IAEA
International Atomic Energy Agency

Regional Workshop on Managing the Interface Between Safety and Security for Research Reactors

Vienna, 6-10 June 2022

SAFETY – SECURITY INTERFACE ASPECTS OF DIGITAL SYSTEMS FOR RESEARCH REACTORS

Alexander Duchac (just retired)
Safety Assessment Section
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security

Contents

- Can we combine I&C safety guide developed for NPPs to research reactors?
- What are the cyber threats to digital I&C systems
- How to protect digital I&C systems against cyber attack
- Application of safety – security interface
- Lesson s learned from ‘successful’ cyber attacks
- Overview of Information and Computer Security publications

Research reactors and NPP have different natures

	NPP	Research reactors
Power output	High to generate electricity	Low
Experimental Facilities	No	Yes
Internal hazards*	Significant concern to I&C	Generally not a significant concern to I&C systems of low hazard potential RR
External hazards**	Significant concern to I&C	Generally not a significant concern to I&C systems
Operational cycle	Long	Short
Potential offsite consequences	High	Generally low

* Fire protection and EMI qualification apply, environmental qualification as necessary

** Seismic qualification applies

The NPPs pose different hazards

- For NPP the consequences of I&C failure is higher, they need
  - High level of design rigor
  - Reliability methods applied in depth
  - Robust design against natural phenomena

- This is may be too much for research reactors
  - Particularly for safety systems

- Research reactors of high hazard potential should follow the NPP guide

The plants have different internal hazards

- For NPP I&C can be exposed to
  - High radiation, steam jets, missiles, high temperature, chemical spray
- In research reactors I&C is generally not exposed to such hazards
  - Rigorous environmental qualification and separation is generally commensurate with the hazard potential
  - Main internal hazard is fire

The plants have different operating cycles

- NPP operating cycles are typically 12 to 24 months
  - On-line test capability for I&C is critical to reliability

- Research reactors have much shorter operating cycles
  - Offline testing can be sufficient to maintain reliability

The application of safety requirements on I&C systems is different

Topic	SSR-2/1 (Rev.1)	SSR-3
Requirements status	Mandatory	Applied using graded approach
Independence of safety systems	Required	Applied using graded approach
Remote shutdown capability	Required	None
Protection system	One +ATWS + Limited scope diverse backup if needed	Two
Experimental Facilities	None	Safe utilization

I&C systems should be adequately protected against cyber threats

- Despite different nature of NPP and research reactor, the computer security is equally important

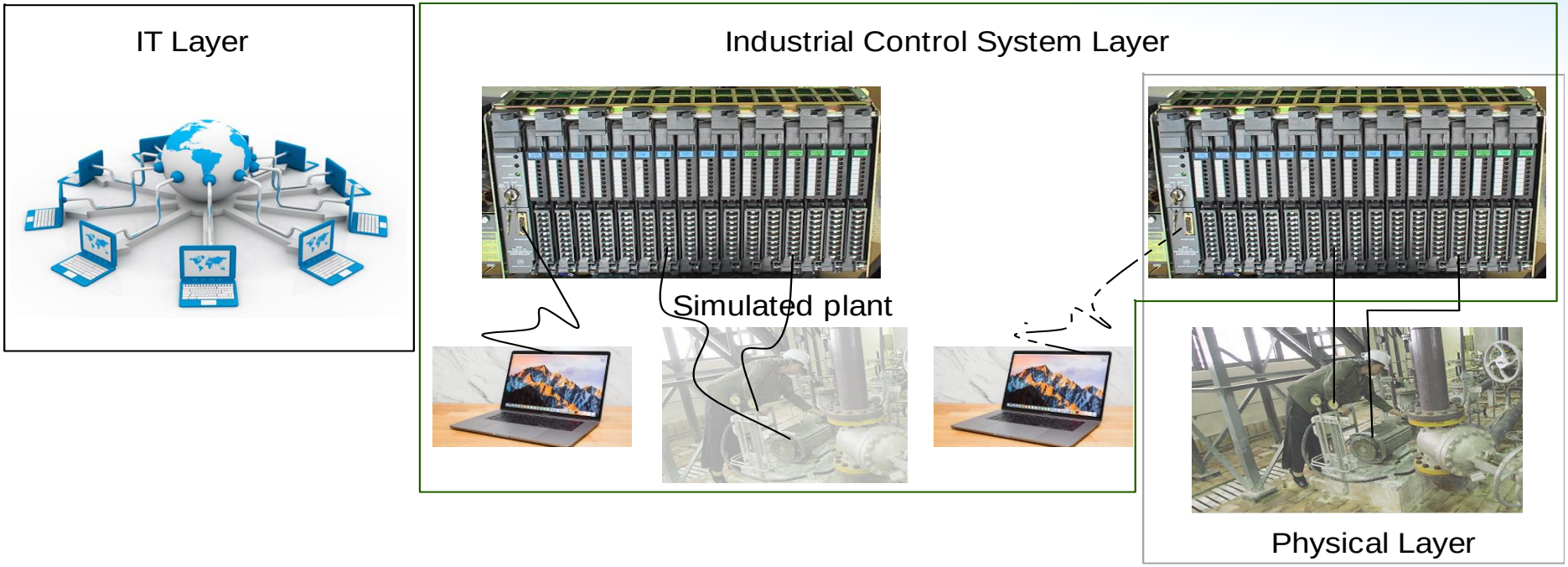
- The ‘critical’ I&C functions should be identified and acknowledged as important to computer security
  - To make the research reactor staff aware of their importance
  - To avoid compromising them during maintenance or modification

