INTEGRATED APPROACH TO CYBERSECURITY

WINS Workshop on Security of Small Modular Reactors

Dave Trask, Principal Engineer Cyber Security

Nov 21, 2019

Canadian Nuclear Laboratories | Laboratoires Nucléaires Canadiens

Cyber Security for SMRs and VSMRs

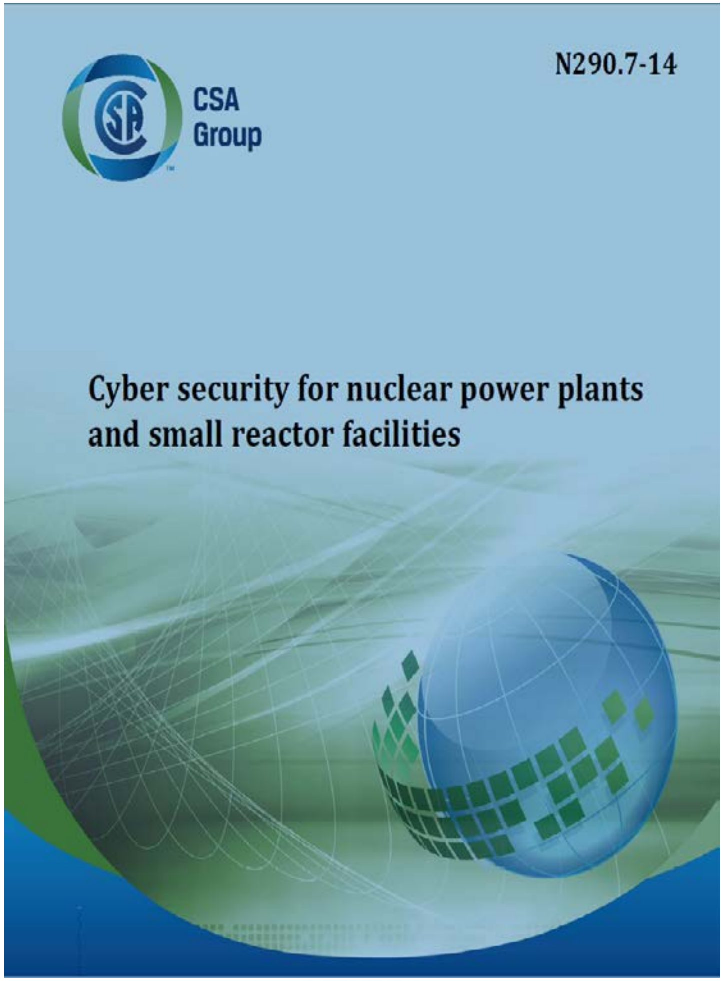
Cyber security program is key to managing risk and directing limited resources towards systems or assets based on their relative value or importance throughout their lifecycle

Digital Designs and architecture - first-of-a-kind solutions

- Remote monitoring and supervisory control
- Increased automation
- Limited on-site staff

➢ Identify potential regulatory uncertainties as soon as possible

Compliance Verification Criteria CSA N290.7



N290.7-14

CSA Group

Cyber security for nuclear power plants and small reactor facilities

CSA N290.7 … ensures consistent scope and language

a) Systems important to nuclear safety

b) Nuclear security

c) Emergency preparedness

d) Safeguards

e) Production reliability (optional)

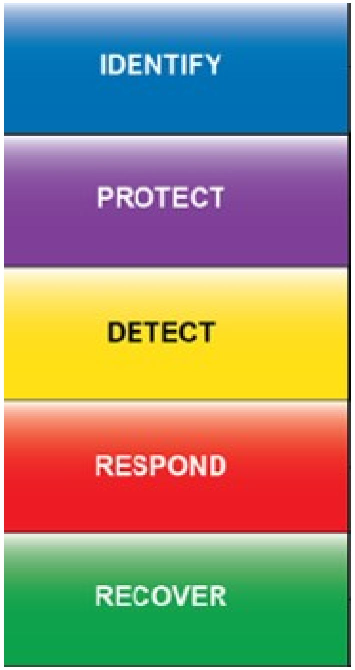
f) Auxiliary assets or systems which, if compromised, exploited, or failed, could adversely impact item (a), (b), (c), (d) or (e)

Cyber Security Essentials

SMR Designers expected to have a cyber security program that identifies their cyber security considerations from inception to decommissioning.

