ICS policies and procedures, staff cannot be expected to maintain a secure ICS environment.
Inadequate security architecture and design	Control engineers have historically had minimal training in security and until relatively recently vendors have not included security features in their products
No specific or documented security procedures from the security policy for the ICS	Specific security procedures should be developed and employees trained for the ICS. They are the roots of a sound security program.
Absent or deficient ICS equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an ICS malfunction.

I&C Systems Challenges

- No authentication – all devices are trusted, unauthorized personnel have physical access to equipment
- Low processing power – not designed for additional anti-virus software
- Clear text protocols – no encryption
- Minimal or no logging capability
- Difficult to physically secure
- Patches from vendor come very slowly, are not immediately installed (need lots of site testing)
- Any network scan can upset the stability of the system (i.e. security scan may affect timing)

I&C Systems Computer Security Implementation

Current Practice for Implementing a Computer Security Policy
and Protection System in a Nuclear Plant

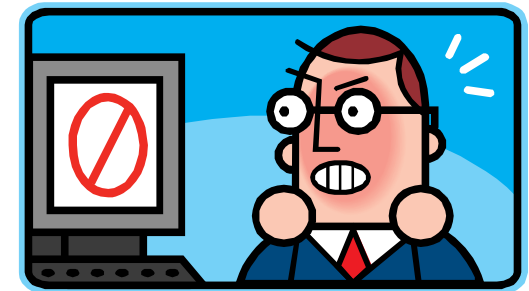
Basic considerations

- Current international standards and guidelines concentrate on information security
 - Many of these consider **information security as the starting point**, and try to apply these requirements **in the nuclear environment**
 - The requirements need to be applied innovatively
 - Well-defined **attack profiles, DBT and risk assessment** are vital
- Concepts taken from safety standards
 - A security classification is necessary
 - Based on the safety and security importance, relevance
 - A graded approach is required
 - Security controls need to be selected based on the risk
 - The defense in depth strategy must be applied

Goals — 10 CFR 73.54

- The licensee shall protect digital computer and communication systems/networks associated with:
 - Safety-related and important-to safety functions
 - Security functions
 - Emergency preparedness (EP) functions
 - Support systems and equipment which, if compromised, would adversely impact safety, security, or EP (SSEP) functions
- The licensee shall protect SSEP systems and networks from cyber attacks that would:
 - Adversely impact the **integrity** or **confidentiality** of data and/or software
 - Deny **access** to systems, services, and/or data
 - Adversely impact the **operation** of systems, networks, and associated equipment

Security
classification
instead!



Implementation — 10 CFR 73.54

- The licensee shall:
 - **Analyze** digital computer and communication systems and networks and **identify those assets** that must be protected against cyber attacks. These are called **critical digital assets**.
 - Establish, implement, and maintain a **cyber security program** for the protection of the critical digital assets
 - Incorporate the cyber security program as a component of the **physical protection program**.

Implementation of computer security

- **Computer security assessment** of I&C systems
 - Threat Analysis, Design Basis Threat
 - Vulnerability Assessment
 - Risk Assessment, Risk Analysis
- Development and introduction of a **Computer Security Management System**
- Implementation and maintenance of a complex **Computer Security Protection System**
 - Selection of the appropriate computer security controls
 - Extension of the existing physical controls



Computer security assessment of I&C systems

1. Assets analysis and management

- Perimeter and context definition
- Assets identification and inventory of relevant assets

2. Threat analysis, Design Basis Threat

- Attack scenarios, attacker profiles
- Analysis and evaluation of threats to relevant assets

3. Vulnerability analysis

- Technical assessment (e.g. penetration testing)
- Analysis and evaluation of vulnerabilities of relevant assets

4. Risk assessment

- Consolidation of the threat and vulnerability analysis results
- Analysis and evaluation of risks

5. Security classification of systems

- Establishment of security zones





















CSMS

Risk based design of computer security

- Based on the „Computer Security at Nuclear Facilities”
- Risk based design
 - Safety: Risk = Consequence (Impact) × Probability (Frequency)
 - Security: Risk ← Consequence (Impact) × Vulnerability
 - Vulnerability: an exploitable capability or an exploitable weakness that could be expected to result in a successful attack causing damage to the asset
- Countermeasures (Controls) are selected based on the risk

