André Lochthofen, Dagmar Sommer (GRS)

Implementation of Computer Security at Nuclear Facilities in Germany

Outline

- Introduction
- Requirements for computer security in German nuclear facilities
- Implementation of computer security at nuclear power plants
  - Basis for GRS assessments concerning computer security
  - Examples of these assessments
- Conclusion

Outline

- Introduction
- Requirements for computer security in German nuclear facilities
- Implementation of computer security at nuclear power plants
  - Basis for GRS assessments concerning computer security
  - Examples of these assessments
- Conclusion

Introduction (1 / 2)

- The operational and safety-related components of German NPPs are often in use since their commissioning in the 1970ies / 1980ies
  - Components reach their end of lifetime

  ↳ Replacement of these “old” components is expected

- A replacement with identical components is not always possible or even not wanted
  - Procurement of spare parts is getting more and more difficult
  - Process optimisation due to the use of modern software-based (smart) components

  ↳ Increasing integration of software-based technology into safety, safety-related and security systems throughout the plants is expected

⇨ The threat of malevolent interferences and cyber-attacks is rising, so that nuclear security can be seriously endangered

Introduction (2 / 2)

- Cyber-attacks are already in progress in process automation
  - Malicious software “stuxnet” - manipulation of SCADA-systems (2010)
  - Malicious software “duqu” - collecting of information (2011)
  - Malicious software “flame” - spying out of systems / operators (2012)

  ↳ Overall more than 10.000 new malicious software per day can be seen

- Maintaining the nuclear security of NPPs
  - Conventional physical protection measures and
  - Protection measures in the field of computer security

⇨ Existing security management process has to be expanded to computer security aspects

Outline

- Introduction
- Requirements for computer security in German nuclear facilities
- Implementation of computer security at nuclear power plants
    - Basis for GRS assessments concerning computer security
    - Examples of these assessments
- Conclusion

Requirements for computer security in German nuclear facilities

- Highest legal requirement: “Act on the Peaceful Utilization of Atomic Energy and the Protection against its Hazards (Atomic Energy Act)”
  - Security: §7 para. 2 no. 5 “A license may only be granted if the necessary protection against disruptive actions or other interferences by third parties is ensured.”

    ⇨ German Cyber Design Basis Threat (German cyber DBT)

    ⇨ German Guideline for the Protection of IT Systems in Nuclear Plants and Facilities of Protection Category I and II against Disruptive Actions or other Interferences by Third Parties (German computer security guideline)
  - GRS information notice concerning the malicious software “stuxnet” (WLN 2010/07)

German cyber DBT

- Confidential document (published in 2013)
- Based on a threat assessment by competent authorities
  - Which attacks can lead to unacceptable consequences?
- Not scenario-based => set of characteristics
  - Important characteristics of cyber-attackers and cyber-attacks
    - ↳ Cyber-attacks can be combined with non-cyber-attacks (e.g. for information gathering)
    - ↳ Attacks can consist of several steps
    - ↳ One attack may hit many targets at different places
    - ↳ Attacker may act from a far remote place

German computer security guideline (1 / 2)

- Restricted document (published in 2013)
- Requires the protection of all software-based systems of a facility which may be used for malicious actions (i.e. also office systems)
- Definition of a computer security objective
- Introduction of a computer security organisation
  - Appointment of a computer security officer (CSO)
- Introduction of a computer security concept
  - Structure analysis of all existing software-based systems / structures
  - Protection of software-based systems according to 4 computer security levels
  - Grouping of software-based systems with the same computer security level into computer security zones

German computer security guideline (2 / 2)

- Requirements for computer security measures
  - General requirements
  - Computer security level-dependent requirements
  - Computer security zone-dependent requirements

↳ For the technical realisation, it should be noted that Computer security measures can be of organisational, structural or technical manner

- Requirement for the facilities to perform a basic security check and a supplementary security analysis
- Responsibility to apply computer security measures also for supply chains, for external services and for remote maintenance access connections

