

R. Grinzinger – C. Versteegen – H. Heinsohn

Software-based instrumentation and control in nuclear power plants – requirements for physical protection

Content

- Increasing networking of IT systems in NPPs in the context of physical protection
- GRS projects to secure IT networks of NPPs
- Derivation of requirements for physical protection of IT systems (including Instrumentation & Control systems) in NPPs
- Demonstration procedure
- Lessons learned
- Summary

Current situation of IT systems in German NPPs

Various features may be present in NPPs:

- Use of Internet in NPPs
- Use of digital Instrumentation & Control (I&C) systems for safety related functions
- Remote access of digital I&C systems
- IT outsourcing by licensees
- At the work places inside the NPP, digital I&C systems can be connected with the IT network of the NPP
- Connection of information systems of the security area (e.g. access control system) with other operational IT systems (e.g. integrated operation management system)

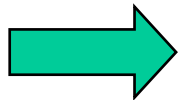
 New requirements for the IT security of NPPs are necessary

GRS projects to secure IT networks of NPPs on behalf of the Länder authorities

- Assessment of IT security measures for IT networks of NPPs due to the introduction of Internet connections
- Assessment and annual review (e.g. audit) of the IT security concept
- Assessment of the rearrangement of integrated operation management systems to a client-server architecture and outsourcing of data centres to external service providers at the same time
- Assessment of the replacement of hard-wired I&C systems with digital ones
 - Exchange of reactor power I&C system
 - Exchange of parts of safety related I&C system

Legal requirements for physical protection of NPPs in Germany

- Detailed requirements for IT security in NPPs do not exist
- Atomic Energy Act (Atomgesetz § 7 para. 2 no. 5):
“The licence may only be granted if the requisite protection against malevolent disruptive acts or other third-party intervention is ensured.”
- Guideline for the physical protection of NPPs (restricted)
- Design basis threat (confidential)



Derivation of a graded system of protection requirements for IT systems in NPPs and design basis IT threats

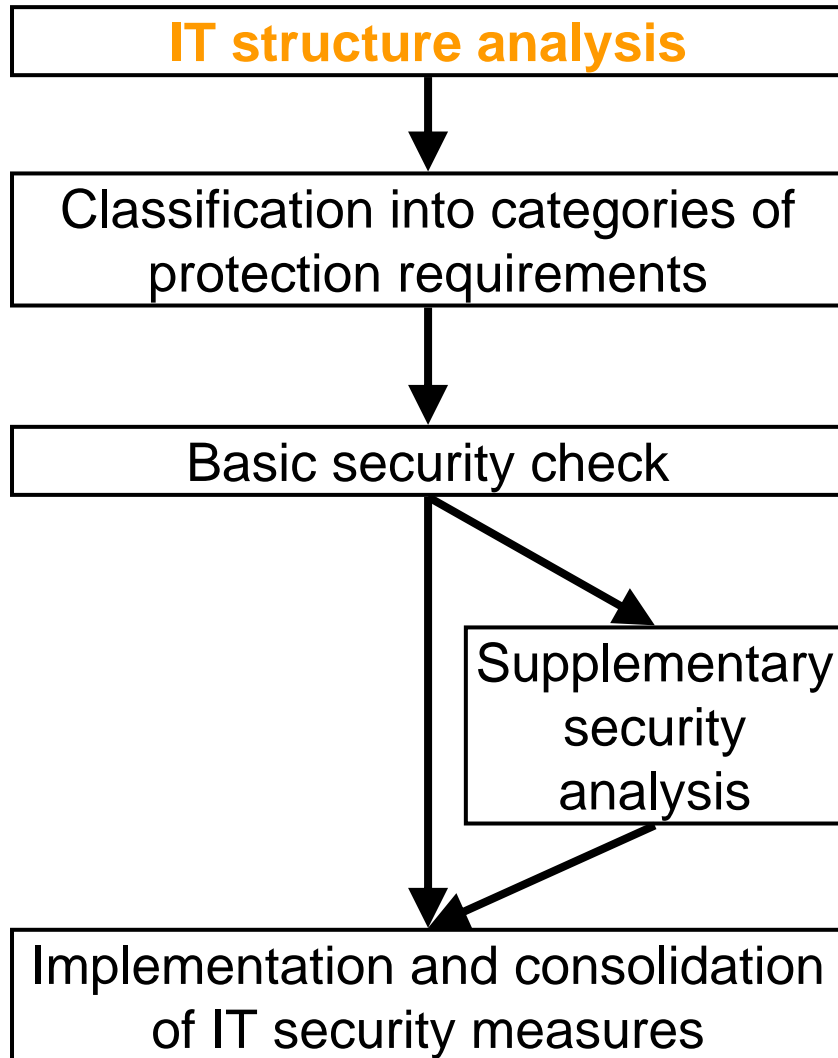
Graded protection requirements for I&C systems in NPPs derived from the guideline for the physical protection of NPPs by GRS

