The German Guideline for the Protection of Computer Systems in Nuclear Facilities and the Assessment of its Implementation

Uwe Stoll, Dagmar Sommer, GRS

Third International Regulator‘s Conference on Nuclear Security

Marrakech, 1 - 4 October 2019

Outline

- Introduction
- Requirements for Computer Security in Germany
- GRS Experience in Implementation of Computer Security in German Nuclear Facilities
- GRS Experience in the Assessment of Computer Systems in German Nuclear Facilities
- 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 ongoing
- 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 components
  - ↳ Increasing integration of software-based technology into safety, safety-related and security systems throughout the plants

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

Introduction (2 / 2)

- Cyber-attacks on industrial control systems (ICS) in recent years:
  - **Stuxnet** - manipulation of ICS systems (2010)
  - **Havex** - collecting configuration data of ICS systems (2014)
  - **Blackenergy-** manipulation of control systems for electrical grid in Ukraine (2015)
  - **CrashOverride** – manipulation of ICS systems in Ukraine (2016)
  - **Triton** – manipulation of ICS systems

  ↳ About 800 million known malicious software

  ↳ About 390.000 new variants per day

- Maintaining the nuclear security of nuclear facilities
  - 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

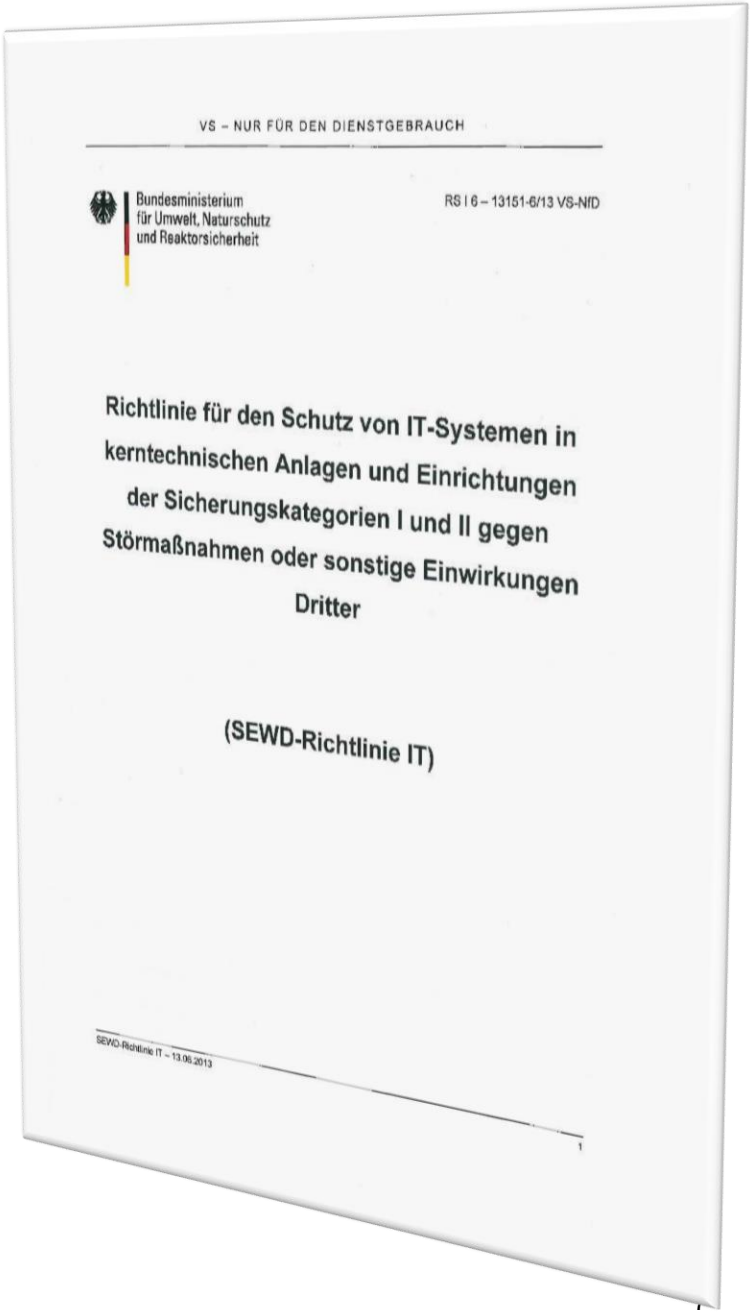
- Introduction
- Requirements for computer security in Germany
- GRS experience in implementation of computer security in German nuclear facilities
- GRS experience in the assessment of computer systems in German nuclear facilities
- Conclusion

