Regulatory perspectives on software for nuclear applications

R. Lojk Director and **Z. C. Zeng** Specialist
System Engineering Division
Canadian Nuclear Safety Commission

Software Certification Consortium Workshop
McMaster University Software Certification Consortium
November 3, 2010
Markham, Ontario

Outline

1. The CNSC and the Regulatory Framework
2. CNSC Standards Framework
3. Software Certification
4. Separation of Control from Safety
5. Concluding Remarks
6. References

Canadian Nuclear Safety Commission

Established May 2000, under the ***Nuclear Safety and Control Act***

Replaced the AECB of the 1946 ***Atomic Energy Control Act***

Canada's independent nuclear regulator
64 years of experience

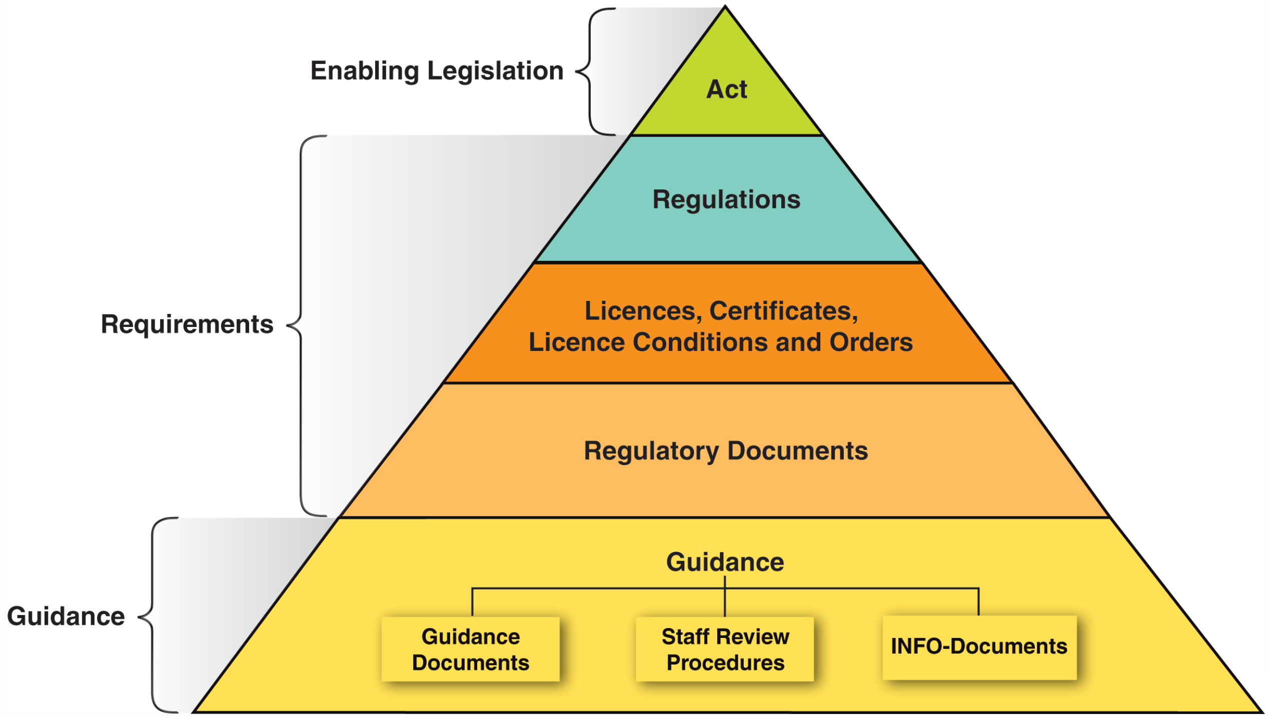
Our Mission Is Clear

Protect the health, safety and security of persons and the environment; and respect Canada's international commitments on the peaceful use of nuclear energy

Canada's nuclear watchdog

The Regulatory Framework

Elements of the Regulatory Framework



CNSC Standards Framework

International Standards:

- IAEA Safety Guide NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants.
- IAEA Safety Guide NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants.
- IEC 61513, Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems.
- ANSI/ISA-S67.04-Part I-2006, Setpoints for Nuclear Safety-Related Instrumentation
- IEC 60987, Nuclear power plants - Instrumentation and control important to safety - Data communication in systems performing category A functions, 2009-10.
- IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions

CNSC Standards Framework (cont'd)

National Standards:

- CAN3-N290.1-80 Requirements for the Shutdown Systems of CANDU Nuclear Power Plants
- CAN3-N290.4-11 Requirements for the Reactor Control Systems of Nuclear Power Plants
- CAN3-N290.6-M82 Requirements for Monitoring and Display of CANDU Nuclear Power Plant Status in the Event of an Accident
- N290.14-07 Qualification of pre-developed software for use in safety related instrumentation and control applications in nuclear power plants
- N286-05 Management system requirements for nuclear power plants

Industrial standard:

- CE-1001-Std (Rev. 2) Standard for Software Engineering of Safety Critical Software

CNSC Regulatory Document:

- RD-337, Design of New Nuclear Power Plants

The new reality

The number of software based Instrumentation and Control (I&C) systems is growing. They are replacing obsolete systems in refurbished plants and will service new nuclear power plants:

- Current analog systems being replaced with Programmable Logic Controller (PLC) and Field Programmable Gate Array (FPGA) based ones
- Reactor shutdown computers being replaced with emulators or replaced by FPGA based systems
- Plant control computers replaced with emulators or by FPGA systems
- New NPPs I&C systems will have to be computer based
- Software will be a mix new, re-configured, and previously-developed; and,
- Additional tools will be needed to develop and validate it

Software Certification considerations

How do you build confidence in software for safety systems?

- Apply software certification as required for other safety critical industries, i.e., aviation industry?
- Implement one European approach where independent third party assesses software-based safety systems (Reference [1] – Slide 18)?
- Require certification as done in Finland, where regulator requires all SC2 (safety class 2) equipments, including software, to be certified & also recommends that lower safety class software be certificated (References [2], [3] – Slide 18)?
- Require a structured approach?

Darlington Reactor Shutdown Systems

OPG's Darlington was the first fully digital nuclear power plant, early 90's, using computer-based reactor shutdown systems. The CNSC had concerns due to:

- Little prior experience anywhere with safety-critical software in nuclear applications
- Lack of established requirements and practices for stringent software quality assurance for such use
- Complexity of programming and software

CNSC directed OPG to re-write the software using formal methodology as a condition of full approval (References [4], [5] – Slide 18)

Darlington Reactor Shutdown Systems (cont.)

What did we learn:

- Regulators should participate from early stage so concerns are addressed
- Existing nuclear and industry standards not sufficient i.e., IEC 60880-2006
  - Software hazard analysis is neither mentioned nor required
  - Loose requirements such as “[t]ricks, recursive structures and code compaction should be avoided” (Principles for design and implementation 7.1.1.5)
- Gaps between regulator’s expectations and standards are not trivial (Reference [3] – Slide 18)
- Best practices are important but so are people, established procedures and formal methods

Software Certification: CNSC Perspective

We believe that software certification from a third party could provide:

- Confidence in the quality of the design process and product
- Confidence in the personnel involved
- Minimization of licensing uncertainty
- Potential for a reduction in licensing effort

But:

- The credential and independence of certification agent must be assured
- Targets of certification should be clearly defined, i.e., tool, application, 3rd party software, etc.
- The regulator still needs to have a good understanding of what is going on.

Software Certification: CNSC Perspective (continued)

It is important to note that:

- When different regulatory categorizations of safety systems exist, these set the risk profile and separate safety from process
- The adequacy of certification be carefully assessed, i.e., what is and is not certified, how it is certified
- Certification should reflect best practices of the nuclear industry and be benchmarked to best practices elsewhere
- There are legal implications associated with certification and decisions may not be straightforwardly technical (Reference [6] – Slide 18)

Separation of Control from Safety: CNSC's Position

All safety systems, including their hardware and software, need to be separated from control systems in order to:

- Ensure reliability and safety
- Reduce complexity
- Facilitate verification
- Protect the safety system from interference and carrying out its intended functions
- Meet Canadian and international regulatory requirements
- Ensure defence lines are not broken on the failure of control functions