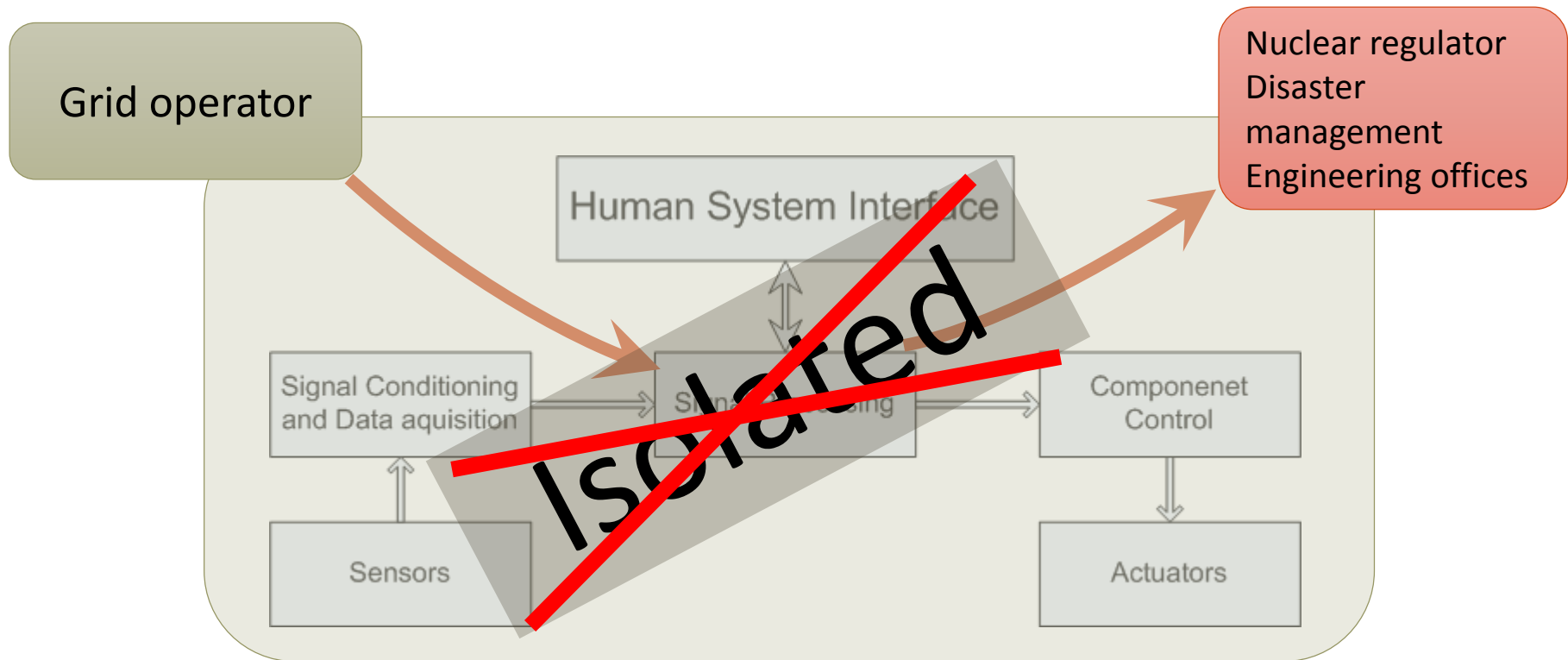
SYSTEM	IMPACTS ON COMPUTER SECURITY	POTENTIAL IMPACTS ON FACILITY	SUGGESTED COUNTER MEASURES	VULNERABILITIES
Reactor protection system	Loss of integrity of safety critical software/data. Loss of function availability.	CRITICAL Plant safety compromised, radiological release.	Security Level 1 measures	
Process control system	Loss of integrity of control software/data. Loss of function availability.	HIGH Plant operation compromised.	Security Level 2 measures	

Selection of Security Controls

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical 
AT	Awareness and Training	Operational 
AU	Audit and Accountability	Technical 
CA	Security Assessment and Authorization	Management 
CM	Configuration Management	Operational 
CP	Contingency Planning	Operational 
IA	Identification and Authentication	Technical 
IR	Incident Response	Operational 
MA	Maintenance	Operational 
MP	Media Protection	Operational 
PE	Physical and Environmental Protection	Operational 
PL	Planning	Management 
PS	Personnel Security	Operational 
RA	Risk Assessment	Management 
SA	System and Services Acquisition	Management 
SC	System and Communications Protection	Technical 
SI	System and Information Integrity	Operational 
PM	Program Management	Management 

Based on RG-5.71: Implement a comprehensive set of security controls based on a guidance document like the NIST SP 800-53

I&C Systems — Vulnerabilities

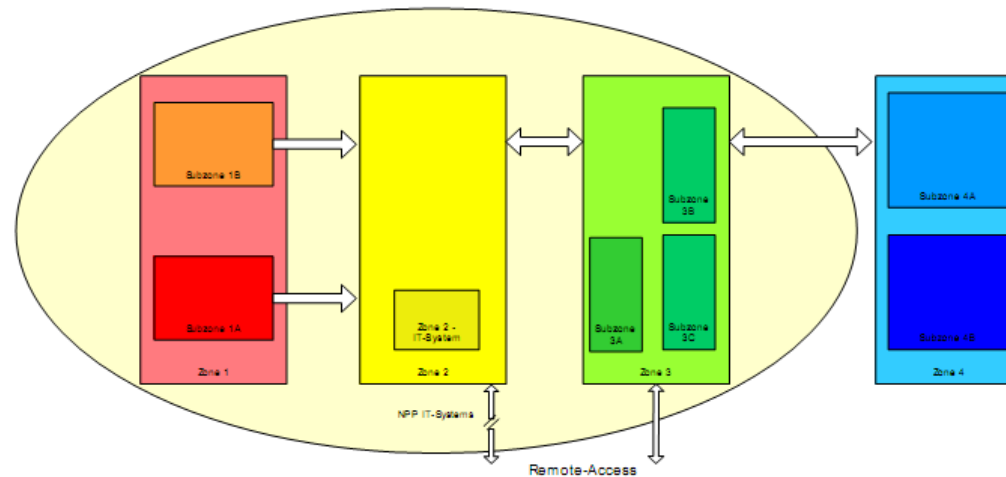


- Each of these individual components is a potential vulnerable point
- The challenge is that these components were not necessarily designed with computer security as consideration.