German Cyber Design Basis Threat (cyber DBT)

- Confidential document (announced 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
    - Blended attack (Cyber-attacks 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 at the same time
    - Attacker may act from a far remote place

German Malicious Acts Guideline IT (1 / 3)

- Guideline for the Protection of IT Systems in Nuclear Plants and Facilities of Protection Category I and II
- Restricted document (announced in 2013)
  - Relevant for nuclear facilities with protection category I and II such as NPPs, interim storage facilities
  - Definition of one computer security objective
  - Definition of the term “computer system”
- Requirements:
  - Protection of all computer systems of a nuclear facility which may be used for malicious actions (i.e. also office systems)
  - Introduction of a computer security organisation
    - Appointment of a computer security officer (CSO)


VS – NUR FÜR DEN DIENSTGEBRAUCH

Bundesministerium
für Umwelt, Naturschutz
und Reaktorsicherheit

RS I 6 – 13151-6/13 VS-NfD

Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter

(SEWD-Richtlinie IT)

SEWD-Richtlinie IT – 13.06.2013

1

German Malicious Acts Guideline IT (2 / 3)

- Introduction of a computer security concept
  - Structure analysis of all existing computer systems, their structures and the entire network topology
  - Protection according to four graded computer security levels
  - Allocation into computer security zones

- Generic requirements for computer security measures
  - General requirements
  - Computer security level-dependent requirements
  - Computer security zone-dependent requirements
  - ↳ Computer security measures can be of organisational, structural or technical manner

German Malicious Acts Guideline IT (3 / 3)

- Requirement for the facilities to perform a basic security analysis and a supplementary security analysis (depending on the security level)
- Consideration of the whole life cycle of computer systems
- Responsibility to apply computer security measures also for supply chains, for external services and for remote maintenance access connections

Outline

- Introduction
- Requirements for computer security in Germany
- GRS experience in implementation of computer security in German nuclear facilities
- GRS experience in the assessment of computer systems in German nuclear facilities
- Conclusion