GRS information notice concerning the malicious software “stuxnet” (WLN 2010/07)

- Cyber-attacks with “stuxnet” have affected the type of industrial control systems, automation systems and SCADA systems by Siemens that are also installed in German NPPs
- Main topics of GRS recommendations:
  - Identification and analysis of possible infected software-based and industrial control systems
  - Elimination of potential “stuxnet”-infections
  - Review and adaptation of user rights to a minimum
  - No internet access for industrial control systems
  - Development of a computer security concept to maintain the nuclear security
- Based on the information available at GRS, no German NPP was infected by “stuxnet”

Outline

- Introduction
- Requirements for computer security in German nuclear facilities
- Implementation of computer security at nuclear power plants
  - Basis for GRS assessments concerning computer security
  - Examples of these assessments
- Conclusion

Basis for GRS assessments concerning computer security (1 / 3)

- Assessments based on a GRS-best-practice-approach
  - Several assessments in the field of computer security at German NPPs
  - Involved in the development of the German computer security guideline

  ↳ Aim: Ensuring the protection against disruptive actions or other interferences by third parties

- Expanding the existing security management process of NPPs to computer security aspects
  - Integration of a computer security organisation (structures / roles)

    ↳ Tasks / responsibilities / powers of a computer security officer
  - Development and introduction of a computer security concept

    ↳ Graded approach of 4 computer security levels and security zones

Basis for GRS assessments concerning computer security (2 / 3)

- Computer security concept
  - Structure analysis documents all existing software-based systems including their structures and network topology
  - Assignment of one computer security level to each system
  - Possible to summarize systems with the same computer security level in one computer security zone

    ➯ Computer security measures can be placed at zone borders, so that in this case not every system needs all computer security measures separately
  - Conducting a basic security check and a supplementary security analysis according to the computer security level
  - Determination of specific computer security measures

    ➯ Highest protection for the highest computer security level,…

Basis for GRS assessments concerning computer security (3 / 3)

- Examples of computer security measures:
  - Prohibition of data links into the highest computer security level
  - Prohibition to connect private technology (e.g. mobile phones) to plant systems and to use plant systems for private purposes
  - Regulated access to software-based systems
    - ➩ Strict user identification (e.g. ID card and biometric feature)
    - ➩ User access restriction
  - Usage of the two-person-principle (e.g. against an internal attacker)
- In addition, also conventional physical protection measures have to be installed to protect the software-based systems (e.g. entrance limitation)

Example 1: Implementation of a computer security concept at a NPP (1 / 2)

- Review: The appropriate documents, the organisational structure, the derivative of the necessary protection requirements and the technical realisation of the computer security measures were reviewed in respect to the GRS-best-practice-approach:
  - Integration of a computer security organisation including CSO
  - Definition / explanation of the requirements of the computer security concept
    - ➯ Structure analysis
    - ➯ Computer security levels and computer security zones
    - ➯ Important tasks and responsibilities of staff members
    - ➯ And other aspects like for example life cycle, handling of mobile equipment, regulation of user accesses,…

Example 1: Implementation of a computer security concept at a NPP (2 / 2)

- Conceptual assessment: Verification of the documented requirements according to the GRS-best-practice-approach
- Technical assessment (audit): Review of the technical realisation
  - Extensive discussions of open points and disagreements between reviewers, plant staff, and state authority

⇨ Approval of the computer security concept

Example 2: Displacement of plant applications into an external computer centre (1 / 2)

- First step: Approval of the conventional physical protection measures of the computer centre building
- Second step: Review of the computer security organisational and personal procedures as well as their technical realisation in the computer centre in respect to the GRS-best-practice-approach
  - Transfer of the computer security measures from the applications into the computer centre environment
  - Transfer of the security objectives from the plant to the computer centre
  - Definition and protection of the network area used by the plant and located in the computer centre
- Internal (by the plant) and external (by the reviewer) audits

