Minor Report Meeting

Security Standards Convergence and Relevance in Process Control Systems

19-05-2009

Presentation Overview

- Security analysis
  - Reasons
  - Scope and Objectives
- Standards Review
  - ISA-99 Review
  - NERC-CIP: a comparison with ISA-99
  - IEC-62351: a comparison with ISA-99

Security Analysis

Reasons for CERN security strategy

- Integration of control systems devices into “traditional” IT systems
- Manufacturers include more and more IT functionalities into their devices
- A growing interconnectivity between the fabric level and the management one
- Lack of standards and guidelines to ensure the robustness of any control system
- Lack of PLC security evaluations made at CERN
- Recovery from attacks usually is very expensive in terms of time, cost and effort

Scope and Objectives

- Discovering and exploiting the vulnerabilities of control system devices
- Addressing the areas of improvements
- Establishing a procedure which have to be performed to obtain a general overview of the security of any device
- Suggesting a guideline to improve the level of security
- Pointing out the most common weak points and the vulnerabilities of devices
- Underlining the security grade reached in the process control field

Standards Review

ISA-99 Review

- Benefits and Drawbacks of the general approach
- Definition of common language
- Process Control Systems and IT Systems
- Improvements in the authentication process
- Importance of the testing phase
- Auditing in Process Control Devices
- How to apply the risk analysis
- Do not use “obscure network protocol”
- Integration
- A dynamic standard
- An incomplete Defense-in-depth strategy

NERC-CIP: a comparison with ISA-99

- Different scopes and targets
- Identification of the critical assets
- Access control model
- Define a security perimeter
- Updating the security plan
- Violation Severity Levels
- What about the physical security

IEC-62351:
a comparison with ISA-99

- Mechanisms to secure some SCADA protocols: IEC 60870-5, DNP3, IEC 60870-6 (TASE.2 and ICCP), and IEC 61850
- Relevance of authentication operations
- strictly connected to security impacts on power systems
- The IEC 62351-7: enhancement of overall management of the communications networks supporting power system operations
- Definition of the “Security Domain”
- Data objects
- A similar risk analysis

Conclusions

- ISA-99 seems to be the more general and suitable standard for any kind of Process Control Systems
- Lots of points in common among the analyzed standards
- Continuous refactoring of the standards because of the discovering of new vulnerabilities and the use of new technologies
- Presence of security lacks in many aspects of PCSs: tools and technologies PCS-oriented, specific security patterns, developing of security analysis techniques…