Adressing IT-Security in nuclear security regulation and implementation with respect to interim storage facilities in Germany

Alice Wiesbaum

Federal Office for the Safety of Nuclear Waste Management

alice.wiesbaum@bfe.bund.de

+49 30 18333 1793

1. Nuclear Facilities in Germany

Germany has 33 nuclear facilities in operation. Six of them are nuclear power plants, seven are research reactors. Sixteen nuclear facilities are interim storage facilities for nuclear material, from which four are centralized. The other twelve interim storages are placed on-site of nuclear power plants in operation as well as decommissioned ones. In addition to that Germany has two repositories for low and medium active waste, one uranium enrich facility and one fuel assembly fabrication plant.

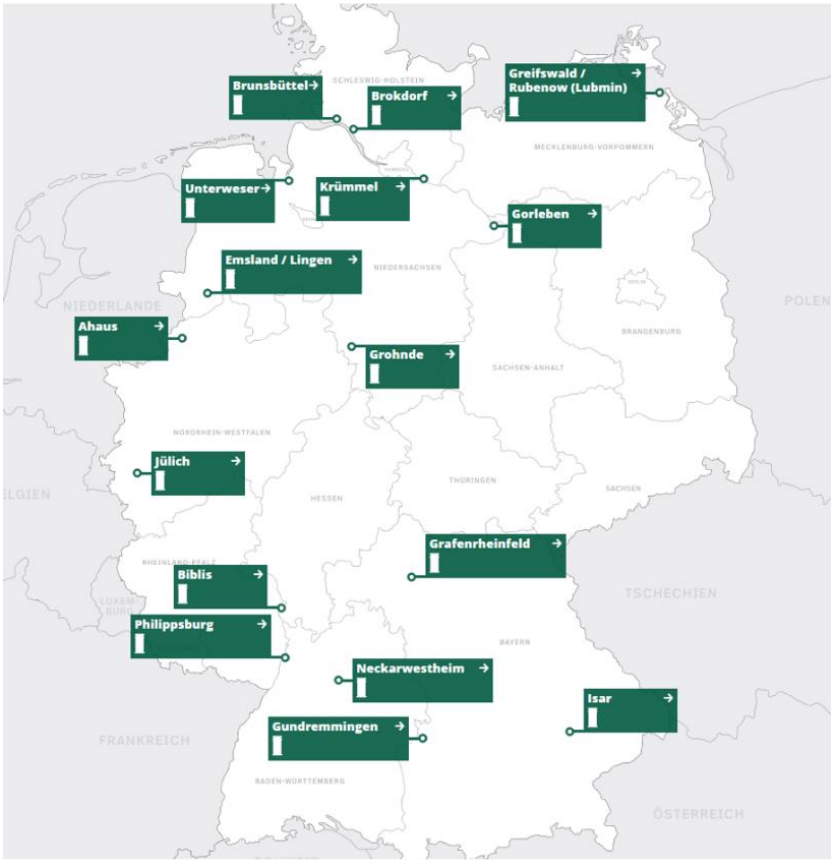


FIG 1 Storage facilities in Germany

This presentation will focus on the sixteen interim storages and the implementation of computer security into the existing security concept on site. Therefore it will give a short overview about the responsibilities during licensing processes in Germany. It will show the regulatory framework and the basics of computer security in Germany. The concrete steps to improve the security of computer based systems will be explained.

In Germany a licence is needed to use, store or nuclear material. Due to the fact that Germany is a federal republic, the responsibility for the security of nuclear facilities does not belong to only one institution. In general the Federal Ministry for the Environment, Nature Conversation and Nuclear Safety (BMU) is responsible

for the national regulations, like implementations of new guidelines. In the case of interim storage facilities the process of licensing is done by the Federal Office for the Safety of Nuclear Waste Management (BASE)[1], but the supervising authority lays within the Ministries of the Federal States ("Länder") (FIG 2).