Separating Control from Safety: Rationale

- Software is developed based on requirements associated with a given safety category
- Control functions are normally assigned to lower safety categories, therefore, less rigours requirements are applied to the development of control function software
- When control software is not separated from safety software or if separated but residing the same computer, using the same resources, IEEE 7-4.3.2 requires that the control function software be developed in accordance of safety system requirements.
- Different certification levels are used for safety (higher category) software and control (lower category) software

Separation Control from Safety: CNSC's Opinion

Combining safety and control has disadvantages which negate any saving:

- Need to conform with IEEE 7-4.3.2 §5.6 requirement
  - Higher certification level should be applied to control software
  - The amount of work for certification will increase exponentially
- Extra effort for developing control software (IEEE 7-4.3.2 requirement)
- Extra cost for certification
- Uncertainty for getting approval
  - Extra effort for convincing regulator to accept the design

Concluding Remarks

CNSC believes that:

- Software certification builds up the regulator's confidence in the product, and so can reduce licensing uncertainty and licensing effort
- Certification has multiple implications, therefore, decisions may not be straightforwardly technical
- Continuous communication with industry is vital to ensure that all concerns are adequately addressed
- The reliability and safety aspects of digital I&C systems at NPPs benefit from the separation of plant controls from plant safety systems

References

References used in this presentation:

[1] Common position of seven European nuclear regulators and authorised technical support organisations, “Licensing of safety critical software for nuclear reactors”

[2] STUK, YVL 5.5, “Instrumentation Systems and Components at Nuclear Facilities”

[3] J. Lahtinen, etc, “*Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain”, Computer Safety, Reliability, and Security,* Lecture Notes in Computer Science, Vol. 6351/2010

[4] G.H. Archinoff, etc, Verification of the shutdown software at the Darlington nuclear generating station. In International Conference on Control and Instrumentation in Nuclear Installations, 1990

[5] J. Rushby, Technical Report CSL-93-7 “Formal Methods and the Certification of Critical Systems”, 1993

[6] J. Hatcliff, etc., A software Certification Consortium and its Top 9 Hurdles, Electronic Notes in Theoretic Computer Science 238 (2009)

For More Information on the CNSC

CANADIAN NUCLEAR SAFETY COMMISSION 2009 – 10 ANNUAL REPORT

FACT: NUCLEAR IN CANADA IS SAFE.

Annual Report 2009–10

Home - Canadian Nuclear Safety Commission (CNSC) - Windows Internet Explorer provided by CNSC-CCSN
http://www.nuclearsafety.gc.ca/eng/
File Edit View Favorites Tools Help
Favorites BORIS NetPrint
Home - Canadian Nuclear Safety Commission (CNSC)
Google
Page Safety Tools
Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire
Canada
Canadian Nuclear Safety Commission
nuclearsafety.gc.ca
Français
Home
Contact Us
Help
Search
canada.gc.ca
Home > Canadian Nuclear Safety Commission (CNSC)
About CNSC
Commission Tribunal
Laws and Regulations
Licensees and Applicants
My Community
Environmental Assessments
Get Involved
Reading Room
Media Centre
Careers at CNSC
Key Links
Proactive Disclosure
Email this Page
Print this Page
We will never compromise safety
Stringent licensing conditions
Interactive Map
Mythbusters
CNSC 101: An Information Session for Stakeholders
How we ensure Canada's nuclear safety >
RSS
http://www.nuclearsafety.gc.ca/eng/#cont
Trusted sites
100%

Latest News

October 20, 2010

- Now available: Canadian Nuclear Safety Commission 2009-10 Annual Report
- CNSC verifying processes and procedures developed by AECL and LLRWMO for the soil remediation activities of properties in Port Hope

October 18, 2010

- Opportunity to file supplementary written submissions on Bruce Power's licence application to transport 16 steam generators by ship (PDF)

October 15, 2010

- The CNSC and Environment Canada have jointly released the 2008 Annual Report on Uranium Management Activities

Upcoming Public Meetings and Hearings

20 October 2010 (Hearing) >
22 October 2010 (Hearing) >
3 November 2010 (Meeting) >
9 December 2010 (Hearing) >
More >

Visit our Web site
nuclearsafety.gc.ca

Any questions?

nuclearsafety.gc.ca

Canada