38th Meeting of the Nuclear Safety Standards Committee

28 November 2014

Agenda item N3.3
NST036 Computer Security of I&C Systems

At Nuclear Facilities
Donald Dudenhoeffer, NSNS
Status of Technical Guidance

Safety Standards Series
- Safety Fundamentals
- Safety Requirements
- Safety Guide
- Safety Report

Nuclear Security Series
- Fundamentals
- Recommendations
- Implementing Guide
- Technical Guidance

Interface Group decides which are “interface documents”
Not “interface documents”
Document Objective:

- The objective of this document is to establish guidance addressing the application of computer security (CS) controls to I&C systems at nuclear facilities.
- The purpose of this report is to provide guidance on applying security controls in the unique environment of nuclear I&C systems.

Provides:

- Guidance on computer security controls implementation for instrumentation and controls systems at nuclear facilities. Current IAEA documents while discussing I&C systems from a safety standpoint, do not address the implementation of security controls within such systems.
- Operators with the framework for implementing computer security controls and to provide Competent Authorities with a framework for developing computer security assurance activities for licensees.
NST036 Computer Security of I&C Systems at Nuclear Facilities

- Nuclear I&C designers have robust processes in place to ensure systems provide for safe, reliable, and deterministic behavior.
- NST036 aims to overlay security considerations on top of these processes to meet safety and security objectives.
- Joint review and development with IEC experts.
NST036 Computer Security of I&C Systems at Nuclear Facilities

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 discusses Security Controls across the system and component life cycle (figure from DS-431)
Comment from NSGC review

- The NST036 Document for 120 day review will be submitted with an alternative text proposed by a Member State for consideration.

Current Text:

3.47. 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.

Alternative text to be likewise included for consideration:

3.47 (alternatively proposed text) Safety and security have to be achieved. The measures to achieve this aim may be altered, but the absence of a security solution should not be accepted.
Summary

- NST036 is a Technical Guide to support the implementation of computer security in the lifecycle of nuclear I&C systems.
- It is being presented to this committee due to its cross-cutting issues and also the high interest.
- The NSGC has approved the current version for Member State Review.
- Comments are welcome and should be submitted via the 120 day Member State Review process.
Questions?