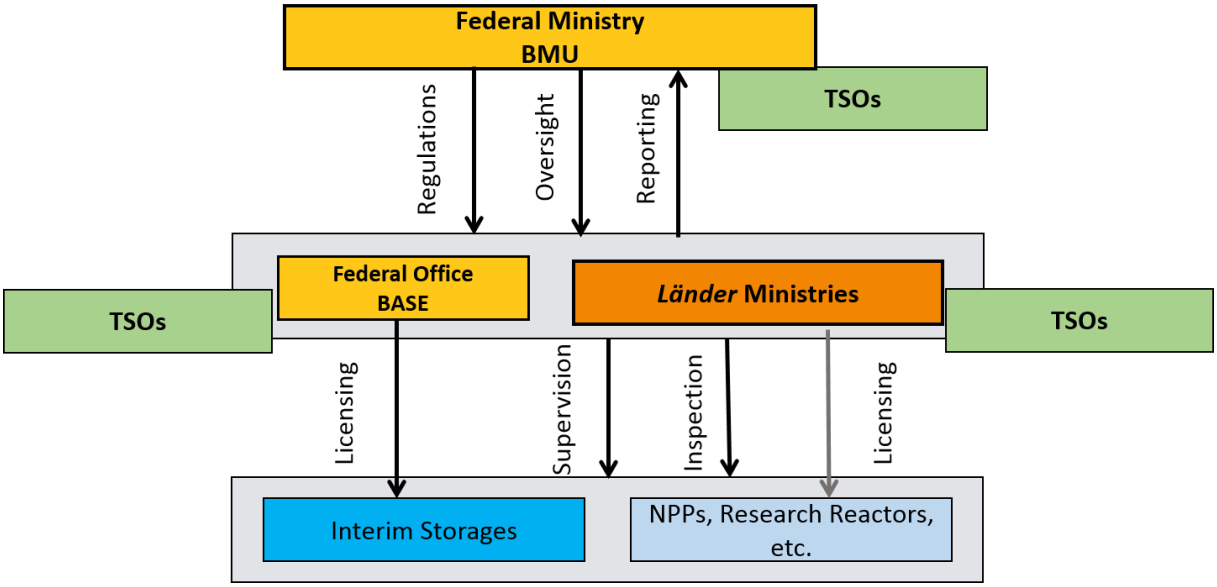


FIG 2 The German regulatory body

For that reason, the stakeholders vary, depending on the location of the interim storage facility. The Federal Ministry, the Federal Office and the Länder Ministries together built the regulatory body in Germany. All three of them work closely together with Technical Support Organizations (e. g. TÜV, GRS).

2. The Regulatory Framework

Germany has many kinds of regulations (FIG 3). On top of all other laws is the German Constitution ("Grundgesetz"). The second layer is built by the Acts. For the sector of nuclear energy the Act of the Peaceful Utilization of Atomic Energy and the Protection against its Hazards (Atomic Energy Act, "AtG"), which is the German equivalent of the CPPNM, as well as the Act on Protection against the Harmful Effects of Ionising Radiation (Radiation Protection Act) are the legal basis. Underneath the Acts are a lot of different Ordinances, e. g. the Radiation Protection Ordinance. The Constitution, the Acts and the Ordinances are generally binding for all people in Germany.

Besides of this generally binding documents, there are guidelines, which are only binding for the competent authorities. For the licensees this guidelines are only binding when used as a specification for example in a licence for the storage of nuclear material.

