www.holtec.com
www.smrllc.com

SMR-300 Cyber Security Strategy

August 13, 2024

Presented by: Patrick Essner

SMR, LLC, A Holtec International Company
Krishna P. Singh Technology Campus
One Holtec Boulevard
Camden, NJ 08104, USA

[Not Export Controlled]

Meeting Agenda

- Introductions
- Purpose & Outcome
- Guidance
- Overview of SMR-300 Cyber Security Strategy
- Open Forum

Purpose & Outcome

- Purpose
  - Provide a high-level overview of Holtec's approach and methodology for compliance with Cyber Security Regulations.
- Outcome
  - Obtain feedback from the NRC Staff on the approach to comply with regulations and the timelines for required submittals.

Regulation

- 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”
  - … provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat…

Guidance

- RG 5.71, “Cyber Security Programs for Nuclear Facilities”
  - provides guidance to applicants and licensees on acceptable methods for satisfying the requirements of 10 CFR 73.54.
  - contains regulatory positions that promote a defensive strategy consisting of a defensive architecture and a set of tailored security controls based on standards provided in the then current versions of NIST SP 800-53 and NIST SP 800-82.
  - divides the security controls into three broad categories: technical, operational, and management.
  - Where applicable, the NRC staff tailored the controls in NIST SP 800-53 and SP 800-82 to the unique environments of nuclear facility licensees and provided these more specific controls.

Guidance

- RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”
  - In July 2011, the NRC published Revision 3 of RG 1.152 to provide specific guidance to NPP licensees for use in the design, development, and implementation of protection measures for digital instrumentation and controls in safety-related applications.
  - It contains regulatory criteria for the evaluation of safety systems to ensure that identified security features are appropriately incorporated into systems and that the development environment is protected against the introduction of undocumented, unwanted code and any other coding that could adversely impact the operation of the safety systems.

Industry Guidance

- NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”
- NIST SP 800-82, “Guide to Industrial Control Systems Security,”
- NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors”
- NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule,”
- NEI 13-10, “Cyber Security Control Assessment”
- IAEA Nuclear Security Series No. 17-T, “Computer Security Techniques for Nuclear Facilities,”
- IAEA Nuclear Energy Series NR-T-3.30, “Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants,”

Submittal Requirements

- NUREG 0800, Section 13.6.6
  - The scope of the review is programmatic. The NRC staff does not review design information contained in the Cyber Security Program

- Question for NRC Staff
  - Is there any guidance on submittal requirements and/or level or detail for CPA stage of a Part 50 application?

SMR-300 Cyber Strategy

- Secure Development Environment
  - A life cycle approach described in RG 1.152 (IEEE 7-4.3.2-2016) is employed for use in the design, development and implementation of protection measures for CDAs in the I&C system to ensure
    - that identified security features are appropriately incorporated into systems
    - that the development environment is protected against the introduction of undocumented, unauthorized code and any other coding that could adversely impact operation of the system.

SMR-300 Cyber Strategy

- Defense in Depth Strategy
  - An acceptable defense-in-depth protective strategy comprises the following elements:
    - a defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level, and
    - a defensive strategy that employs multiple, diverse, and mutually supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack.

SMR-300 Defensive Architecture

- [[
  [[
-
  -
  -
  -
  -
  -
  -]]
  -]]

SMR-300 Security Controls

- [[

]]

[[

]]

Open Forum