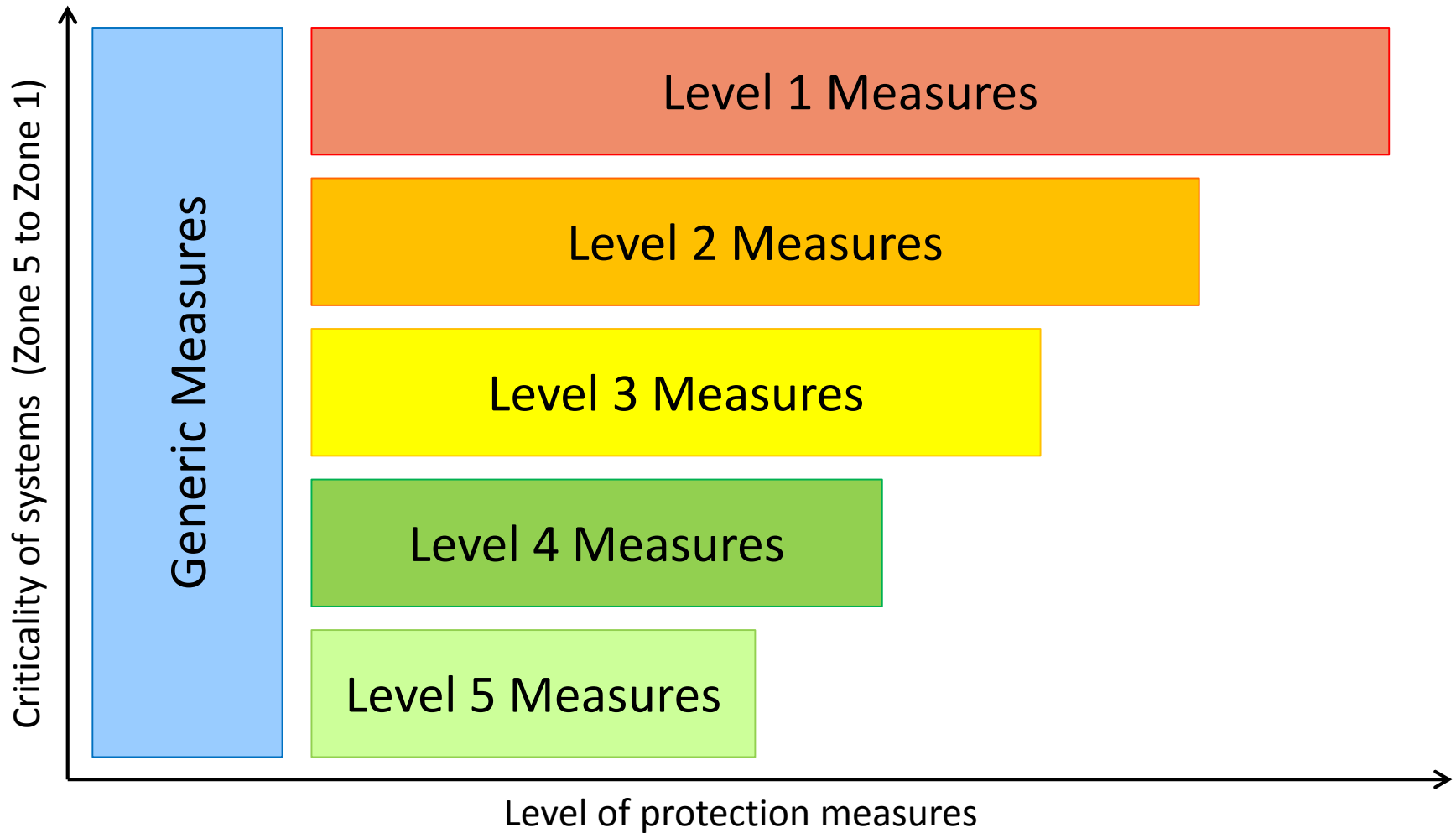
Security classification and zone model

Based on the „Computer Security at Nuclear Facilities”

- Classification: security / security related
- Graded approach: several security levels (based on risk analysis)
- Security zones
 - Inclusion of physical security and physical access control into the CSMS
 - Plant and system-specific
- Countermeasures i.e. security controls are selected on the basis of the security level / security zone / security subzone



Security Zones: Requirements



Generic measures for protection levels

The following generic measures should be applied for the systems:

- a) The licensee should regulate policies and procedures for each level.
- b) Protection procedures developed under a) should apply for and read by all users.
- c) Staff permitted access to the system should be suitably qualified, experienced and protection--informed.
- d) Users should be given access only to those functions on those systems that they require for carrying out their jobs.
- e) Licensee should ensure that appropriate access control and user authentication is in place.
- f) Licensee should apply appropriate anomaly detection systems and procedures.
- g) Application and system vulnerabilities should be monitored, and appropriate measures should be taken, if necessary.
- h) Licensee should undertake re-assessment of system vulnerability periodically.
- i) Licensee should control removable media in accordance with protection operating procedures.
- j) Computer and network protection components should be strictly maintained on periodical and continuous bases.
- k) Licensee should strictly log and monitor computer and network protection components (e.g. gateways, intrusion detection systems, intrusion prevention systems, virtual private network servers).
- l) Licensee should operate appropriate data backup/recovery procedures.
- m) Licensee should restrict physical access to components and systems according to their functions.

Specific measures for protection level 5/4

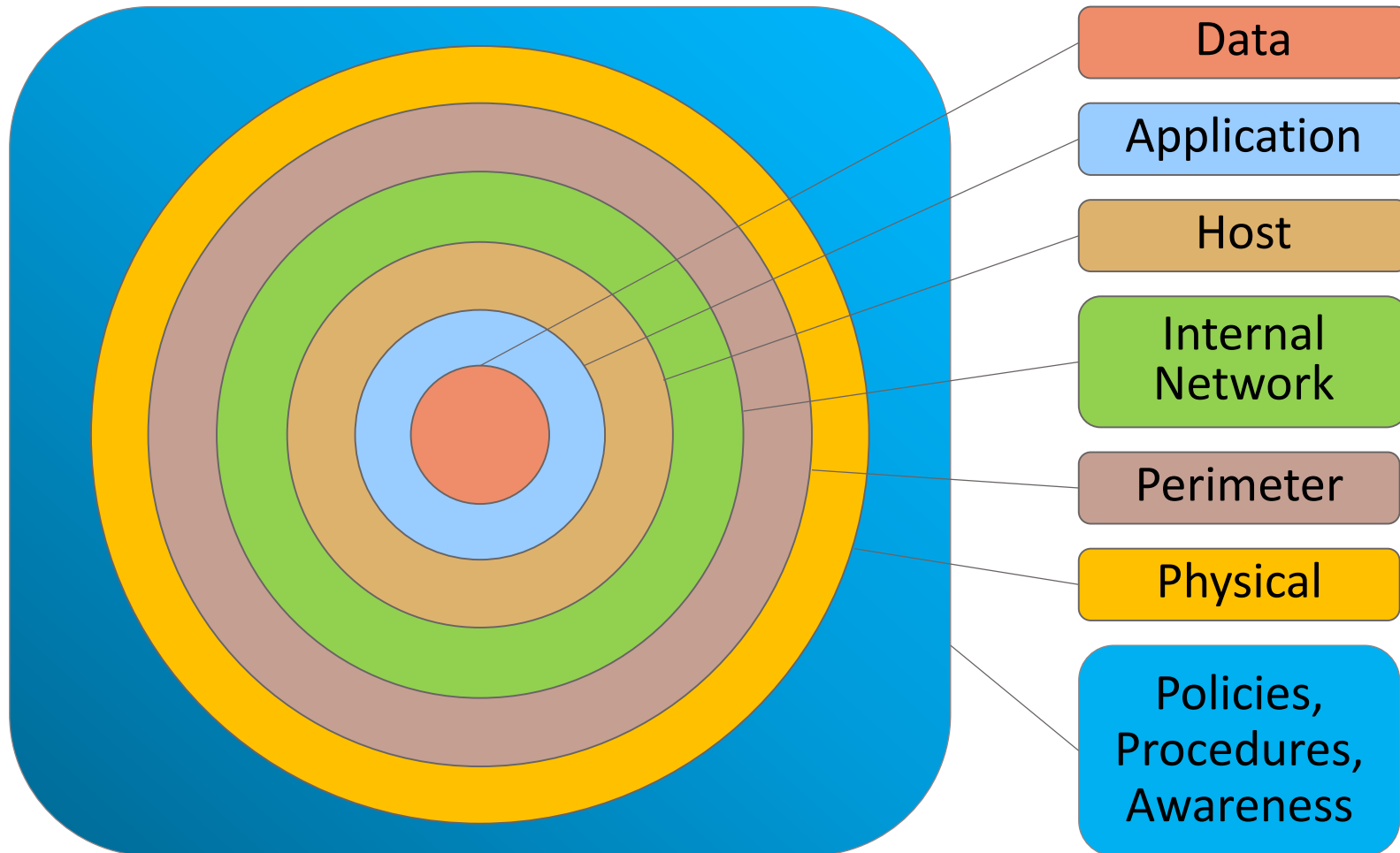
Specific measures for protection level 5 in addition to the generic measures:

- a) Only approved and qualified users are allowed to make modifications to the systems.
- b) Access to the Internet from level 5 systems is allowed provided that adequate protective measures are applied.
- c) Remote external access is allowed for authorized users provided that appropriate controls are in place.