[1] former BfE, renamed since 01.01.2020

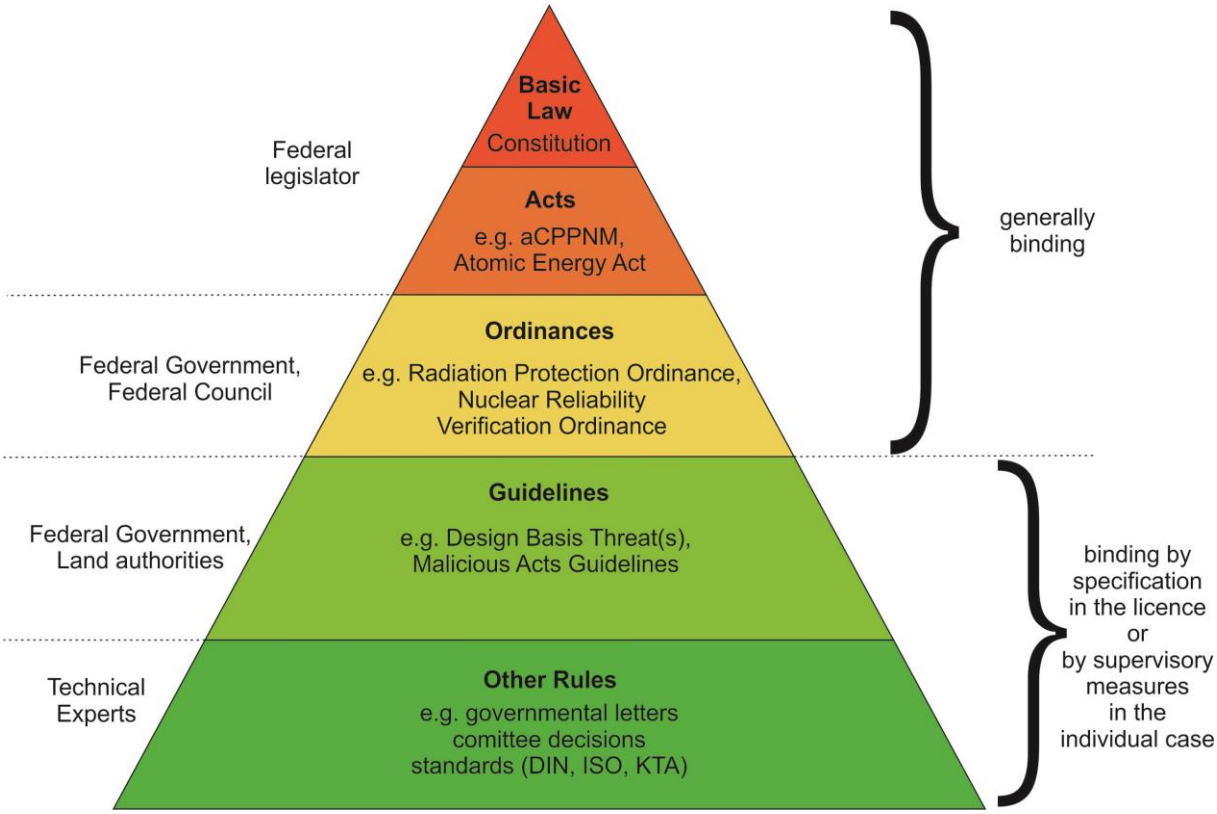


FIG 3 German Laws

This guidelines contain for example the German Design Basis Threat (DBT) and all the Malicious Acts Guidelines used as a rulebook for the security in nuclear facilities. The last kind of documents are other regulations like international standards (DIN, ISO) or decisions of comittees.