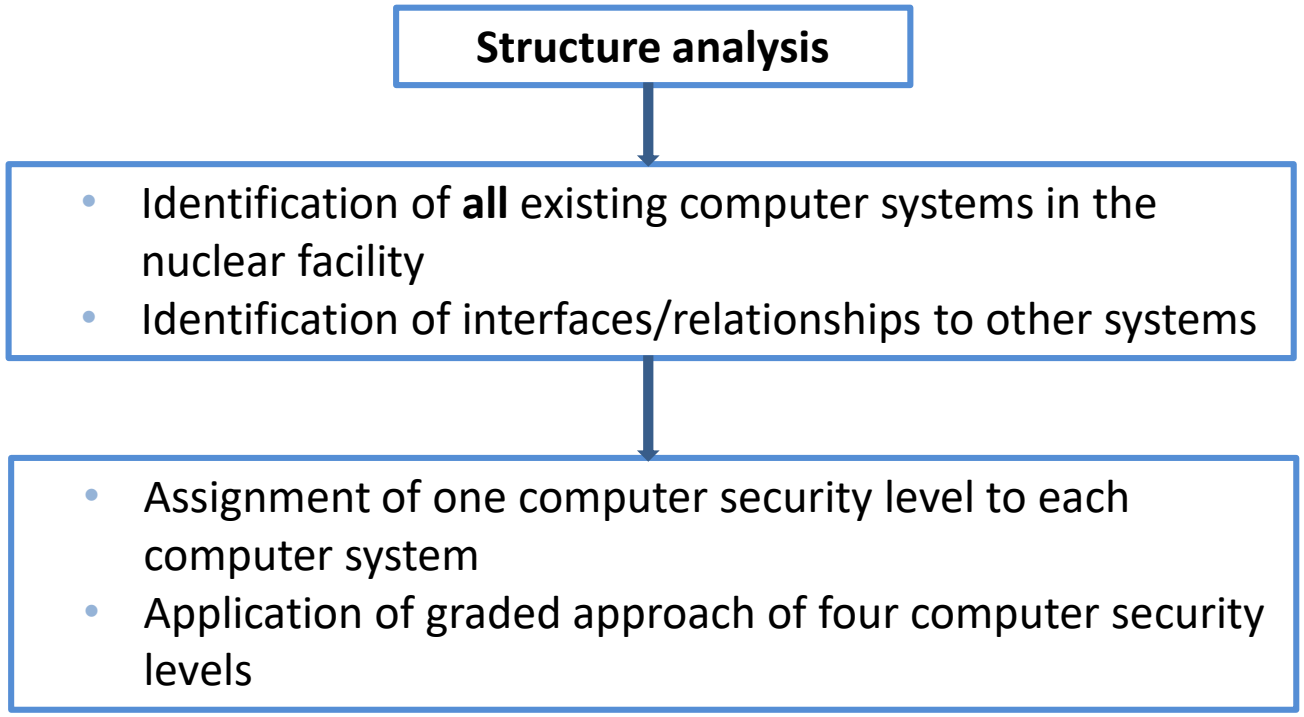
GRS Experience in Implementation of Computer Security in German Nuclear Facilities (1 / 4)

- Development / Implementation of a **computer security management process**
  - Definition of
    - appropriate procedures,
    - necessary organisational structures,
    - resources and
    - management principles regarding to computer security

- Integration of a computer security organisation (structures / roles)
  - Introduction of a **computer security officer** (CSO)
  - Definition of tasks / responsibilities / powers
  - Advantage: CSO is under the control of the head of the facility security

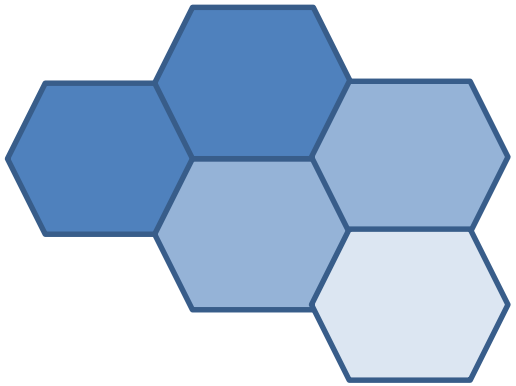
GRS Experience in Implementation of Computer Security in German Nuclear Facilities (2 / 4)

- Development and introduction of a computer security concept



↳ Germany: Predetermination of computer security levels for different computer systems of the NPPs

GRS Experience in Implementation of Computer Security in German Nuclear Facilities (3 / 4)



- Introduction of computer security zones
  - Possible to summarize computer systems with the same computer security level in one computer security zone

  ↳ Advantage: 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 analysis and a supplementary security analysis according to the computer security level
- Determination / consolidation / implementation of specific computer security measures
  - Highest protection for the highest computer security level,…
  - Basic protection for the lowest computer security level

GRS Experience in Implementation of Computer Security in German Nuclear Facilities (4 / 4)

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

Outline

- Introduction
- Requirements for computer security in Germany
- GRS experience in implementation of computer security in German nuclear facilities
- GRS experience in the assessment of computer systems in German nuclear facilities
- Conclusion