Specific measures for protection level 4:

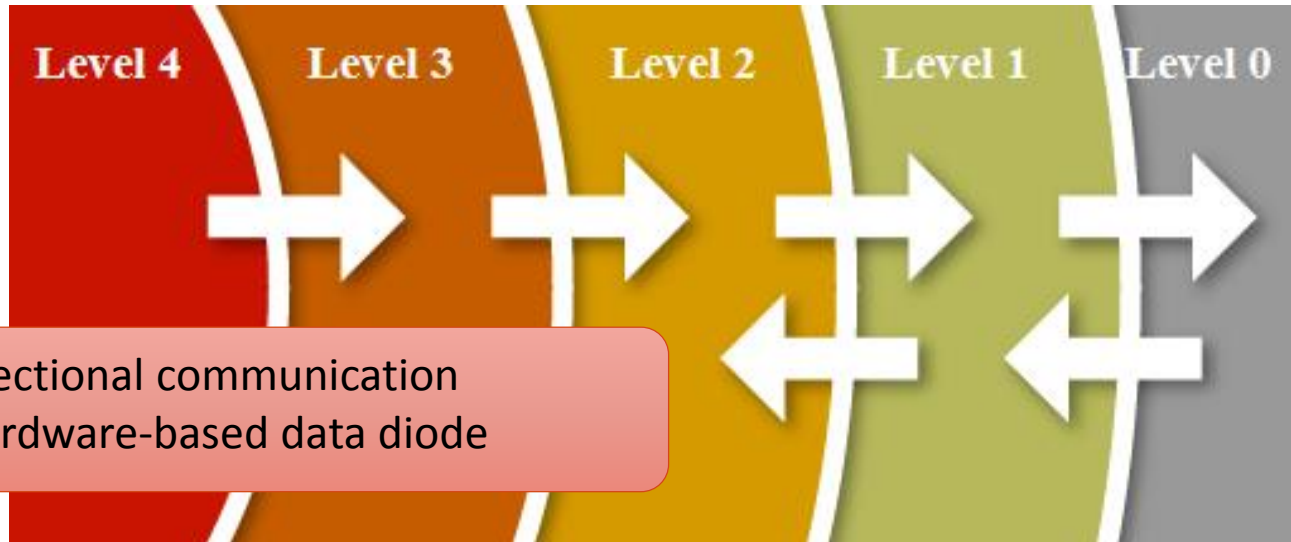
- a) Only approved and qualified users are allowed to make modifications to the systems.
- b) Access to the Internet from level 4 systems may be given to users provided that adequate protective measures are applied.
- c) Security gateways are implemented to protect this level from uncontrolled traffic from external company or site networks, and to allow specific activities which are controlled.
- d) Physical connections to systems are controlled.
- e) Remote maintenance access can be allowed and controlled on a continuous basis if the compliance with protection policy defined for remote computer and user is ensured.
- f) System functions available to users are controlled by access control mechanisms. Any exception to this principle should to be carefully studied and protection should be ensured by other means.
- g) Licensee may allow remote external access for approved users provided that appropriate access control mechanisms are in place.