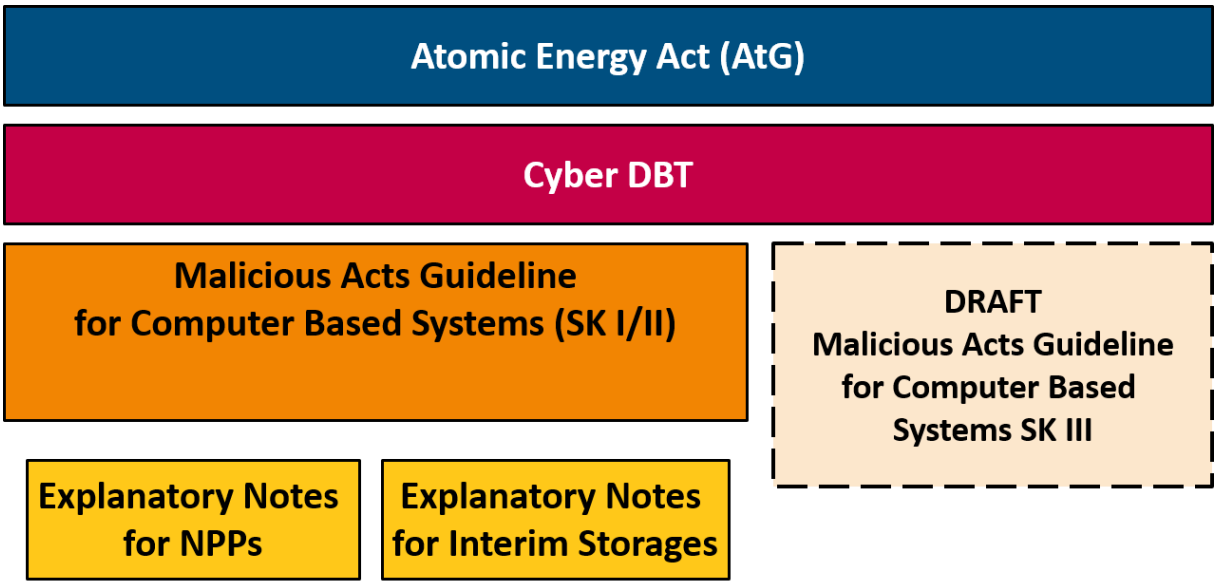


FIG 4 Regulatory Framework for Computer Security

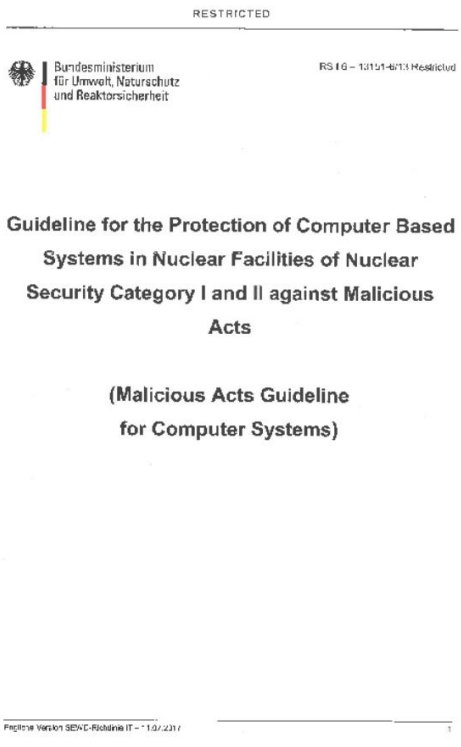
In the Atomic Energy Act the requirements for the applicant are written down. This requirements contain the reliability of the applicant, the safety of the storage according to the state of the art of science and technology, the necessary financial security (liability insurance) and the protection against malicious acts. The protection against malicious acts is the main task in case of security. It is written in § 6, para. 2 AtG and says: "A licence shall be granted if there is a need for such a storage and […] if the necessary protection has been provided against disruptive action or other interference by third parties. […]". The requirement to protect computer based systems is included into para. 2 no. 4.

To fulfill this requirements Germany has two Designed Basis Threats (one for classical security and an own "cyber DBT" for computer security), which are created by a cooperative working group chaired by the Federal Ministry and consisting of members of the State and the Federal States and members of the national security agencies. In case of computer security, the BSI is also a member of the creative working group for the cyber-DBT. All DBT's are reevaluated every three years and as appropriate on an ad-hoc basis due to new findings.

Concrete regulations are done in guidelines. For interim storages there are in particular two guidelines containing requirements for security. The Malicious Acts Guideline and a special Malicious Acts Guideline for Computer Based Systems. To explain how to fulfill the requirements of the Malicious Acts Guideline for Computer Based Systems, the Federal Ministry also created Explanatory Notes (FIG 4).

3. Computer Security in Germany

In general the basics of computer security are written down in a document of the Federal Office for Information Security (BSI). It is called BSI-Grundschutz and gives standards and recommendations for all kind of authorities and companies. It is an open document, which offers a systematic approach to information security that is compatible to the international standards ISO/IEC 27001.


RESTRICTED

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

RS II 6 – 13151-6/13 Restricted

Guideline for the Protection of Computer Based Systems in Nuclear Facilities of Nuclear Security Category I and II against Malicious Acts

(Malicious Acts Guideline for Computer Systems)

For the higher requirements of computer security in the field of nuclear energy the Malicious Acts Guideline for Computer Based Systems is used additionally (FIG 5). The Guideline is restricted and especially written for nuclear facilities of category I and II like NPP's and interim storage facilities (both category I).

The standards of the BSI-Grundschutz are taken into account in the Guideline for Computer Based Systems. Additional measures for the higher requirements of category I and II facilities are defined there.