- IT controls are necessary to prevent/detect a cyber attack

Cyber threat may be introduced by

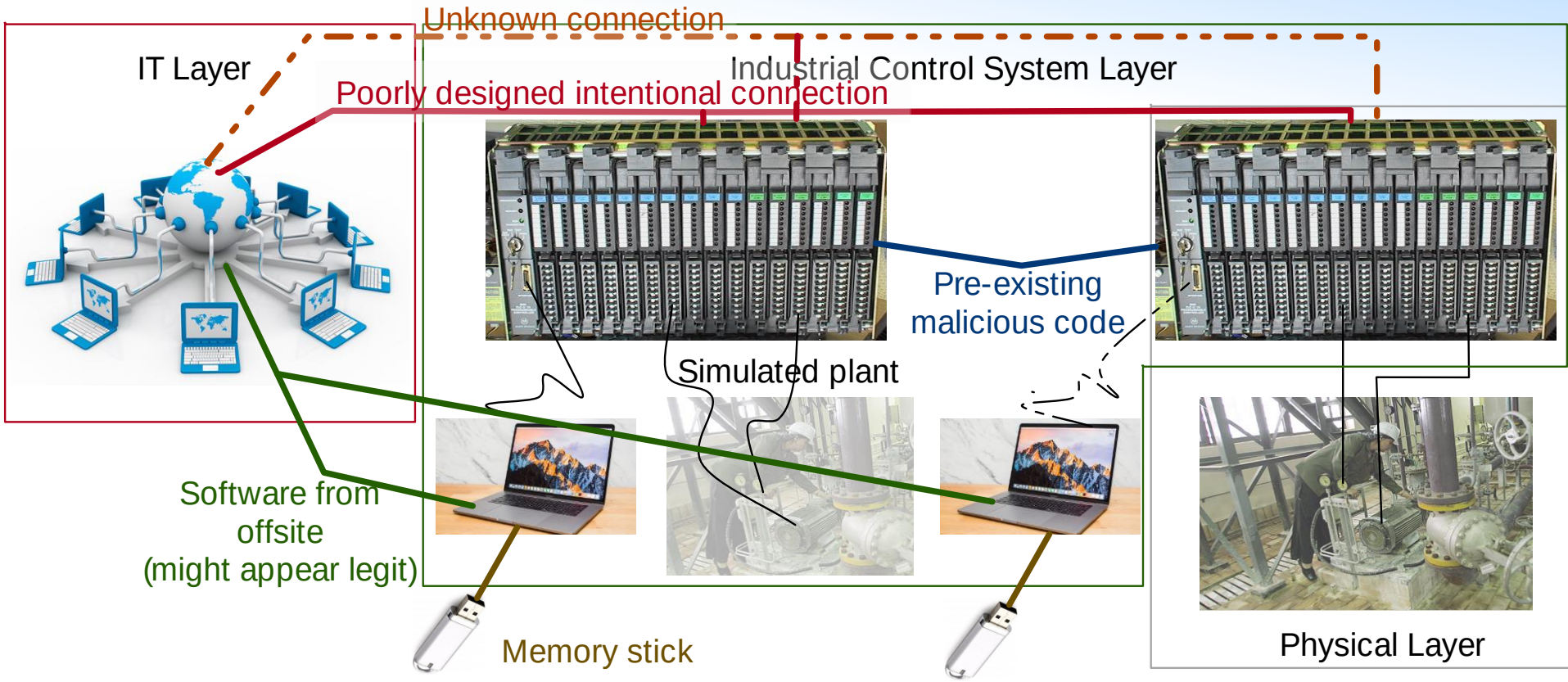
- Physical (unauthorized) access
- Electronic access
  - Software (installed & under development)
  - Configuration data
  - Control inputs (signals, and human)
- A defense in depth approach is needed
  - I&C system must implement the security controls
  - Security controls must not interfere with safety
- Remember: Hackers could modify systems remotely