Defense in Depth Layers



Defense in Depth protective strategy

- Based on RG-5.71 Defensive Architecture



Level 4: Vital Area

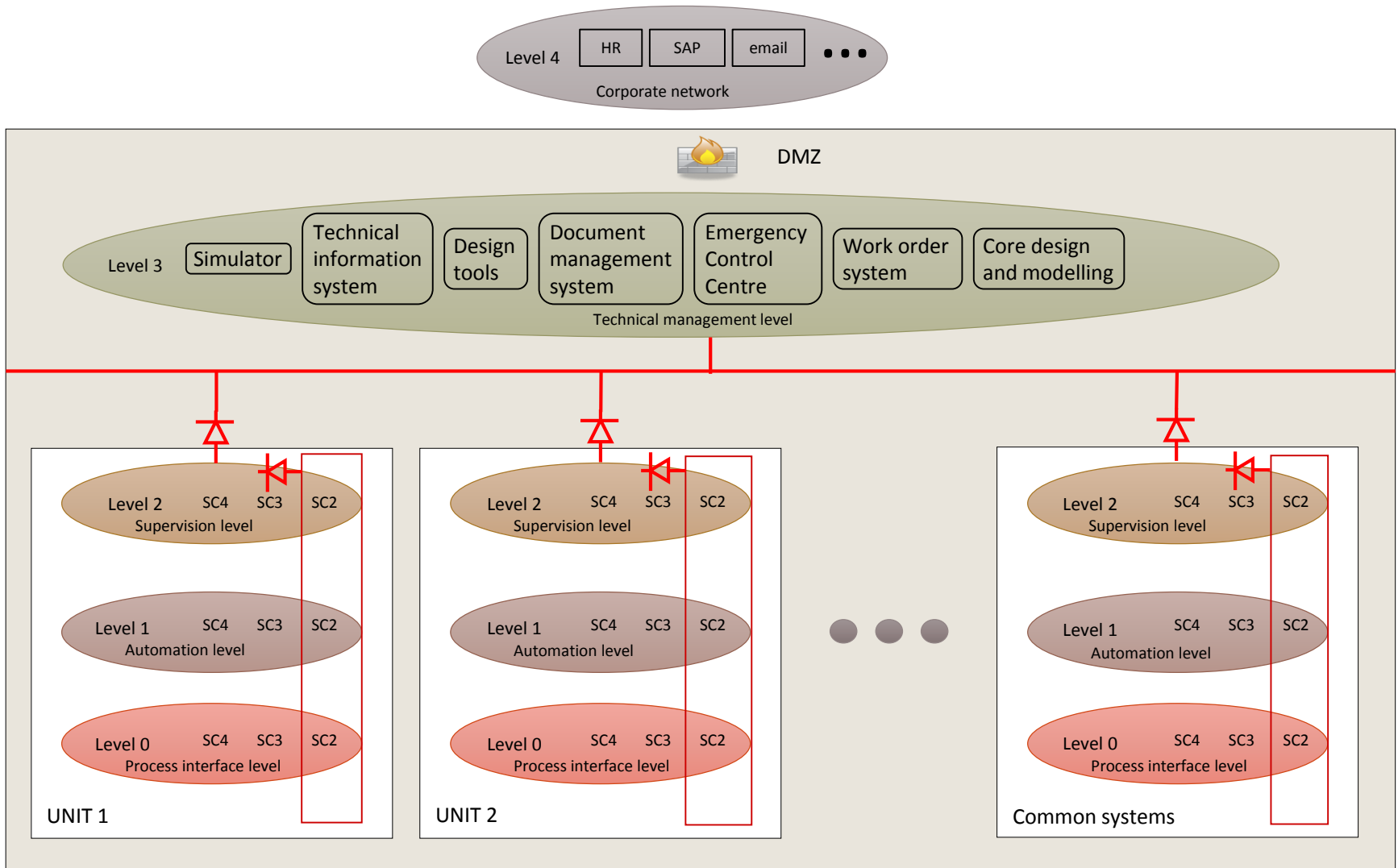
Level 3: Protected Area

Level 2: Owner-Controlled Area

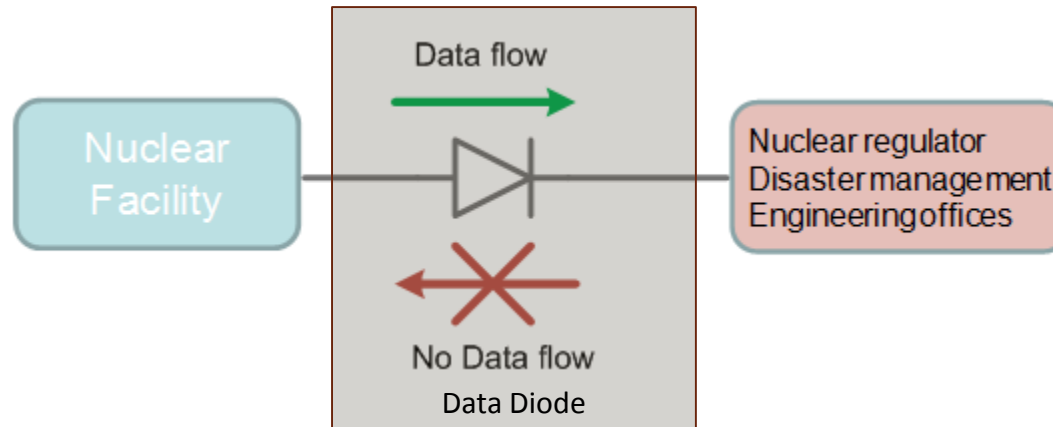
Level 1: Corporate Accessible Area

Level 0: Public Accessible Area

Possible Separation at a Multi-unit Site

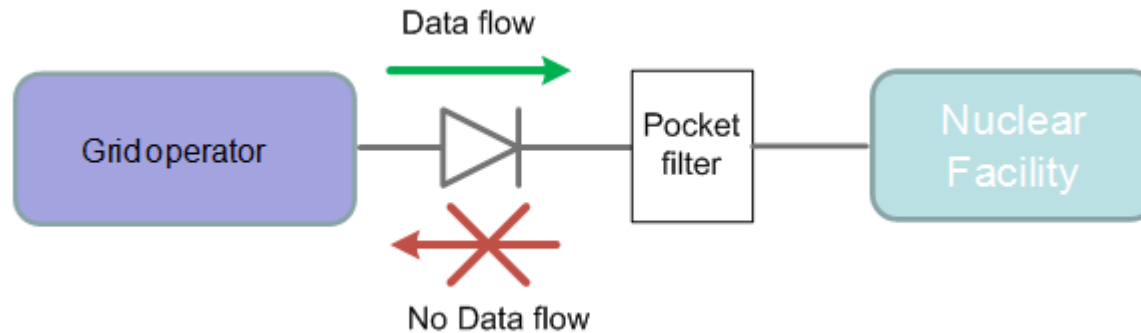


Exporting information



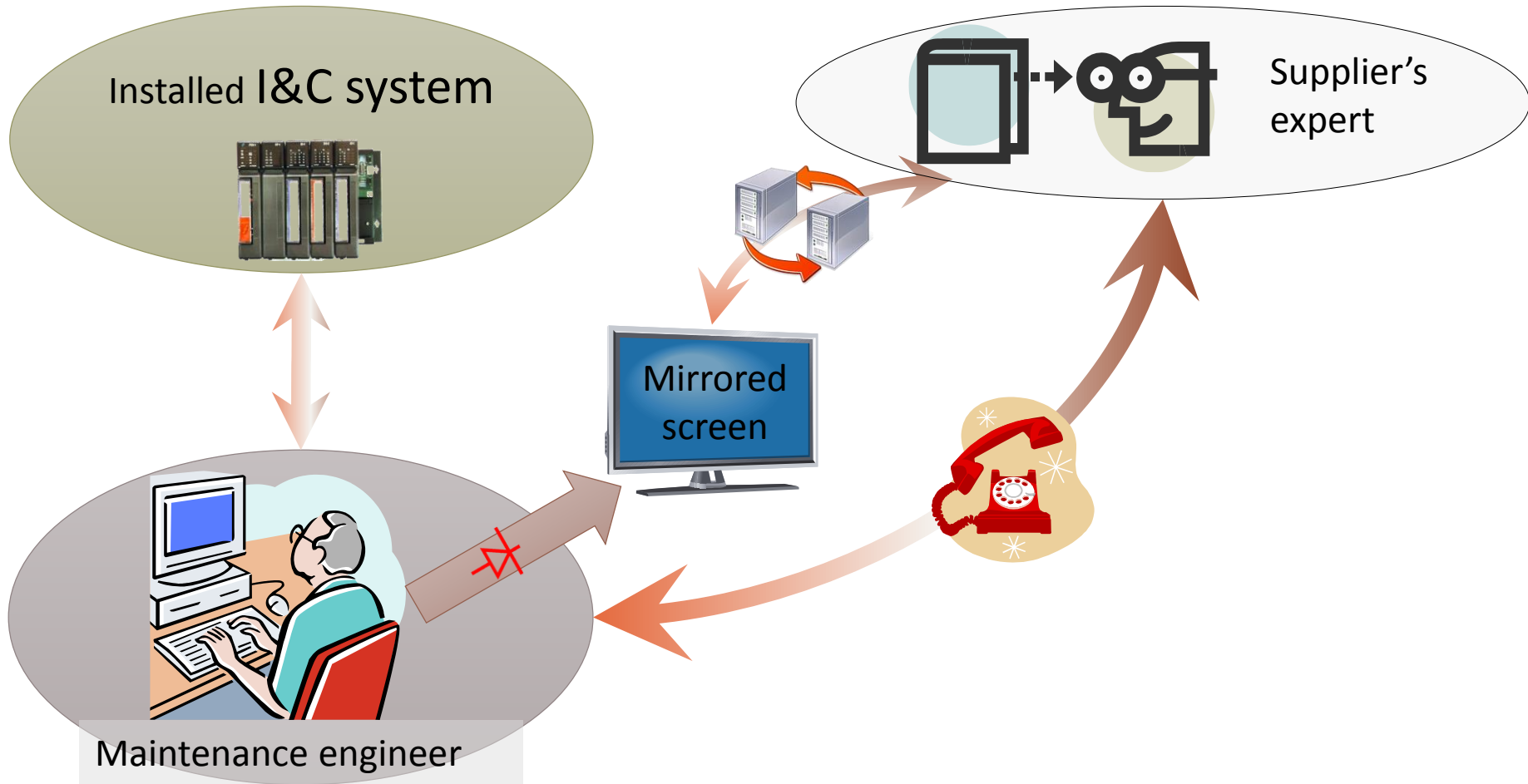
- No need for fast data transfer, delay is tolerated for 10s of seconds
- No need to send back even a single bit
- Reliability can be increased by telegram repetition and application of redundancy
- Monitoring can be solved by counting telegrams and watching for missing ones

Importing information



- Only a few (less than 10) signals are needed
 - Set point for the electric power regulator
 - Set point for the reactive power regulator
- Manual approval is provided for the operator

Remote maintenance?



