Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Status of Cyber Security Implementation in Canadian NPPs

Korean Nuclear Society Conference
Jeju, Korea, May 11-13, 2016

Chul Hwan Jung
Technical Specialist
Systems Engineering Division
Canadian Nuclear Safety Commission

e-Docs 4982091

nuclearsafety.gc.ca

Canada

Contents

Canadian Nuclear Safety Commission (CNSC)

Canada's Nuclear Watchdog

Regulates the use of nuclear energy and materials to protect the health, safety and security of Canadians and the environment; implements Canada's international commitments on the peaceful use of nuclear energy

CNSC Presence

- Headquarters in Ottawa
- 5 offices at NPPs
- 1 site office at Canadian Nuclear Labs
- 4 regional offices
- Staff: ~800

Calgary Western Regional Office

Saskatoon Uranium Mills and Mines Division Regional Office

Gentilly-2

Point Lepreau

HQ

Chalk River

Laval Eastern Regional Office

Bruce

Darlington

Pickering A and B

Mississauga Southern Ontario Regional Office

Nuclear Power Plants in Canada

Darlington

Pickering

G2

Point Lepreau

Bruce

Darlington (4-unit station)
- Refurbishment of current 4-unit station scheduled to begin in 2016

Point Lepreau (single-unit station)
- Refurbishment completed and unit returned to service end 2012

Gentilly-2 (single-unit station)
- HQ permanently shut down facility in December 2012. Unit currently in safe shutdown state

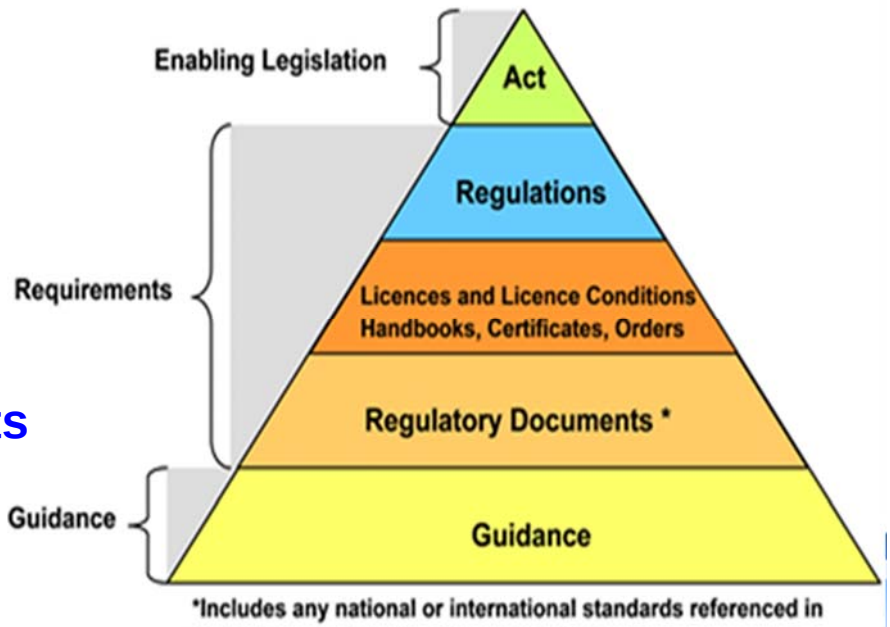
Bruce (8-unit station)
- Refurbishments ongoing (2 of 8 units completed as of 2016)

Pickering (6 of 8 units operating)
- Shutdown expected in 2024

CNSC's Regulatory Framework

The CNSC's Regulatory Framework consists of

- **Acts** passed by Parliament that govern the regulation of Canada's nuclear industry
- **Regulations**
- **Licences/Conditions**
- **Regulatory Documents** used by the CNSC to regulate the nuclear industry



Nuclear Control and Safety Act (NSCA)

- The NSCA establishes the regulatory framework for nuclear matters in Canada
- CNSC has the authority under the NSCA to make regulations
- Regulations set requirements for all types of licence applications and obligations
- CNSC has thirteen (13) regulations

Regulations: Applicable for Cyber Security for NPP Design & Operation

- *General Nuclear **Safety** and Control Regulations*
  - provide general requirements for licensee obligations
  - "every licensee shall take reasonable precautions to maintain the security of nuclear facilities"
- *Nuclear **Security** Regulations*
  - provide security requirements for high-security sites (e.g., NPPs)
  - provide security information requirements and general security obligations of licensees

Requirements for Cyber Security in REGDOCs and LCHs

To incorporate appropriate requirements for cyber security of NPPs and small reactor facilities, CNSC staff have updated:

- Regulatory Documents (REGDOCs)
- Licence Conditions Handbooks (LCHs)

REGDOC-2.5.2 Design of Reactor Facilities: NPPs (2014 May) - Cyber Security (1/4)

(5.2 Design management):

- *Appropriate design management shall achieve the objectives: cyber security programs are provided to address design-basis threats.*

(5.7 Design documentation):

- The design documentation shall include a description of cyber security programs.