Computer security uses the fact that threats must penetrate three layers



Good cyber security practices can significantly reduce the threat

There are opportunities for bypass



There are many paths to insert malicious code

A different mindset is needed to think about cyber threats

- Unexpected functions – not just failures
- Maybe multiple effects – not just single failure
- Maybe multiple systems involved – not just 1

The design process should account for a cyber threat

- The attack SW can be already present in the systems
  - Inserted during original software or hardware development
  - Inserted before IT protections put in place
  - Threats can bypass IT checks by appearing to be valid updates to development systems
    - Direct connections to plant systems are unnecessary

- Engineers need to recognize and avoid cyber threat as part of the design process
  - Don’t do anything stupid
    - e.g. high/low interlocks

A defence in depth approach applies to manage the cyber threats

- Prevention
  - Fail-secure devices that block unauthorized data communication
  - Strong administrative measures
- Management
  - Detect, delay and respond to precursors
- Mitigation
  - Stop execution of malware
- Recovery
  - Improve based upon lessons learned

- But! Security measures must not interfere with legitimate safety actions or place the plant outside of its design envelope

What I&C architecture must do

- Ensure that it does not compromise cyber controls provided by:
  - Physics
  - Mechanical features
  - Robust administrative controls
- Provide robust implementation of I&C functions that may cause a vulnerability to cyber attack
- Specify limits on I&C architectural approaches
- Identify constraints on the I&C systems

Lessons from ‘successful’ cyber attacks

- Cyber attack can insert new and malicious functions into I&C systems
- Cyber attack can affect multiple systems
- Threats can be introduced using the development system
- Threats can lay quiet until the system becomes trusted
- Either or both safety and non-safety system may be involved

IAEA
International Atomic Energy Agency

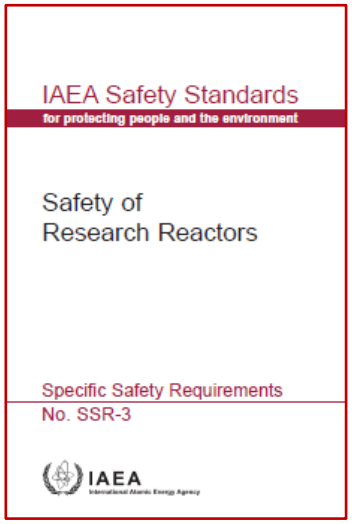
Overview of IAEA safety and security publications

What is (currently) available to address safety and security interface related to design, operation and maintenance of digital I&C systems?