Example 2: Displacement of plant applications into an external computer centre (2 / 2)

- Measure-example: Integration of the two-person-principle in the procedures of the computer centre due to technical solutions:
  - Electronic locks at the doors to secure that at least two persons go into the room
  - Room monitoring systems for a visual control of the entrance
  - Specially protected computer security racks
  - Restricted user accesses in combination with strict user identifications
  - Separation of data administrator rights (one administrator may not have an access to two associated networks)

⇨ Approval of the entire displacement

Example 3: Implementation of a software-based trunked radio system for the physical protection division of a NPP (1 / 3)

- At the initial point, the NPP had already implemented a computer security concept
- Structural analysis: All components and data connections of the trunked radio system were checked
  - Main software-based part for normal operation (“normal system”)
  - Non-software-based part used as backup system (“backup system”)
  - Remote maintenance access connection
- Determination of computer security requirements: The trunked radio system was assigned to a computer security level
  - Normally for systems of the physical protection division the second highest computer security level had to be chosen

    ↳ Impossible due to structural and organisational defaults

Example 3: Implementation of a software-based trunked radio system for the physical protection division of a NPP (2 / 3)

- Result of further assignment discussions:
  - ➪ “backup system” was assigned to the second highest level
  - ➪ “normal system” was assigned to a level with less need for protection

- Basic security check and supplementary security analysis:
  - Implementation of level-related computer security measures for the “normal system” and the “backup system”
  - For the “normal system” also some additional “higher” computer security measures had to be implemented (e.g. protection of the remote maintenance access connection)

Example 3: Implementation of a software-based trunked radio system for the physical protection division of a NPP (3 / 3)

- Realisation:
  - The requirements of the computer security measures for the “normal system” were fulfilled by the existing computer security measures due to the computer security concept
  - The requirements of the additional “higher” computer security measures for the “normal system” were implemented (e.g. decoupling measures for the remote maintenance access connection)
  - Resulting from the fact that the “backup system” is not software-based, the corresponding requirements were fulfilled due to the existing conventional physical protection measures

⇨ Approval of the implementation of the software-based trunked radio system

Outline

- Introduction
- Requirements for computer security in German nuclear facilities
- Implementation of computer security at nuclear power plants
  - Basis for GRS assessments concerning computer security
  - Examples of these assessments
- Conclusion

Conclusion (1 / 2)

- An increasing amount of analogue (not software-based) components is already or will be replaced by software-based components
  - Thus the threat of malevolent interferences and cyber-attacks via these components to the plants also increases

    ⇳ In addition to the conventional physical protection of a NPP also the computer security must be considered in order to maintain the nuclear security

- Requirements for computer security in German NPPs
  - German cyber design basis threat
  - German computer security guideline
  - GRS information notice concerning “stuxnet” (WLN2010/07)

Conclusion (2 / 2)

- Assessments concerning computer security based on the GRS-best-practice-approach
- Expanding the existing security management process of the NPPs to computer security aspects
  - Integration of a computer security organisation (structures / roles)

    ↳ Tasks / responsibilities / powers of a computer security officer
  - Implementation of a computer security concept

    ↳ Graded approach of 4 computer security levels and security zones
- Examples of the implementation of computer security at NPPs
  - Implementation of a computer security concept
  - Displacement of plant applications into an external computer centre
  - Implementation of a software-based trunked radio system

Thank you for your attention

IAEA Nuclear Security Series No. 17
"Computer Security at Nuclear Facilities"

- Technical guidance published in 2011 by IAEA
- Specific guidance to nuclear facilities on implementing a computer security programme and advices on evaluating existing programmes
  - Approaches, structures and implementation procedures
- Introduction of a computer security organisation (including a computer security officer)
- Approach with 5 computer security levels and possible computer security zones
- IAEA intends to work on more documents for computer security in nuclear facilities in the near future