(7.9.2 Use of computer-based systems or equipment):

- The I&C development lifecycle should be coordinated with the human factors engineering lifecycle and the cyber security lifecycle.

REGDOC-2.5.2 Design of Reactor Facilities: NPPs (2014 May) – Cyber Security (2/4)

(*7.22.4 Cyber Security):*

- The design of computer-based I&C systems important to safety shall:
  - provide a cyber security defensive architecture.
  - be protected from cyber attacks in order to maintain confidentiality, integrity and availability.

REGDOC-2.5.2 Design of Reactor Facilities: NPPs (2014 May) – Cyber Security (3/4)

(7.22.4 Cyber Security):

- A cyber security program shall be developed, implemented and maintained so as to achieve the security required in each phase of the computer-based I&C systems' lifecycle.
- Cyber security features shall not adversely affect the functions or performance of SSCs important to safety.

REGDOC-2.5.2 Design of Reactor Facilities: NPPs (2014 May) – Cyber Security (4/4)

(7.22.4 Cyber Security):

- The design of a cyber security program should consider:
  - **documentation** for how the design authority establishes, implements and maintains the program
  - application of **defence-in-depth protective strategies** to provide a high level of assurance
  - addressing potential **security vulnerabilities in each phase** of the computer-based I&C systems lifecycle
  - inclusion of security controls for **a secure development environment** during the development phases

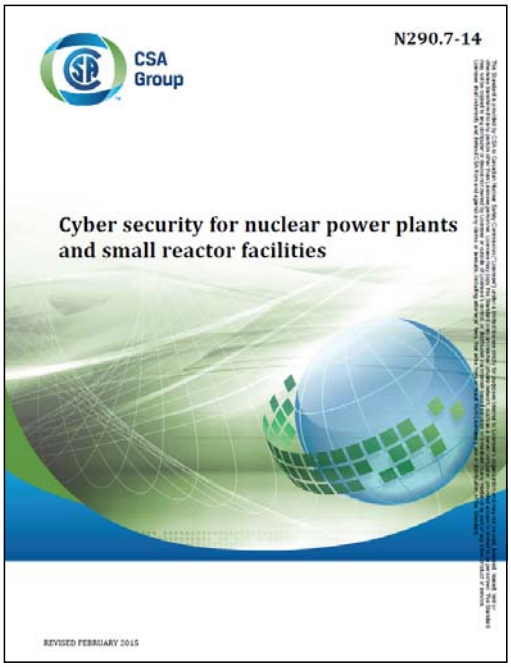
Design Basis Threat Analysis (DBTA)

- The *Nuclear Security Regulations* (NSR) require the CNSC to establish a design basis threat analysis (DBTA) which specifies the Design Basis Threat (DBT) for licensees to conduct a facility-specific Threat and Risk Assessment (TRA) to determine the adequacy of its physical protection system.
- CNSC staff addressed cyber threat in the DBTA and issued it in 2014.

Licence Conditions Handbook (LCH)

- LCH clarifies the regulatory requirements and other relevant parts of the licensing basis for each condition in the licence
- CNSC staff have added requirements for cyber security in the security section when the LCH is renewed

CSA N290.7 Standard – Cyber Security for Nuclear Power Plants and Small Reactor Facilities (2014)



- Industry-developed standard in which CNSC participates as committee member
- Will form the cornerstone for regulation of cyber security at NPPs and small reactor facilities in Canada

CSA N290.7 Cyber Security for Nuclear Power Plants and Small Reactor Facilities (2014)

- New standard
  - Started drafting in December 2012, published in December 2014
- CSA N290.7 TSC members: NPP licensees, CNSC, NPP design vendors, research lab licensee, SMR design vendor, consultants
- Based upon the experience gained in the implementation of cyber security programs at the Canadian NPPs and the experience of CNSC staff's regulatory activities.

CSA N290.7 – Table of Contents

- Scope, definitions
- Cyber Security Program
  - General requirements, elements of the program
  - Establishing, implementing, reviewing and maintaining the program
  - Interface with other programs and processes
- Roles and responsibilities
- Identification and classification of CEAs
- Cyber security architecture
- Controls, lifecycle management
- Annex A definitions for cyber security controls

CSA N290.7 – Scope of Standard

Addresses cyber security at NPPs and small reactor facilities for the following computer systems and components:

a) systems important to nuclear safety;
b) nuclear security;
c) emergency preparedness;
d) production reliability;
e) safeguard; and
f) auxiliary assets or systems which, if compromised, exploited or failed, could adversely impact Item (a), (b), (c), (d) or (e).