Early design

- Secure development environment
- Supply chain program
- Classification
- Defensive security architecture



National Institute of Standards and Technology (NIST)
Framework for Improving Critical Infrastructure Cybersecurity

Architecture … Identification and Classification

- Risk = Consequence x Likelihood

- Consequence (Significance):

Safety	Security	Emergency Preparedness	Safeguards	Grid Reliability

- Likelihood (Vulnerability / Susceptibility) (based on N290.7 cyber security attack pathways):

Physical	Wired	Wireless	Portable Media / Devices	Supply Chain

Cyber Security Classification

Significance	Safety [CSA N290.14]	Security [IEC 61226 | Physical Areas]		Emergency Preparedness [IEC 61226]	Safeguards [10 CFR 73]	Grid Reliability [AP-913]
High	Category 1		Vital Areas ?		Material Access Areas ?	
Moderate	Category 2					Cat I
Low	Category 3	Category C Safety Class 3	Protected Areas	Category C Safety Class 3		Cat II, III

Defensive Cyber Security Architecture Security Controls	Low	Moderate	High
Wireless	Conditional	🟨 Conditional	NO
Remote Access	Conditional	NO	
Uni-Directional Communications		🟨	Data Diode
Centralized SOC/SIEM	🟨	🟨	🟨
Zoning (physical/logical)	🟨	🟨	🟨

🟨 More restrictive in Draft CSA N290.7-20

Cyber Security Controls

N290.7-14			
Significance	Vulnerability		
	Low	Moderate	High
High	All		
Moderate	Baseline	All	
Low	Baseline		All

Draft N290.7-20	
Significance	
High	All
Moderate	Baseline + As Required By Susceptibility Analysis
Low	Baseline + As Required By Susceptibility Analysis to confirm adequacy of Baseline

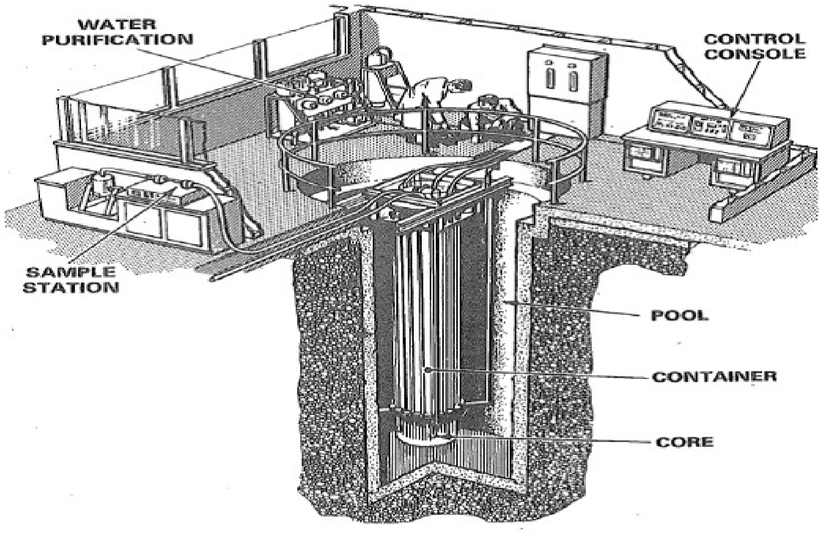
SLOWPOKE

Characteristics for Unattended Operation

- Assess current regulations for **20-kWt SLOWPOKE-2**

(Safe LOW Power *k*-ritical Experiment) tank-in-pool research reactor

  - **Licensed for *unattended* operation for up to 24h**
  - Inherent/passive safety features



- Reactor can safely accommodate all credible reactivity insertions by means of its self-limiting power excursion
- Reactor's inherent self-limiting power excursion behaviour and its strictly limited maximum excess reactivity, cannot be significantly increased by any action permitted to a reactor user
- There is no credible malfunction or combination of faults which would create a significant hazard to the reactor or persons about the reactor.