The IAEA safety and security publications

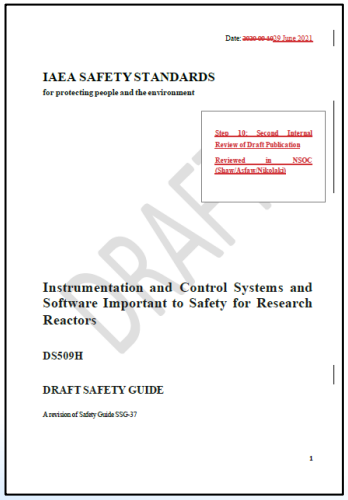
- Lay down provisions for ensuring the safety and security of programmable digital I&C systems
- Address major interfaces with the computer security activities
- Provide for I&C development life cycle activities with computer security programmes

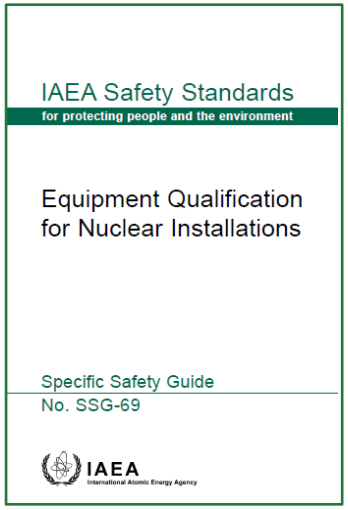
Overview of IAEA safety and security publications



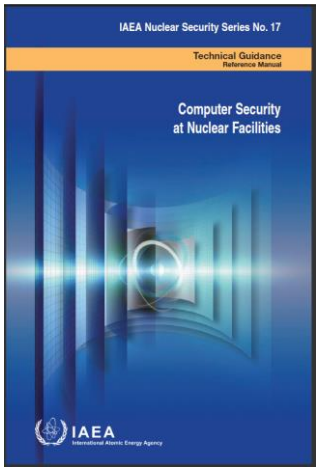
Requirements for Design (SSR)

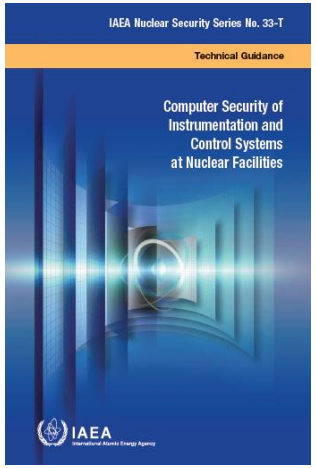
Recommendations "what should be done" to meet requirements (SSG)

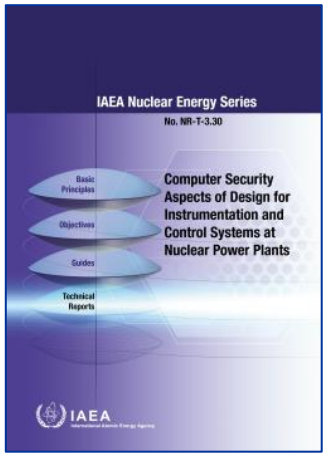




Computer security guidance publications for nuclear facilities





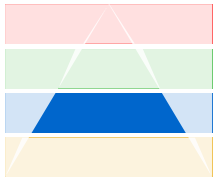


What I&C systems it applies

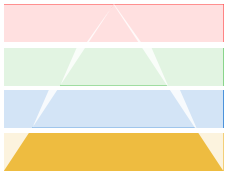
- SCADA (supervisory control and data acquisition) systems
- Distributed control systems
- Centralized digital control systems
- Control systems composed of programmable logic controllers
- Micro-controllers and ‘smart’ devices
- Systems using programmed logic devices
  - FPGA, smart devices and application-specific integrated circuits

Overview of information provided in IAEA computer security publications

State Nuclear Security Regime	• Sensitive Information • Roles and Responsibilities • Strategy • The Threat	• NSS23-G • NST045
Organizational Frameworks for Information Protection	• Laws and Regulation • Information Security Policy • Computer Security Programme (CSP) • Risk Informed Approach • Security Culture	• NSS23-G • NST045
Nuclear Facility CSP Implementation	• Facility Analysis: Functions and Systems	• NST047
Risk Assessment	• Vulnerability Analysis • Risk Determination • Sensitive Information and Sensitive Digital Asset (SDA) Identification	• NST047
Digital Asset Protection	• Computer Security Measure Implementation	• NST047 • NSS33-T

