Waste Safety Standards Committee

40th Meeting

2-3 November 2015

Agenda item W3.1

NST036 Technical Guide

Computer Security of I&C systems at Nuclear Facilities

Michael T Rowland

IAEA-NSNS (Information Management)
Nuclear Security Issues

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the IAEA Nuclear Security Series publications.
Nuclear Security Recommendations

• “present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals”

• Actually refer to “Fundamental Principles”, “recommended requirements” and similar high level recommendations

• Can’t call them requirements or use “shall”, but need to be *strong high level “should”*

• Purpose: “recommend measures that States need to take to achieve and maintain an effective nuclear security regime consistent with the Fundamentals”
“4.10. Computer based systems used for

- **physical protection**, 
- **nuclear safety**, and
- **nuclear material accountancy and control**

should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat.”
NSS Information and Cyber Related Guides

Fundamentals:
- NSS 20 Objective and Essential Elements of a State’s Nuclear Security Regime
  Objectives, Concepts, Principles

Recommendations:
- NSS No. 13 - Physical Protection of Nuclear Material and Nuclear Facilities
  (INFCIRC/225/Revision 5)

Implementing Guides:
- NSS No. 23-G Security of Nuclear Information

Technical Guidance:
- NSS 17 Computer Security for Nuclear Facilities
- NST036 Computer Security of Nuclear I&C Systems
Nuclear Security Series (NSS) vs. Safety Standards

• The IAEA-NSNS does not produce Nuclear Security Standards
• NSS publications do not contain “shall” or “must” requirements.
• Provide guidance documents focused on multiple tiers of support to the Member State
  • The State
  • The Competent Authorities (regulators, other government agencies)
  • The Licensees/Operators
• IAEA-NSNS has Practical Arrangement / Cooperation with
  • IEC committee SC45A/WG9
  • ITU
Document Objective:

- Nuclear Security Series Technical Guidance
- No formal interface requirement with Safety Committees (Technical Guidance)
- Provide guidance on computer security for Instrumentation and Control (I&C) systems at nuclear facilities (includes NPPs, RRIs, and FCFs)
- Includes safety and security considerations which have to be addressed in order to provide security throughout the life cycle of an I&C system
- This publication does not provide comprehensive guidance on the safety considerations for I&C systems.
Provides guidance on:

- The application of computer security measures to I&C systems which provide safety or auxiliary functions at nuclear facilities.
- Application of these measures to I&C systems providing Nuclear Security and NMAC functions.
- The role of computer security in protecting these systems from cyber-attacks.
- The relationship between computer security and safety
Document Background:

Meeting History
June 2012 - 1st Consultancy Meeting
Nov 2012 – 2nd Consultancy Meeting
Feb 2013– 3rd Consultancy Meeting
Sept 2013 – Technical Meeting
Mar 2014 – 4th Consultancy Meeting
Aug 2014 – 5th Consultancy Meeting
NST036 Computer Security of I&C Systems at Nuclear Facilities

- Nuclear I&C designers have processes in place to ensure systems provide for safe, reliable, and deterministic behavior.
- NST036 aims to integrate security measures into these processes to meet security objectives while maintaining safety.
- Joint review and development with International Electrotechnical Commission (IEC) experts.
NST036 discusses Security Controls across the system and component lifecycle (figure from DS-431)
NST036 Computer Security of I&C Systems at Nuclear Facilities

Comments combined from 120 day MS Review (April 2015):

Total Comments: 340

Accepted: 215 (mainly for clarity)

Accepted with modification: 44 (consistency with other IAEA publications)

Rejected: 77 (incompatible with other NSS guidance, other comments, unclear)

No Action Required (commentary and not editorial): 4

Comments from:

• Afghanistan, Canada, China, Cuba, Finland, France, Germany, India, Iran, Pakistan, Republic of Korea, Russian Federation, Slovakia, Spain, United Kingdom, United States
Safety Considerations for Computer Security Measures

Para 3.48:

- Allows for maintaining safety and while providing compensatory security measures on an interim basis. Consistent with similar guidance in DS-431.

- Current proposed text to 8th NSGC:

```
3.48. If there is a conflict between safety and security, then design considerations taken to assure safety should be maintained provided that a compatible solution to ensure security is pursued. Compensatory computer security measures should be implemented to reduce the residual risk to acceptable levels and be supported by a complete justification and security risk analysis. The implemented measures should not rely solely upon administrative controls for an extended period. The absence of a security solution should never be accepted.
```
7.102. SSR 2/1 Requirement 8 [1] states:

“Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.”

7.103. Neither the operation nor the failure of any computer security feature should adversely affect the ability of a system to perform its safety function. If there is a conflict between safety and security, then design considerations taken to assure safety should be maintained provided that a solution addressing the security risks is pursued. The acceptance of the absence of a security solution is strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.
Questions?

Michael T. Rowland
Nuclear Security Information Officer
International Atomic Energy Agency
Vienna International Centre
A-1400 Wien
Austria
Tel: +43 (1) 2600-26073
Fax: +43 (1) 2600-29299