Remote Monitoring and Supervisory Control

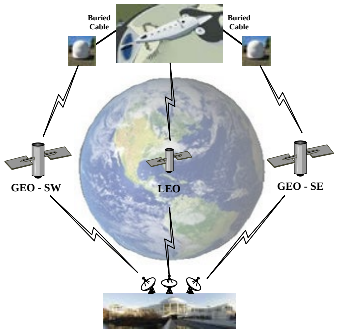
Benefits

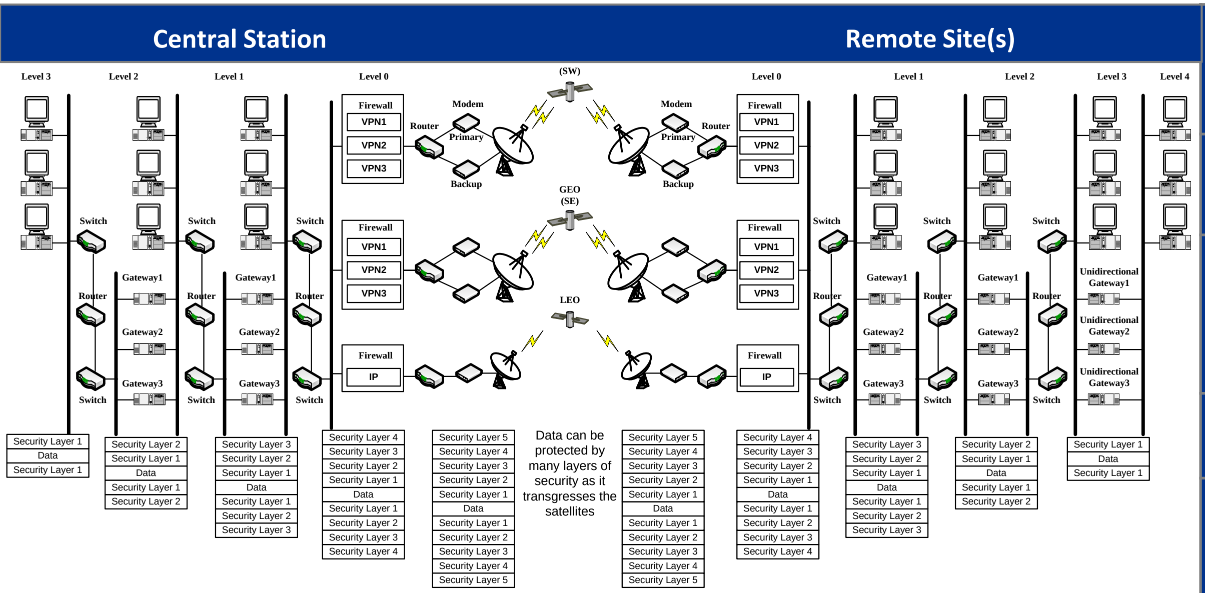
- Reduce need for full time on site licensed operators
- Reduce vulnerabilities by reducing access and human interactions
- Operate many sites from central location

Design Considerations and Fault Tolerance

- Security of Remote Controls / Maintenance
- Remote Security Operations Centre
- Cyber Security Incident Response Requirements and Capabilities
- On-site staff to support:
  - Cyber Security Incident Response Plans
  - Supplemental detection of unauthorized activities

