IT SECURITY AT THE GERMAN RESEARCH REACTOR FRM II BASED ON THE GERMAN IT SECURITY GUIDELINE SEWD-IT

M. BAUN, R. BROSCHE, A. KASTENMÜLLER

Technische Universität München, Forschungsneutronenquelle Heinz Maier-Leibnitz (FRM II)
Lichtenbergstr. 1, D-85748 Garching, Germany

ABSTRACT

The necessary protection against disruptive measures and other actions by third parties (the German acronym is SEWD) also requires IT security engagements. The new SEWD-IT policy was put into effect in the year 2013. It addresses concepts and the protection objectives of the SEWD-IT directive. Among others, operators of nuclear facilities are required to analyze their installations with respect to SEWD.

As part of the implementation of the guideline (SEWD-IT), at the FRM II an IT structure analysis was carried out, in particular the concepts of the SEWD-IT guideline were applied thus yielding the introduction of IT protection requirements and IT security zones.

As a result, a comprehensive system list was generated, in which all systems of the research reactor FRM II were analyzed and classified according to their respective protection requirement and in line with the SEWD-IT regulations. For systems of the security classes "very high", "high" and "important", detailed security analyzes were carried out.

1. Introduction

The necessary protection against disruptive measures and other actions by third parties (the German acronym is SEWD) also requires IT security engagements. The new SEWD-IT policy was put into effect in the year 2013. It addresses concepts and the protection objectives of the SEWD-IT directive. Among others, operators of nuclear facilities are required to analyze their installations with respect to SEWD. As part of the implementation of the guideline (SEWD-IT), at the FRM II an IT structure analysis was carried out, in particular the concepts of the SEWD-IT guideline were applied thus yielding the introduction of IT protection requirements and IT security zones. The procedure for implementation of the SEWD-IT policy at the FRM II research neutron source will be described below.

2. Special features of the research reactor FRM II

The FRM II is operated by the Technical University of Munich (TUM) on its premises of the Research Campus in Garching. The FRM II started user operation in April 29, 2005 and provides neutrons for science, industry and medicine in up to four cycles of 60 days a year.

The scientific use of the reactor for the experimental facilities such as the cold source KQ / KNQ, the hot source (HNQ), the irradiation facility (MEDAPP) (the so-called converter facility), as well as the various irradiation facilities is in the foreground. The scientific use of the FRM II takes place within the framework of the “MLZ” (Heinz Maier-Leibnitz Zentrum), a cooperation between the TUM, Forschungszentrum Jülich and the Helmholtz Zentrum Geesthacht with the collaboration of the Max Planck Society and nine other university groups. This results in a close connection to numerous scientific faculties of the TUM and external research institutions.

The Figure 1 shows an overview of the cooperation framework

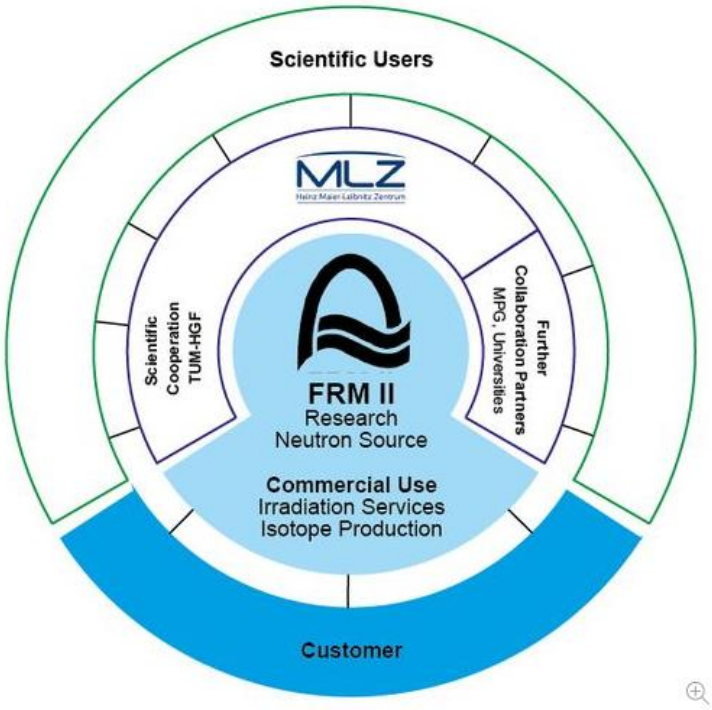

Fig. 1 : FRM II cooperation framework

Due to the characteristic of the FRM II as a research neutron source and its interdisciplinary use, the construction and operation of this nuclear facility in comparison to other nuclear facilities (especially nuclear power plants) shows i. a. the following features