- Protection requirements category “very high”
 - I&C systems that may be used for the release of substantial amounts of radioactive materials
 - unauthorised access must be avoided, detected and documented
- Protection requirements category “high”
 - I&C systems that may be used for the demand of systems according to I&C systems of category “very high” or
 - information, data and applications in IT systems that may be used for the direct support of the release of substantial amounts of radioactive materials
 - unauthorised access must be hindered, detected and documented
- Protection requirements category “normal”
 - information and data of the IT systems that may be used for the preparation of a release of substantial amounts of radioactive materials
 - unauthorised access must be detected and documented

Design basis IT threats for IT systems of NPPs derived from the common design basis threat by GRS

- Threat by an outsider IT attacker
 - Attack via the Internet using any available computers and skills
- Threat by an insider IT attacker
 - Attack by an authorised competent user of the NPP's IT network
- Threat by a combination of an insider IT attacker with an outsider IT attacker
 - Insider IT attacker supports outsider IT attacker in overcoming the IT barriers in the NPP's IT network.

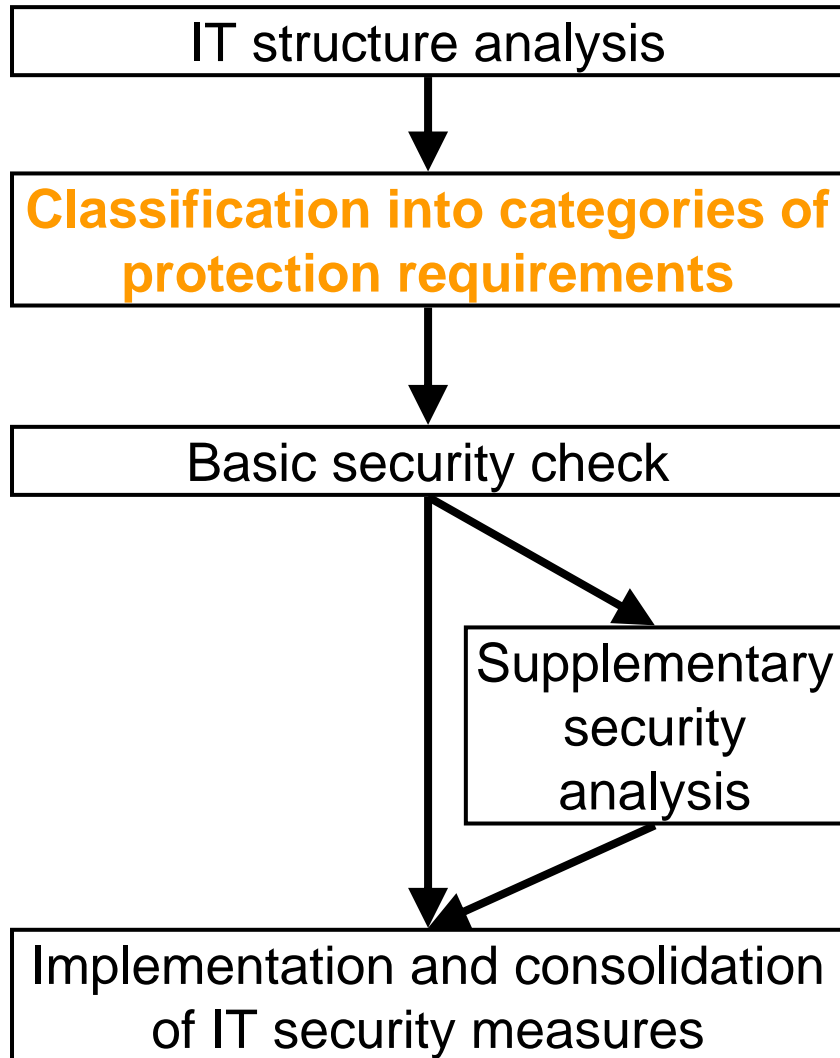
Demonstration procedure for physical protection of IT systems in NPPs (following BSI-Standard 100-2)