SMR SCADA Systems for Remote Monitoring and Control - Wireless Solutions




Central Station
Remote Site(s)
Level 3
Level 2
Level 1
Level 0
(SW)
Level 0
Level 1
Level 2
Level 3
Level 4
Switch
Router
Gateway1
Gateway2
Gateway3
Firewall
VPN1
VPN2
VPN3
Modem
Primary
Backup
GEO
(SE)
LEO
IP
Unidirectional Gateway1
Unidirectional Gateway2
Unidirectional Gateway3
Security Layer 1 / Data / Security Layer 1
Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2
Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3
Security Layer 4 / Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3 / Security Layer 4
Security Layer 5 / Security Layer 4 / Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3 / Security Layer 4 / Security Layer 5
Security Layer 5 / Security Layer 4 / Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3 / Security Layer 4 / Security Layer 5
Security Layer 4 / Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3 / Security Layer 4
Security Layer 3 / Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2 / Security Layer 3
Security Layer 2 / Security Layer 1 / Data / Security Layer 1 / Security Layer 2
Security Layer 1 / Data / Security Layer 1

Data can be protected by many layers of security as it transgresses the satellites

Availability	• Diversity • Redundancy • Separation • Modulation (ACM, Frequency Hopping)
Confidentiality	• Encryption • Modulation • (Spread spectrum, Frequency Hopping)
Integrity	• Zones and Conduits • Multiple layers of security – Physical layer – Network Layer – Application Layer
Non-Repudiation	• Mutual Authentication
Safety	• Autonomous operation/shutdown – Tolerate delay and loss of communication – Keep-Alive Signal • Inherent/passive safety features

Threats

Safety - Unintentional / Accidental

Hazardous events	Threats					
	Repetition	Deletion \ Loss	Insertion	Re-sequencing	Corruption	Delay
HW systematic failure	x	x	x	x	x	x
SW systematic failure	x	x	x	x	x	x
Cross-talk		x	x		x	
Wires breaking/Loss of Signal/Jamming		x			x	x
Antenna misalignment		x			x	
Cabling errors		x	x		x	x
HW random failures	x	x	x	x	x	x
HW ageing	x	x	x	x	x	x
Use of un-calibrated instruments	x	x	x	x	x	x
Use of unsuitable instruments	x	x	x	x	x	x
Incorrect HW replacement	x	x	x	x	x	x
Fading effects		x		x	x	x
EMI		x			x	
Human mistakes	x	x	x	x	x	x
Thermal noise		x			x	
Magnetic storm		x			x	x
Fire		x			x	x
Earthquake		x			x	x
Lightning		x			x	x
Overloading of TX system/Oversubscription		x				x
Wire tapping/ Signal tampering/ injection/ interference	x	x	x	x	x	x
HW damage or breaking		x			x	x
Unauthorised SW modifications	x	x	x	x	x	x
Transmission of unauthorised messages	x		x			

Jarmo Alanen, Marita Heitikko, Timo Malm, Safety of Digital Communications in Machines, VTT TIEDOTTEITA –Research Notes 2265, VTT Industrial Systems, 2004

Security - Intentional / Malicious

Confidentiality – preventing unauthorized disclosure or access to information.

Eavesdropping
Traffic analysis

Integrity – preventing unauthorized modification of information

Replay
Tampering/Message Modification
Masquerade
Man-in-the-middle

Availability – preventing denial of service and ensuring authorized access to and use of information

Denial of Service
Denial of Access

Non-repudiation – preventing the denial of an action that took place or the claim of an action that did not take place. (proof of origin and proof of delivery)

Threats and Countermeasures

- Consider safety and security aspects of satellite networks used for remote monitoring and control