FIG 5 Malicious Acts Guideline for Computer Systems

It contains the general objectives to prevent nuclear material from theft, sabotage or diversion and additionally the general objective of computer security: “Sensitive computer based systems and the associated processes have to be protected against malicious acts in accordance with their security requirements so that neither a direct nor an indirect violation of the general objectives of nuclear security can be affected”.

It requires computer security organization, for example a member of the security stuff, who is responsible for the computer based systems in the facility (computer security officer). It contains requirements against malicious acts, details on how to plan a computer security concept, and the need for planning and preparedness for and response to computer security incidents.

4. Implementation of computer security into existing security concepts

To start the implementation of computer security the licensees of interim storage facilities had to start with an IT-structure analysis. During this analysis all computer based systems of the facility where listed and ordered. It was the starting point of creating a general concept of computer security by the licensees as well.

In the second step the licensees checked every single computer based system for their relevance due to security. The systems where sorted into sensitive and non-sensitive computer based systems (FIG 6). The concrete measures written in the security concept for computer based systems depend on this classification.

All sensitive systems were then again subclassified into the four categories of their potential risk: normal, increased, high and very high. This computer security levels differ in their requirements in a way, that with a higher level the requirements increase (e. g. prevent access from outside).

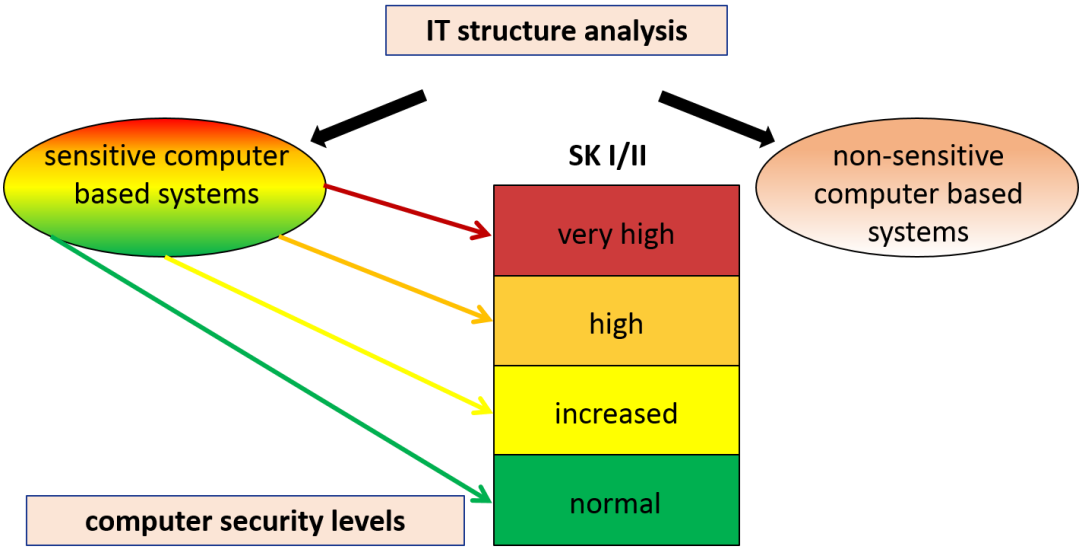


FIG 6 IT-structure analysis

At the same time the computer based systems were clustered into zones to reduce the amount of systems in total (FIG 7). The zones can contain systems which are physically close to each other (e. g. computer systems inside one room) as well as systems which belong together due to their operations (e. g. access control center).

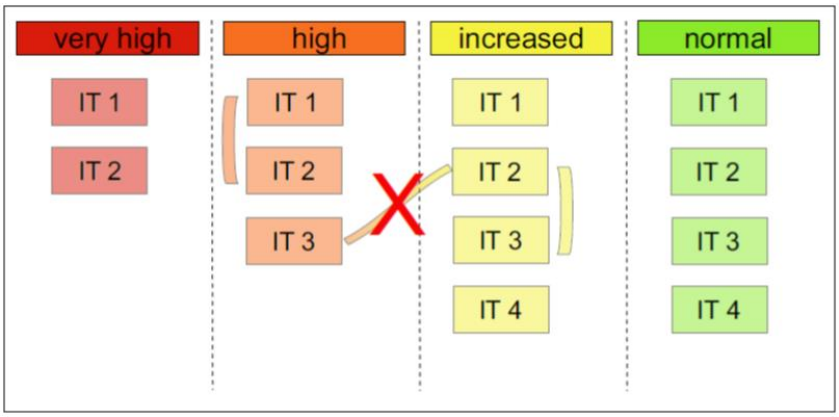


FIG 7 Zones of computer based systems

The security level of the zone is the same as the security level of the computer based systems, which belong to the zone. Therefore it is only possible to build zones from systems of the same security level.