IT structure analysis

- Analysis and documentation of the structure of the existing IT systems
- Compiling a network topology plan
- Consideration of e.g.
 - existing infrastructure
 - networked and stand-alone IT systems
 - communication links between the IT systems and with the external world
 - underlying organisational and personal situation

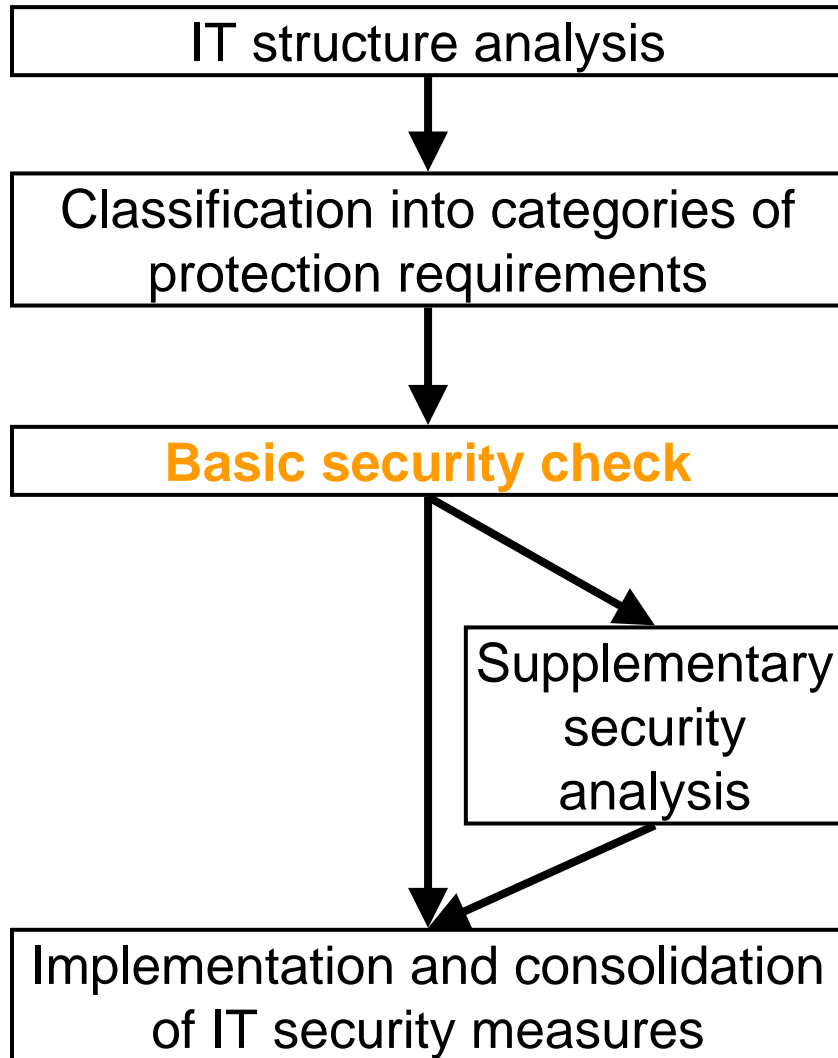
Demonstration procedure for physical protection of IT systems in NPPs (following BSI-Standard 100-2)



Classification into categories of protection requirements

- Classification of the IT systems into the three protection requirement categories
 - category “very high”, e.g.
 - protection and safety actuation system
 - category “high”, e.g.
 - limitation system
 - category “normal”, e.g.
 - documentation system