Example 1: Implementation of a computer security concept at a NPP

- Assessment aspects: Review of
  - appropriate documents,
  - organisational structure,
  - derivative of the necessary security requirements and
  - technical realisation of the computer security measures
- Conceptual assessment: Verification of the documented requirements
- Technical assessment: Review of the technical realisation
  - Extensive discussions of open points and disagreements between licensee, regulator and reviewers

⇨ Approval of the computer security concept of the plant

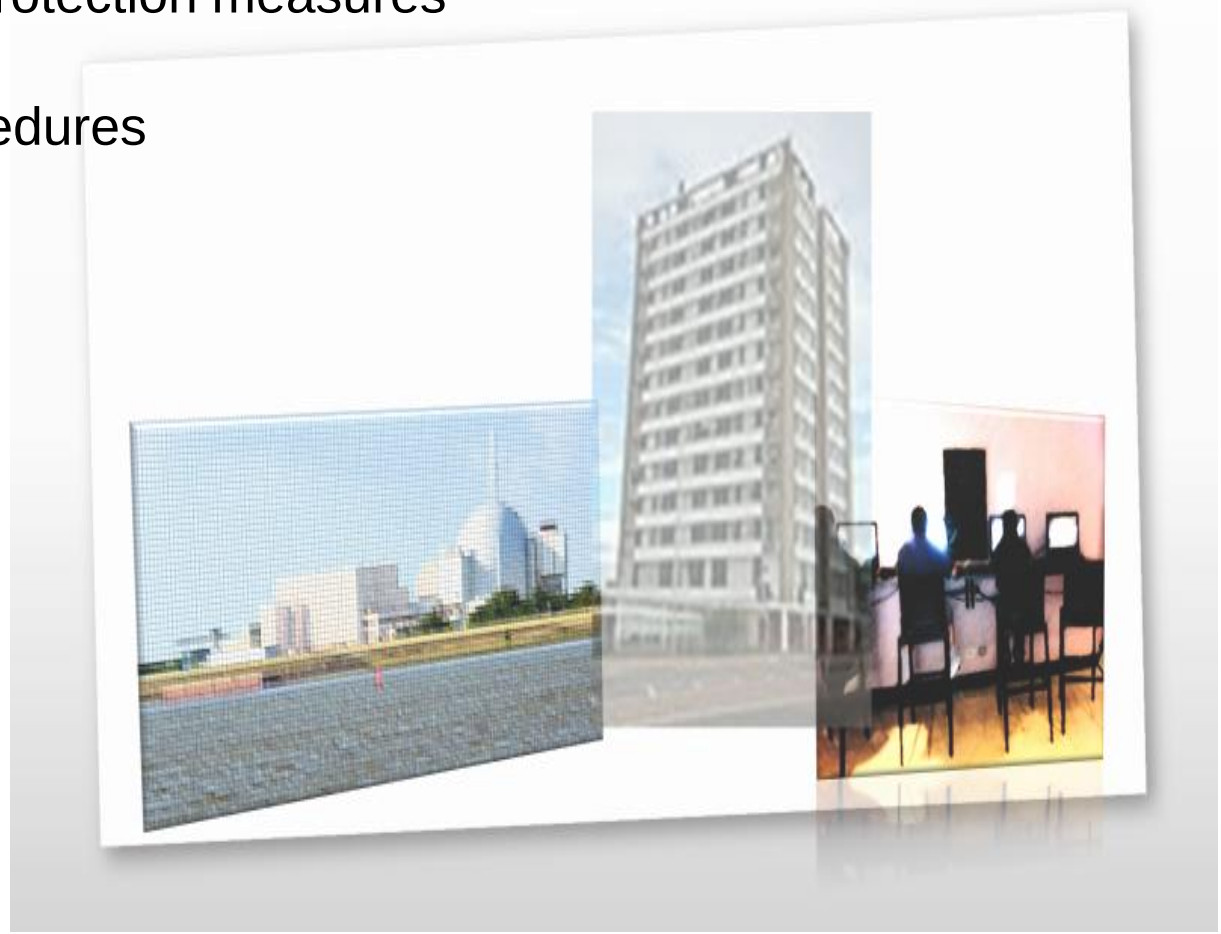
Example 2: Outsourcing of plant computer systems to an external data centre (1 / 3)