The zones themselves can also be connected. To make sure that all requirements for one security level are fulfilled, it is forbidden to link zones with different security levels.

In the last step the licensees wrote a complete security concept for all computer based systems including the measures taken by the licensees. This concept shows the current situation in the facility, has to be evaluated regularly and cover the whole lifetime of the computer based systems.

This structure of implementing requirements on computer security into existing security concepts of facilities in operation had three milestones over a time period of three years (FIG 8).

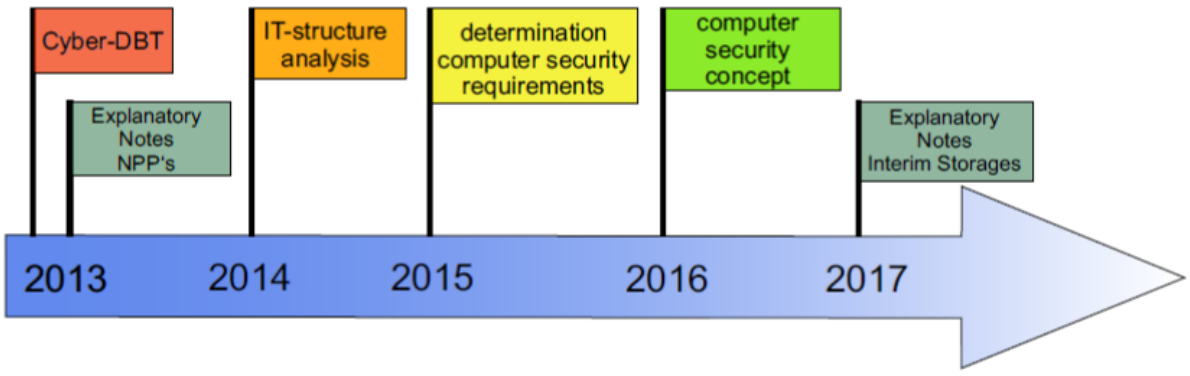


FIG 8 Timeline of computer security implementation

The start was in 2013 when the Federal Ministry put the cyber-DBT and therefore the new Malicious Acts Guideline for Computer Based Systems into force. Also in 2013 the Federal Ministry wrote a document with explanatory notes for the licensees of nuclear power plants to help them fulfill the requirements of the guideline and to create a national standard. An analogue document with explanatory notes especially for interim storage facilities was written in 2017.

The explanatory notes give advice on which sensitive computer systems should be assigned to which specific computer security level. Both explanatory notes are confidential.

In 2013 the licensees started with their IT-structure analysis. This first step had to be finished until 2014, when the classification of the computer based systems started. At the next milestone in 2015 the classification was done and the licensees had another one year to write a whole computer security concept based on the work done before.

Since 2016, every time an applicant is asking for a licence, the complete concept for all computer based systems is proofed during the licensing process. Because computer systems can change very fast, the security concept for computer based systems is constantly developed and updated.

[1] BFE.BUND.DE, https://www.bfe.bund.de/DE/ne/zwischenlager/zwischenlager_node.html;jsessionid=2529381740C4ECDAE8693D014201A1C8.1_cid391

[2] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURAL CONSERVATION, BUILDING AND NUCLEAR SAFETY, Advanced Information Package prepared for International Physical Protection Advisory Service, BMUB, Bonn, 2017

[3] UWE BÜTTNER, Nuclear Computer Security in Germany, BMU, G7 NSSG Cyber Side Meeting, 2018

[4] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURAL CONSERVATION AND NUCLEAR SAFETY, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorie I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT), BMU, Bonn, 2013