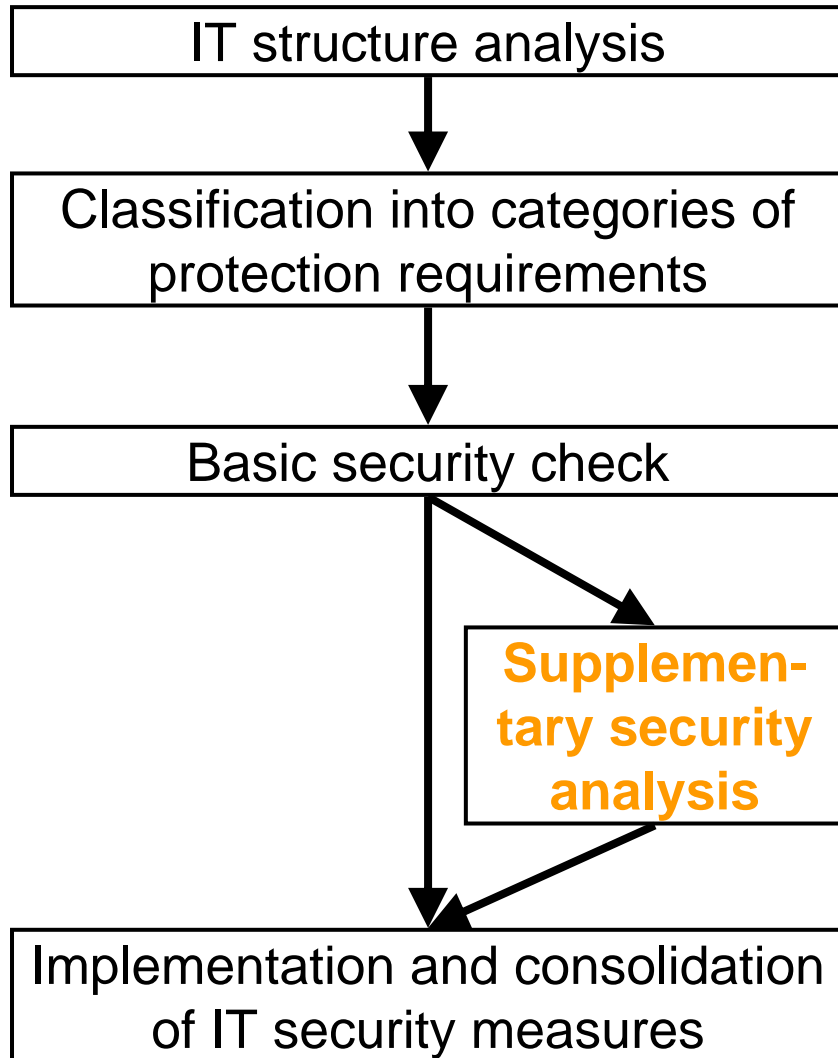
Demonstration procedure for physical protection of IT systems in NPPs (following BSI-Standard 100-2)



Basic security check

- Comparison of the necessary security measures with the actual security measures in operation
- Consideration of organisational aspects and technical requirements
- The BSI-Standard specifies security measures for IT systems with protection requirements of the category “normal”
- IT systems of the categories “high” and “very high” must fulfil further protection requirements → Supplementary security analysis

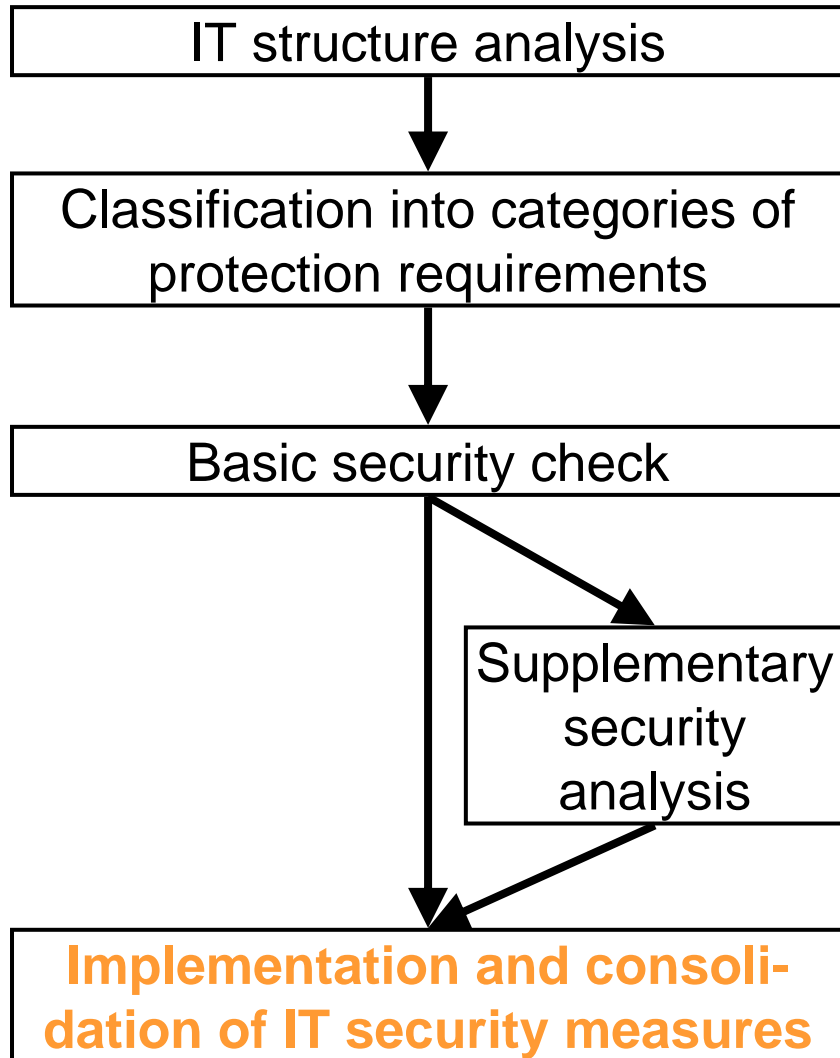
Demonstration procedure for physical protection of IT systems in NPPs (following BSI-Standard 100-2)