- Inherent safety features: this refers to the fact that the FRM II is constructed such that laws of nature ensure that deviations from the specified target state are intercepted. These include in the core design, for example, the negative reactivity coefficients.

- The FRM II is the latest (research) reactor in Germany (the FRM II has become critical for the first time in March, 2004). Extensive safety and security aspects of the digital reactor control technology (TXP), the digital reactor protection system (TXS), as well as the crosslinking have already been intensively considered and implemented in the facility design and the licensing procedure (1994 - 2004).

- A result of this facility design is a strictly isolated architecture (siloed solutions/applications) of those IT systems (e.g. TXP, TXS) that are in compliance with SEWD-IT guideline to other IT systems.

- Strictly separate network structures exist for the respective organizational areas (operation, science, administration).

- As a scientific department of the TUM, the data networks of the organizational areas operation, science and administration are connected to the public network via the Security Gateway SECOMAT of the Leibnitz Rechenzentrum (LRZ).

3. Implementation of SEWD IT requirements

In order to achieve an appropriate level of security, a systematic approach is required to design the security process. The security process is comprised of the following phases:

1. Initiation of the security process
2. Accepting of responsibility by the management
3. Designing and planning the security process
4. Creation of the policy for IT security
5. Establishment of a suitable organisational structure for IT security management
6. Provision of financial resources, personnel, and the necessary time
7. Integration of all employees into the security process
8. Creation of a security concept
9. Implementation of the security concept
10. Maintenance of IT security during live operations and implementation of a continuous improvement process

The Figure 2 shows an overview of the security process at FRM II.

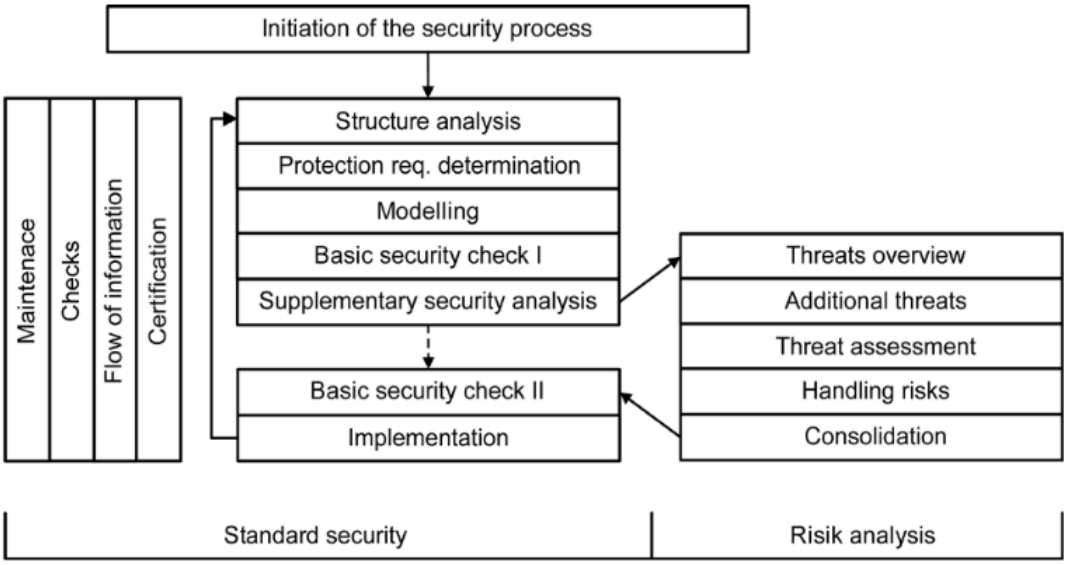

Fig. 2 : The FRM II security process

The most important steps to implement a security concept at FRM II are

A) Structure analysis
B) Determination of the protection requirements
C) Basic security check and supplementary security analysis (security analysis)

3.1. Organisation of the security process

The integration of an IT Security Officer (ISO) into organisation-wide procedures and processes.

