Consultancy Meeting (CM)

Topic: Applying Security Controls to Instrumentation and Control Systems: Security and Safety Considerations

Date: 20-22 June (3 days)

Location: IAEA, Vienna Austria

IAEA POC: Donald Dudenhoeffer, d.dudenhoeffer@iaea.org, +43 (1) 260026424

The objective of this consultancy meeting is to address the application of computer security (CS) controls to Instrument and Control (I&C) systems at nuclear facilities. The CM will address not only discuss computer security controls for nuclear facility I&C systems, but will also examine considerations for nuclear safety systems and the potential implications of security controls on such systems. The output of this meeting is envisioned as a report on issues and areas requiring amplification, additional study and guidance from the IAEA to support the implementation of an integrated computer security program within the nuclear I&C framework.

This CM builds upon the framework of NSS 17, which presented an overview of nuclear facility computer security, but did not go into great detail for specific I&C computer security implementation. This CM will also address like comments requesting greater I&C guidance that evolved from the 120 day review of NSS 17 and from the Technical Meeting conducted in May 2011. Additionally the meeting will expand upon the computer security element provided in IAEA Nuclear Energy Series NP-T-3.12: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, SSR 2/1: Safety of Nuclear Power Plants: Design, and DS-431: Design of Instrumentation, Control Systems for Nuclear Power Plants, and DS-436: Instrumentation and Control and Software Important to Safety for Research Reactors.

The consultancy would consist of a group of 8-10 individuals consisting of both nation states and IAEA members.

Potential Meeting Topics/Issues to be discussed

- What is the state of current guidance? Standards?
    - What are some gaps in current guidance pertaining to CS for Nuclear I&C?
- Identification of I&C assets whose security is critical to facility safety
    - What is the relationship between security levels and safety classification?
- Considerations when allocating security controls to I&C systems
    - Concerns related to applying standard IT controls to I&C systems?
    - What controls must be applied within the I&C system?
    - How should access controls be implemented for operators, vs. maintainers, vs. other onsite personnel
- Types of interfaces between I&C and the outside world
    - How do threats and controls vary depending type of interface, e.g., network, portable memory, maintenance computers, direct human input?

    - Is it necessary to consider possibility of remote operation, e.g., severe accident bunker, small modular reactors, emergency facility data requests?
- Considerations for implementing controls within I&C systems
    - Unique challenges for CS controls implementation?
    - Is special treatment needed for features that implement both CS controls and safety strategies?
    - Technology dependencies, e.g., computer vs. FPGA based systems?
- CS implications on I&C architecture
    - Need for a separate security watchdog that can monitor I&C but not affect its behaviour?
    - Features needed for independence between different CS levels and their relationship to features for independence between different safety classes?
- What is the potential impact of CS on I&C Systems and vice versa?
    - Need to consider CS controls in defence in depth and diversity analysis for new plants, and for operating plants?
- Control of the development environment
    - For development of I&C software?
    - For development of configuration data, e.g., protection set points, calibration constants,
- Responses to suspected penetration.
    - Conservative action even if possible false alarm?
- Differences between power plants, research reactors, and fuel cycle facilities that would affect CS design and implementation
- Considerations for new-builds and plant modernization.