Computer security personnel

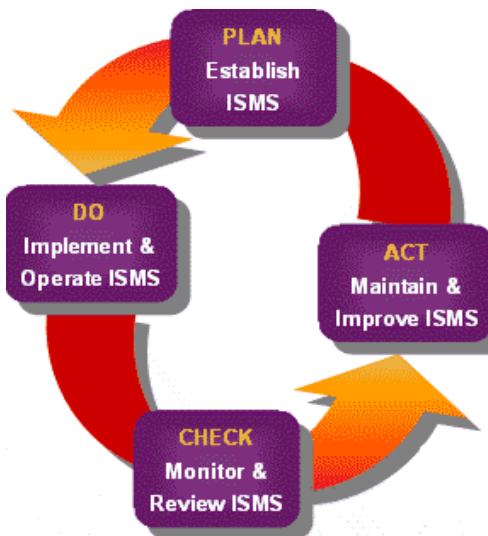
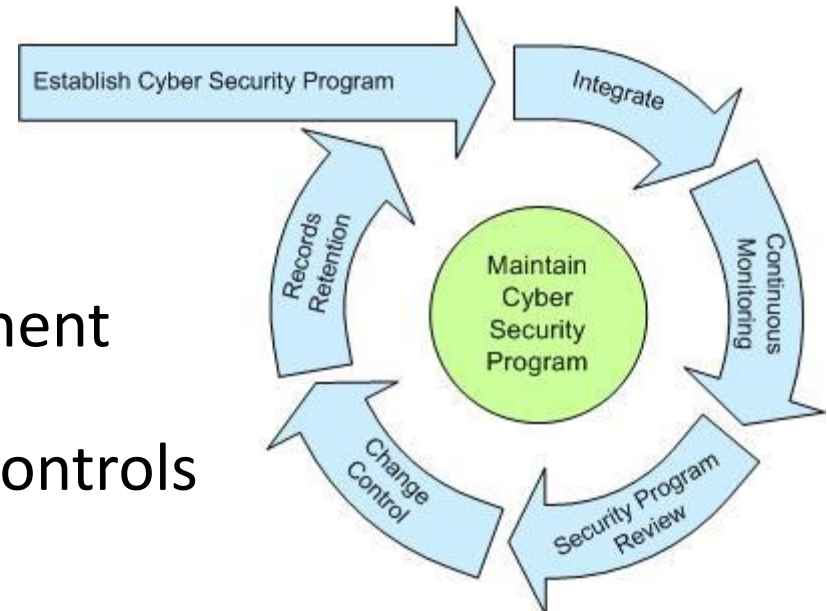
- Computer security requires *dedicated human and financial resources*
 - This means the *establishment of a specialist organization / team(s) and appointment of responsible leaders / managers*
 - The *regular training* and education of the computer security *organization and personnel is important*
 - As well as the continuous *monitoring, audit, evaluation, and subsequent updating* of the Computer Security Management System
- Computer Security Incident Response Team
 - Small, highly qualified expert team
 - Its task is the prompt reaction to „Stuxnet-like” incidents, the mitigation of consequences and provision of countermeasures
 - frequent training and exercises for the efficient handling of unexpected or critical safety incidents of digital I&C systems

Parts of the CSMS

- Precise, detailed and up-to-date **asset registry**
 - The critical and vulnerable digital assets affected by the attack can be identified very quickly after an incident using the registry
- The supervision and control of the internal and external (supplier, subcontractor) development and operational **IT, computer system, and I&C processes**
- Important documents of the CSMS
 - **Asset inventory** (later: registry)
 - **Risk assessment and evaluation** (later: internal audit)
 - **Computer Security Policy**
 - System-Level Computer Security Policies
 - **Disaster Recovery Plan**, DRP
 - **Business Continuity Plan**, BCP

Security Life-Cycle

- Asset identification and management
- Risk assessment, Security classification
- Computer Security Management System
- Implementation of security controls



- Continuous maintenance of CSMS
 - Planning → Implementation → Audit → Modification (Update) ↻
 - Regular evaluation of experiences, changes → integration of updates

I&C Systems Computer Security — Review

Remaining Challenges

- Information Sharing – Regulatory
- Who to Trust – Vendor, Integrator, Government?
 - Partnerships need mutual beneficial outcomes
- Active Monitoring - Resource Issues
 - if actively monitoring, can you respond?
- Collection of Data for Incident Response and Proactive Forensics
- How to Prove Attackers Off System (hard to do)
- Design Basis Threats may not adequately address the cyber component
- Consequences go well beyond just whether the system is on or off or damaged (compromise may include system manipulation)

Conclusions

- Attackers have both the means and the will to disrupt operations
- Control systems are no longer proprietary systems isolated from corporate networks
- Integrated systems use open standards such as Ethernet, TCP/IP, and web technologies
- Many attacks on ICS come from inside the corporate networks
- Standard IT security standards can interfere with control systems
- Digital ICS will only grow and must be considered in the initial the design process

References

- Process control and SCADA security - General Guidance - http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf?epslanguage=en-gb
- Control Systems Cyber Security: Defense in Depth Strategies - www.inl.gov/technicalpublications/documents/3375141.pdf
- Guide to Industrial Control Systems (ICS) (NIST sp 800-82) – <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- Improving SCADA Security - [www.us-cert.gov/control_systems/practices/pcsf/2005/d/improving_scada-security-litteer-rohde.pdf](http://www.us-cert.gov/control_systems/practices/pcsf/2005/d/improving_scada_security-litteer-rohde.pdf) - 2009-05-13
- ANSI/ISA-TR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems
- US CERT - http://www.us-cert.gov/control_systems/csstandards.html
- UK CPNI - <http://www.cpni.gov.uk/advice/infosec/business-systems/scada/>