An ISO had been appointed to promote and coordinate the task of IT security in the organization in order to successfully plan, implement and maintain a security process.

The ISO controls the IT security process and is participating in all tasks relating to it. He creates the policies for IT security and coordinates the creation of the security concept, the contingency planning concept and other subconcepts and system security guidelines as well as issuing additional guidelines and rules for IT security. The ISO is also involved in all projects having a significant effect on the processing of information and in introducing new applications and IT systems in order to ensure that the security aspects are taken into account in the various phases of the project.

An IS Management Team was founded under the direction of the ISO. The IS Management Team consists of function owners like the ISO, the technical director, the physical security officer, as well as, if necessary, representatives of the individual departments or subareas. The IS Management Team supports the IT Security Officer by coordinating the safeguards global to the entire organisation, collecting information, and carrying out monitoring tasks.

3.2. Structure analysis

The structure analysis is used to perform a preliminary survey of the information required for the additional procedures when creating a security concept. In this case, this means documenting the components (information, applications, IT systems, rooms, communication, networks, etc.) required to perform the business processes or specialised tasks specified to be in the scope of the SEWD-IT RL. As a result, a comprehensive system list was generated, in which all systems of the research reactor FRM II are listed for further analyzation and classification.

3.3. Determining the protection requirements

The specification of the protection requirement for in-scope IT systems can only be carried out by individual analysis, due to the specific features of the FRM II. All in-scope IT systems of the FRM II were analysed and classified according to their respective protection requirement and in line with the SEWD-IT regulations in security classes "very high", "high", "important" and “normal”. Criteria for the specification of the protection requirements refer to a maximum possible impact in regarding a violation of the global safety objectives rules of the SEWD-RL IT policy.

3.4. Defining security zones

Vulnerable IT systems are arranged in IT security zones based on their security and protection requirements. This arrangement simplifies the definition and implementation of procedures, as they can be moved to the transitions between the zones. All IT systems within an IT security zone must be assigned the same IT protection requirements class. The IT protection requirement class of an IT security zone is defined as the IT protection requirements class of its IT systems. If an IT system is assigned to a zone with a higher IT protection requirement class, the IT protection requirements class of the IT system must be increased accordingly due to the maximum principle.

Vulnerable IT systems from different functional areas can be assigned to different IT security zones, even if the IT systems are assigned to the same IT protection requirements class. If necessary, several IT security zones can be formed within one functional area. Multiple vulnerable IT systems within an IT security zone may be protected by consolidated safeguards.

3.5. Basic security checks and supplementary security analysis

For efficiency reasons, we use a two-step approach. The first level defines the protection requirements of the IT system. The underlying threat model assigns the target objects typical threats and the corresponding default security measures. It takes into account which threats and security measures should be assigned. Based on the modules of the BSI IT-Grundschutz Catalogues, using this method can increase the IT security level quickly and efficiently. In this first level (basic security check) the safety measures are taken mainly to eliminate the fundamental risks common to all IT systems. In addition, the second stage examines which other information-related risks are relevant and must be taken into account.

For systems of the security classes "very high", "high" and "important", an additional supplementary security analysis is performed. The goal in this case is to decide for each individual target whether additional risk analyses are required. In order to streamline this process, the target objects are divided into appropriate groups prior to performing a supplementary safety analysis.

4. Abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik (German federal office for IT security)
FRM II	The research neutron source Heinz Maier-Leibnitz
Grundschutz	defines the minimum IT security requirements
IT	Information Technology
ISO	IT Security Officer
SEWD-RL IT	the IT guideline for protection against disruptive measures and other actions by third parties (the German acronym is SEWD)
TUM	Technical University of Munich
TXP	Siemens Teleperm XP
TXS	Areva Teleperm XS