- First step: Approval of the physical protection measures of the building
- Second step: Review of the computer security organisational and personal procedures as well as their technical realisation
  - Transfer of the security (physical and computer) objectives from the plant to the data centre
- Major focus: Communication between plant and data centre
  - Data connection with strong encryption technology that spans end-to-end
  - Dedicated network line
- Completion: Internal (by the plant staff) and external (by the reviewer) review to assess the different protection and security measures

  ↳ Advantage: Periodically repetition of these reviews to maintain the achieved protection degree

Example 2: Outsourcing of plant computer systems to an external data centre (2 / 3)

- Examples of possible computer security / physical protection measures
  - Integration of the two-person-principle in the procedures of the data centre due to technical solutions
    - Electronic locks at the doors to secure that at least two persons go into the room
    - Specially protected computer security racks
    - Restricted user accesses in combination with strict user identifications
    - Specific data administrator rights for different persons



Example 2: Outsourcing of plant computer systems to an external data centre (3 / 3)

- Minimal functionality for both software and hardware
  - Software of servers and clients
  - Network connections between the computer systems
  - Users, administrators and their access rights on the computer systems

⇨ Approval of the whole outsourcing process

  - Allowed traffic through firewalls

Example 3: Implementation of an IP-based leased line between plant security and police (1 / 2)

- Intention: Migration of the (analogue) leased line system between the plant security and the police to a computer system (incl. IP-protocol)
  - Maintenance of the analogue leased line system by the line operator ends
- Basis: Leased line system is an important component for the plant security
  - Requirements to protect this system are high
  - Operated by a third party (not under the nuclear regulatory control)
- Examples of computer security measures
  - Strongly encrypted communication between both partners
  - Limited administrative access to the communication systems
  - Detection of an information security loss in between the communication partners

Example 3: Implementation of an IP-based leased line between plant security and police (2 / 2)

- Challenge: Complete assessment of an extensive firewall systems cannot be achieved during such a review process
  - Consideration of internationally accepted security assessment certificates
    - "Common Criteria for Information Technology Security Evaluation" provide lots of requirements concerning computer security management and used technologies
  - Examination of the unique aspects for the nuclear security

↳ Advantage: The amount of reviewing can be reduced and the transparence of the reviewing process is strengthened

⇨ Approval of the implementation of the IP-based leased line

Outline

- Introduction
- Requirements for computer security in Germany
- GRS experience in implementation of computer security in German nuclear facilities
- GRS experience in the assessment of computer systems in German nuclear facilities
- Conclusion

Conclusion (1 / 2)

- Increasing number of cyber-attacks on industrial control systems (ICS) in recent years
- An increasing amount of analogue (not software-based) components in nuclear facilities is already or will be replaced by software-based components
  - Thus the threat of malevolent interferences and cyber-attacks via these components to the nuclear facilities also increases
    - ↳ In addition to the 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 and certain nuclear facilities
  - German cyber design basis threat
  - German Malicious Acts Guideline IT

Conclusion (2 / 2)

- GRS experiences in implementation of computer security
  - Expanding the existing security management process of the nuclear facilities to computer security aspects
    - Integration of a computer security organisation (structures / roles)
      - Tasks / responsibilities / powers of a computer security officer (CSO)
    - Implementation of a computer security concept
      - Graded approach of four computer security levels and security zones
- GRS experiences in the assessment of computer systems
  - Implementation of a computer security concept
  - Outsourcing of plant computer systems into an external data centre
  - Implementation of an IP-based leased line

Thank you for your attention!

Any questions?