Supplementary security analysis

- IT systems with protection requirements of the categories “very high” and “high”
- It has to be shown that malevolent disruptive acts or any other kinds of third-party intervention are safely avoided
- The BSI Standard contains practically no requirements for the supplementary security analysis → requirements have to be developed for each anticipated case of application

Demonstration procedure for physical protection of IT systems in NPPs (following BSI-Standard 100-2)



Implementation and consolidation of IT security measures

- Stipulating the tasks and responsibility (implementation plan)
- Security measures that accompany implementation

Lessons learned from IT security projects – notable organisational aspects /1/

- IT security projects require experts of different areas:
 - technology/process engineering of NPPs
 - NPP safety
 - IT security
- IT security concepts have been introduced for the plants
 - Establishment and maintenance of the IT security process
 - Structure and roles of IT security organisation
 - IT security zones and security areas
 - Corporate IT security
- Specification of the personnel and plant regulations in the NPPs
 - The physical protection commissioner (already appointed in all German NPPs) is also in charge of protecting the IT network of the NPP against third-party intervention.
 - The physical protection commissioner is directly invested with the required powers by the licensee. (continued on next page)

Lessons learned from IT security projects – notable organisational and technical aspects /2/

- Specification of the personnel and plant regulations in the NPPs (continued from previous page)
 - An IT security official has been introduced. The IT security official assists the physical protection commissioner in IT security related issues.
- Distribution of redundant digital I&C trains over different rooms, which are protected against an insider threat by an access system
- Current discussion: data links from I&C systems with protection requirements of the category “very high” to IT systems with less need for protection (on principle no data links, but extremely secured data links may be admissible)
- Access to the IT system only after strict identification (e.g. plant ID card and biometric feature)
- Consideration of the requirements for the protection against an insider IT attacker when developing software and when servicing (e.g. four-eyes principle)

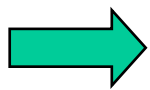
Summary

- The Atomic Energy Act of the Federal Republic of Germany describes the fundamental requirements for the protection against malevolent disruptive acts or other third-party intervention.
- So far, there exist no specific requirements for IT security in NPPs in German laws and regulations.
- Using the existing regulations for physical protection of NPPs, it is possible to develop state-of-the-art requirements for IT security.
- The fulfillment of these requirements can be demonstrated by applying a demonstration procedure following the BSI-Standard.
- For several years GRS has already been working successfully in this field on behalf of several German Länder authorities. The presented methods are the result of this work.

Thank you.

Annex 1: Requisite protection – protection goals

- Any risk to life or health as a result of considerable direct radiation or due to the release of a substantial amount of radioactive materials must be avoided, also in case of a malevolent disruptive act or any other third-party intervention.
- Any singular or repeated theft of nuclear fuel in amounts allowing the direct preparation of a critical assembly without any reprocessing or enrichment of the fuel must also be prevented in the case of a malevolent disruptive act or any other third-party intervention.



Requisite protection is ensured if these protection goals are achieved

Annex 2: BSI – Federal office for information security

- Central IT security service provider for the German government (www.bsi.de)
- BSI themes, e.g.:
 - Certification (IT certificates)
 - Evaluation