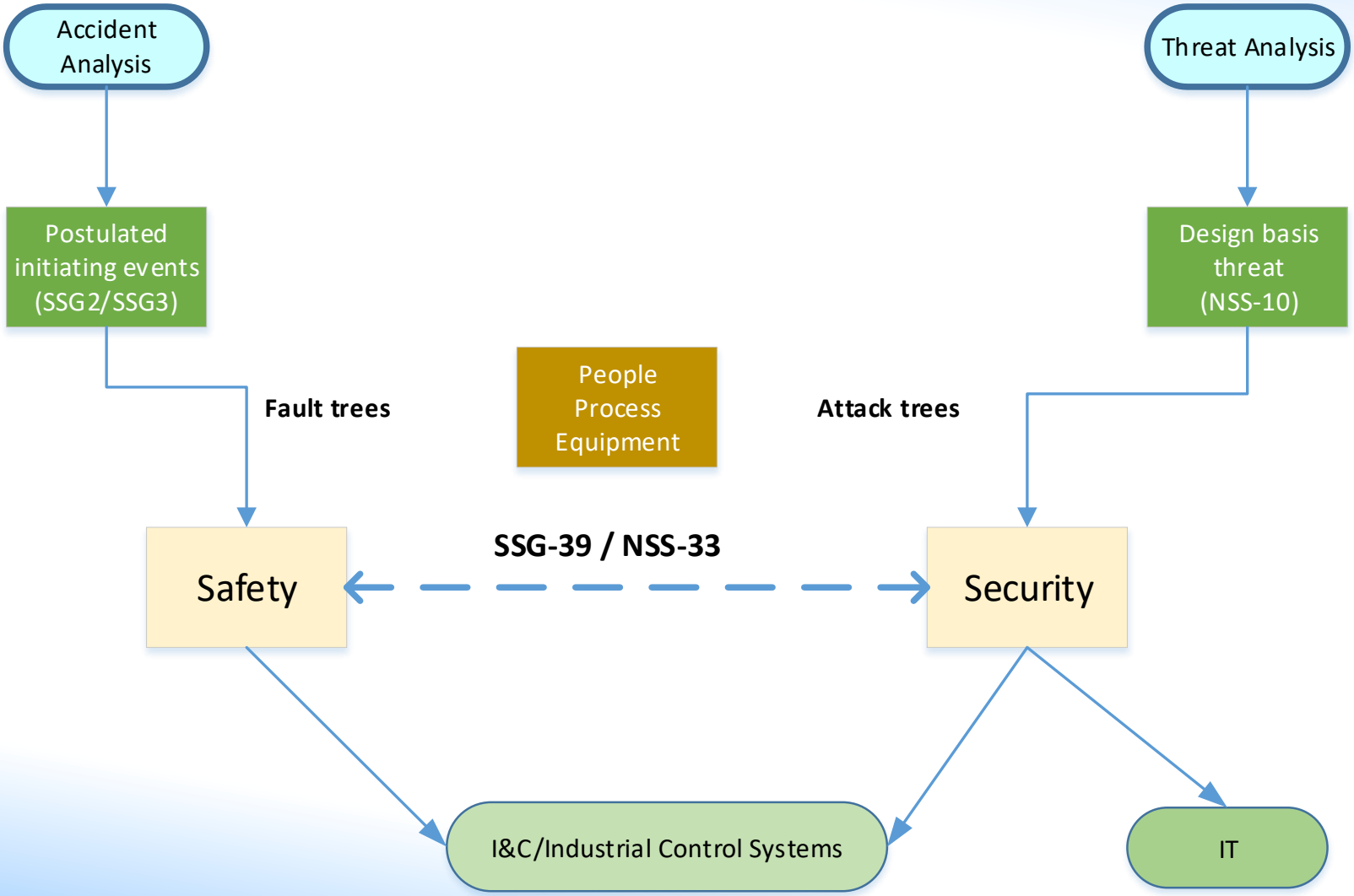


Guidance



Technical Guidance

Approach to analyze Safety–Security Interface



Conclusions

- Cyber attack can insert new and malicious functions into I&C systems
- Cyber attack can affect multiple systems
- Threats can be introduced using the development system
- Threats can lay quiet until the system becomes trusted
- Either or both safety and non-safety system may be involved
- Engineers need to recognize and avoid cyber threat as part of the design process
- I&C development life cycle activities must integrate computer security programmes

IAEA
International Atomic Energy Agency

Thank you!