CSA N290.7 – Identification of CEAs

- CEAs shall be identified as those cyber assets that perform or impact on SSEP and Safeguards* functions
- CEAs may be identified as those cyber assets that impact production reliability
- The identification of CEAs shall be conducted without accounting for existing physical or logical mitigating measures

* Excludes IAEA-owned safeguard equipment

CSA N290.7 – Classification of CEAs

- The CEA cyber security classification scheme shall be documented and based on
  (a) safety or security **significance**; and
  (b) **vulnerability** to cyber threats.
- The safety or security significance of a CEA shall be classified in levels:
  - high, moderate, or low significance
- The classification of the CEA vulnerability may take into consideration existing physical or logical mitigating measures.

CSA N290.7 - Security Controls

- Cyber security controls shall be implemented such that they:
  (a) are applicable; (b) are technically feasible; and
  (c) do not impact the CEA's functionality and performance.

	Low Vulnerability	Moderate Vulnerability	High Vulnerability
High Safety or Security Significance	All controls	All controls	Immediate Remediation
Moderate Safety or Security Significance	Five baseline controls	All controls	All controls
Low Safety or Security Significance	Five baseline controls	Five baseline controls	All controls

CSA N290.7- Lifecycle Management

- The cyber security program shall manage potential security vulnerabilities in each phase of the system or asset lifecycle.
- The cyber security program shall:
  - ensure that a secure development environment (including tools and development facilities) is established for CEA development;
  - ensure that a secure development process is applied to CEA development.

Cyber Security Program – Requirements on NPP Licensees

Key Cyber Security Program elements:

- policies and procedures
- identification and classification of CEAs
- roles and responsibilities
- awareness and training
- interface with other programs and processes
- security architecture
- security controls
- incident response, recovery, and reporting;
- CEA lifecycle approach
- program effectiveness evaluation, review, and maintenance

Cyber Security Program Requirements of Operating NPPs

Site-specific cyber security programs are in place in all NPPs following issuance of CNSC Action Item raised in 2008.

- Regulatory Framework (current)
  - ✓ Regulatory Position Statement: Letter to NPP licensees outlining CNSC expectations (July 2008)
  - ✓ References: IAEA NSS-17, NEI 04-04, NUREG/CR-6847
  - ✓ LCH: SCA: Security
- Regulatory Framework (near future)
  - ✓ CSA N290.7 in LCH: SCA: Security

State of cyber defensive architecture in Canadian NPPs

- Networks responsible for safety systems, process control systems, physical security systems and business systems are segregated
- Safety system network connected to process system network via one-way communication device (no possibility of bidirectional information flow)
- Administrative and mechanical controls prevent unauthorized access (portable mobile devices, etc.) to safety, process control and physical security computers
- Licensees have robust cyber security measures in place

Roadmap for Cyber Security at NPPs

- Pilot inspections completed:
  - ✓ Darlington in Q4 of 2014–15 and Bruce in Q3 of 2015–16
  - ✓ Revise inspection guide as appropriate and begin rollout of baseline inspection program for NPPs
- Baseline Inspections
  - ✓ Pt. Lepreau in Q4 of 2016-17
- In 2015, Canada hosted IAEA IPPAS Mission included Module 5 Cyber Security. Canadian cyber security at NPPs was thoroughly reviewed by IAEA.
- In 2015, CNSC required all NPP licensees to perform a gap analysis between their current cyber security programs and the requirements of N290.7, and to submit an implementation plan to resolve any identified gaps.
- In April 2016, all NPP licensees have submitted their gap analysis and implementation plan which are currently under CNSC staff's review.

Further Developments for Other Nuclear Facilities

- With publication of CSA N290.7, next phase has started for cyber security regulatory expectations to other major nuclear facility in Canada
  - ✓ In 2015, Canadian Nuclear Labs took transitional actions for preparing and submitting of an implementation plan in compliance with CSA N290.7 by the end of 2016.
- Importance of adopting a graded approach with risk-informed for smaller reactor facilities
- Review of applicability of CSA N290.7 (in whole or part) to other non-reactor facilities

Conclusion

- CNSC regulatory framework for cyber security has been developed
  - Regulatory documents, new CSA N290.7 Standard
- Compliant cyber security programs implemented by licensees at operating Canadian NPPs - gap analysis has been performed against CSA N290.7 and implementation plan is in place to resolve identified gaps
- Compliance verification activities of site cyber security programs are currently being rolled-out

Canadian Nuclear Safety Commission / Commission canadienne de sûreté nucléaire

Thank You!

nuclearsafety.gc.ca

facebook.com/CanadianNuclearSafetyCommission

youtube.ca/cnscccsn

twitter.com @CNSC_CCSN

Canada