Canadian Nuclear
Safety Commission

Commission canadienne
de sûreté nucléaire

Canada

ASSESSING CYBER SECURITY IN SMALL MODULAR REACTORS

Yubo (Kevin) Lei
Specialist
Systems Engineering Division
Canadian Nuclear Safety Commission

CNSC CCSN

Presentation Overview

- Vendor design review (VDR) overview
- CNSC cyber security regulatory requirements and guidance
- Cyber security review criteria
- Examples of good practices
- Potential cyber security challenges for SMRs

What is a vendor design review?

- A “pre-licensing review”
- There are no licensing or compliance licensing activities
- Provides regulatory feedback to a vendor
  - Understanding/applying regulatory requirements
  - Inform overall acceptability of the reactor design

Phase 1: early stage design review

- Confirm vendor understands CNSC requirements and expectations
- 5 cyber security **review criteria**
- Phase 2 review goes into considerably more depth

Regulatory Requirements/Guidance

- REGDOC 2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*
- CSA N290.7, *Cyber Security for Nuclear Facilities*
- Guidance
  - IAEA NSS No. 17, *Computer Security at Nuclear Facilities*
  - IAEA NSS No. 33-T, *Computer Security of I&C Systems at Nuclear Facilities*
  - IEC 62645, *Nuclear Power Plant-Implementation and Control Systems for Security Programmes for Computer-based Systems*

Cyber Security Review Criteria – Main Goal

- Examine the vendor’s strategy of cyber security in the design to protect computer-based instrumentation and control systems and components important to **safety** from cyber threats

Review Criteria 1 – Cyber Security Program

- The vendor’s submissions provide information that a cyber security program will be developed, implemented and maintained. The cyber security program will address potential security vulnerabilities and achieve the security required in each phase of the computer-based I&C systems’ lifecycle.

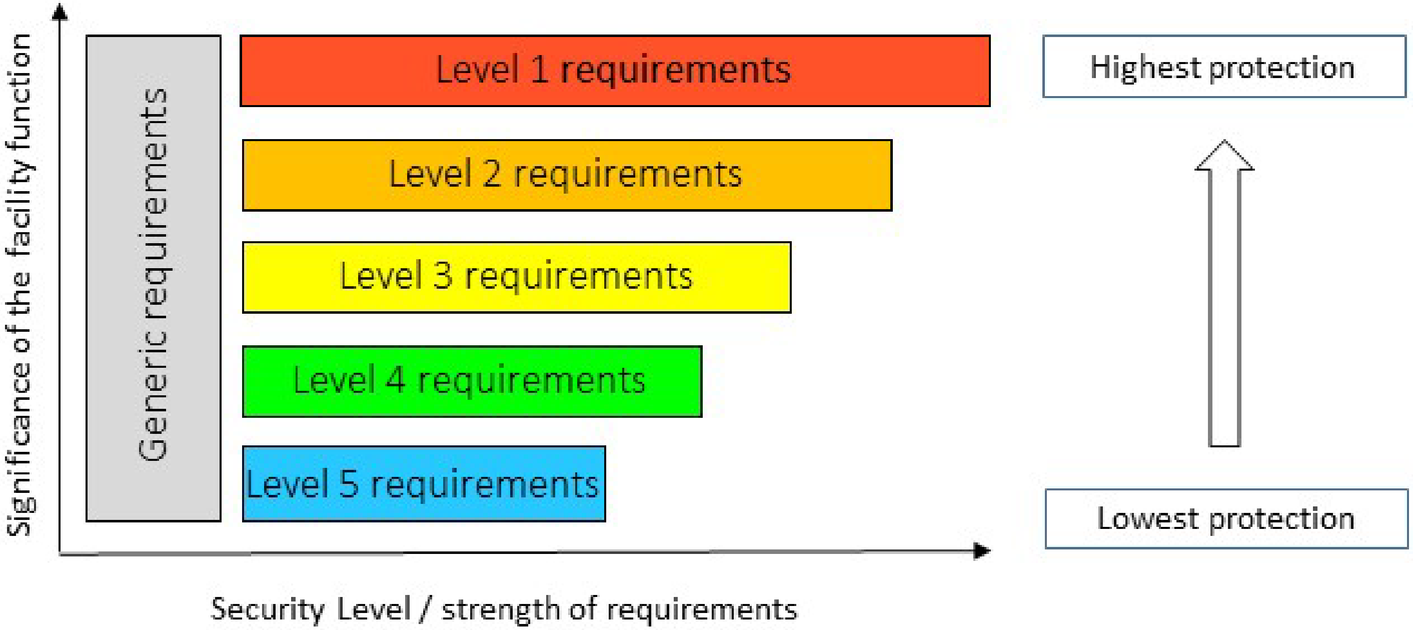
What we look for – Cyber Security Program

- Cyber program of vendor organization and licensee organization
- Cyber vulnerabilities can be introduced during design, development, operations, maintenance
- Elements of cyber security program

Review Criteria 2 – Cyber Security Architecture

- The vendor’s submissions provide information that the design of computer-based I&C systems will provide a cyber security defensive architecture. The defensive architecture will have cyber security defensive levels separated by security boundaries, and the systems requiring the greatest degree of security will be located within the most secure boundaries.

What we look for – Cyber Security Architecture



IAEA NST047 Computer Security Techniques for Nuclear Facilities, Feb 2018

Review Criteria 3 – CIA

- The vendor’s submissions provide information that the design will consider the protection of computer-based I&C systems and components important to safety functions from cyber attacks to maintain their **confidentiality**, **integrity** and **availability**.

What we look for - CIA

- Does vendor understand the definitions of confidentiality, integrity, and availability in the context of protection of computer-based I&C systems?

Review Criteria 4 – Access Controls

- The vendor’s submissions provide information that the computer-based I&C systems important to safety will be protected from unauthorized physical or logical access

What we look for – Access Controls

- Interface with physical security measures
- Policies and procedures (i.e. portable devices, access rights)
- Identify system hardening measures

Review Criteria 5 – Cyber Security Features

- The vendor’s submissions provide information that security functions and security supporting functions of I&C systems will not adversely affect the functions of systems and components important to safety. The design will ensure that neither the operation nor failure of security measures implemented will adversely affect the ability of the systems important to safety.

What we look for – Cyber Security Features

- Aware of key concept that safety and security measures designed/implemented in an integrated manner
- Guidance document
  - IEC 62859, *Requirements for coordinating safety and cyber security*

Good Practices by Vendors

- Cyber security monitoring capabilities
- Secure development environment on isolated network
- Integration with physical protection program measures

Good Practices (what we'd like to see more of)

- Defensive cyber security architecture
  - Establish zones
- Cyber security in the supply chain
- Cyber security and awareness training
- Validation activities during each phase of design

Potential Cyber Security Challenges for SMRs

- If reliance on remote staff for
  - Security operations
  - Safety operations
  - Cyber security monitoring
- Greater emphasis on **response controls**
- Communication link important

Conclusion

- CNSC performed several early stage review SMRs
- 5 review criteria
- Good practices by vendors and what we like to see more of
- Potential Cyber security challenges

Thank You! Questions?

nuclearsafety.gc.ca

Connect With Us

nuclearsafety.gc.ca