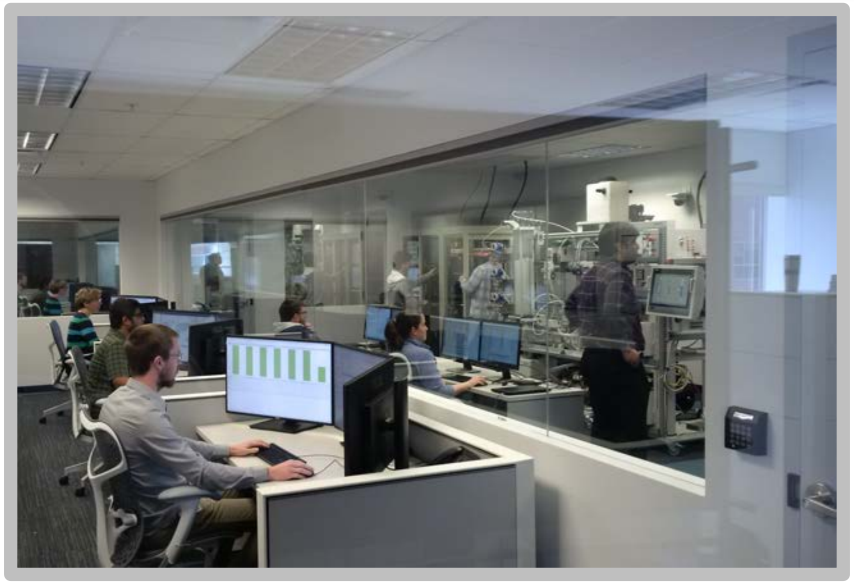
- Authorized, unaltered messages arrive in time, in order, and at the correct destination to precipitate the necessary control action

Objectives	Threats	Countermeasures																	
		Frequency Modulation	Signal Masking	Encryption	Hashing (CRC, MD, Secure)	MAC, HMAC	Digital Signature	Restricted Access	Inconsistency	Redundancy	Sequence identifier	Timestamp	Timeout/Time expectation	Time Triggered	Bus guardian	Prioritization of messages	Inhibit Times	Source and Destination Ids	Feedback Message
Confidentiality	Signal Interception Eavesdropping	x	x	x			x												
	Traffic analysis	x	x																
Integrity	Replay/ Repetition										x	x					x		x
	Excessive Jitter													x		x	x		x
	Insertion								x		x	x	x	x					x
	Incorrect sequence								x		x	x							x
	Deletion	x							x		x	x	x	x					x
	Corruption	x			x	x	x		x										x
	Tampering/ Modification	x			x	x	x		x										x
	Delay	x											x			x	x		
	Masquerade					x	x												
	Man-in-the-middle					x	x												
	Addressing					x	x											x	
Availability	Loss of Service	x								x					x				
	Denial of Service	x						x		x									
	Resource exhaustion	x								x					x		x		
	Denial of Access	x						x		x									
Non-Repudiation	Repudiation						x												

Remote Maintenance Using Mixed Reality

- Reduce staff entering a hazardous work environments (ALARA) and/or reduce the need for specialist to travel to remote sites
  Subject matter experts can guide a less experienced workers from remote locations.
- Consider Device Security capabilities.
  Device encryption, device and network authentication, hardened executable, tamper detection, verified operating system
- Security of sensitive data
  Assess security requirements for data encryption, in transit and at rest
- Public-cloud computing environments send data off-site and possibly out of country.
  Assess security requirements for on-premise versus cloud computing environments.
- Review environment and connectivity for solution’s bandwidth capabilities.
  Some solutions may operate better in low-connectivity areas, some as low as 256kps and can be connected to a mobile hotspot.

Cyber Security



- National Innovation Centre for Cyber Security located in Fredericton and part of leading cyber security ecosystem in Canada
- Facility informs threat models that serve as a testing framework and for developing cyber security solutions
- Capabilities and services available in:
  - Realistic incident response exercises and training
  - Roles-based training
  - Provisioning and operation of security operations centre (SOC)
  - Assessing compliance to CSA N290.7 “Cyber Security for NPPs”
  - Performing security assessments of products and suppliers in order to secure the supply chain
  - Deploying CNL-developed non-invasive, real-time technology to detect cyber intrusion in safety-critical nuclear process control systems

Questions?

Canadian Nuclear Laboratories | Laboratoires Nucléaires Canadiens

Dave Trask
Principal Engineer, Cyber Security
Canadian Nuclear Laboratories
Dave.Trask@cnl.ca