Implementation of Computer Security at Nuclear Facilities in Germany

André Lochthofen, Dagmar Sommer

GRS mbH, Schwertnergasse 1, D-50667 Cologne

Abstract:

In recent years, electrical and I&C components in nuclear power plants (NPPs) were replaced by software-based components. Due to the increased number of software-based systems also the threat of malevolent interferences and cyber-attacks on NPPs has increased. In order to maintain nuclear security, conventional physical protection measures and protection measures in the field of computer security[1] have to be implemented. Therefore, the existing security management process of the NPPs has to be expanded to computer security aspects. In this paper, we give an overview of computer security requirements for German NPPs. Furthermore, some examples for the implementation of computer security projects based on a GRS-best-practice-approach are shown.

1 INTRODUCTION

During the last years, the licensees of nuclear power plants (NPPs) have modernised extensively the operational and safety-related components of their plants, because the original components reach their end of lifetime. Hereby the number of software-based electrical and I&C components in the plants has increased. Some reasons are the complicate procurement of spare parts, because the "old" analogue technology is no longer offered by the manufacturers, and the process optimisation due to the use of the "new" software-based (smart) technology. Due to this increased 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. Therefore, in addition to the physical protection measures computer security measures for the protection of the software-based systems have to be developed and realized.

In 2010, the detection of the malicious software "stuxnet" has impressively demonstrated that cyber-attacks are possible and are already in progress in process automation /2/. "Stuxnet" exploits different vulnerabilities of Microsoft products to manipulate SCADA (Supervisory Control and Data Acquisition) systems with SIMATIC WinCC or SIMATIC PSC7 from Siemens /3/. In doing so "stuxnet" cannot only spread information but can also manipulate industrial processes and operational sequences /4/. Consequently "stuxnet" can manipulate the control systems of plants. Furthermore, other cyber-attacks have shown that these attacks can include much more sophisticated manipulations than failure of one system or common cause failure of a set of systems and that one attack may hit more than one target

[1] In our paper we use “computer security” as established in /1/:
“*[…], computers and computer systems refer to the computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility. This includes not only desktop computers, mainframe systems, servers, network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers). In essence, this publication is concerned with all components that may be susceptible to electronic compromise.*
[…] the term computer security will be used to cover the security of all computers as defined above and all interconnected systems and networks formed by the sum of the elements. The terms IT security and cyber security are, […], considered synonyms of computer security […].”

at different places at the same time. Another aspect is that the attacker can act from a far remote place. To prevent or to repel such cyber-attacks and its manipulations in NPPs specific counter measures in the field of computer security must be taken.

In this paper, a selection of corresponding computer security requirements for German NPPs is presented. Furthermore, some examples of realised computer security projects are shown and the essential principles of the GRS assessment are explained.

2 REQUIREMENTS FOR COMPUTER SECURITY IN GERMAN NPPS

In Germany, the legal requirements for licensing NPPs are defined in the "Act on the Peaceful Utilization of Atomic Energy and the Protection against its Hazards (Atomic Energy Act)" /5/. From the security point of view the German NPPs in particular have to comply with § 7 para. 2 no. 5 "A license may only be granted if the necessary protection against malevolent disruptive actions or other interferences by third parties is ensured.". For ensuring this necessary protection in the field of computer security (i. e. protection against cyber-attacks) since July 2013 the documents - the German cyber design basis threat (cyber DBT) /6/ and the German guideline for the protection of software-based systems in nuclear facilities /7/ - are obligatory for all German NPPs. As in the field of computer security in the past for the German NPPs no specific requirements were available, GRS published as a result of the cyber-attack with the malicious software "stuxnet" in 2010 an information notice /2/ concerning this topic. In addition, since 2011 an international technical guidance published by the IAEA about computer security at nuclear facilities /1/ is available.

2.1 German guidelines for computer security at German NPPs

The German cyber DBT /6/ is a confidential document, which describes important characteristics of postulated cyber-attackers and their postulated attacks. Characteristics of an attack include that cyber-attacks can be part of or a combination with "conventional" (non-cyber) attacks, e. g. for information gathering, and that these attacks can consist of several steps.

The German guideline for the protection of software-based systems in nuclear plants and facilities of protection category I and II against malevolent disruptive actions or other interferences by third parties /7/ is a restricted document, which defines requirements for computer security measures. This guideline was developed taking into account international guidance as well as the national expertise of operators, competent authorities and expert organisations including the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS).

In the guideline /7/, it is defined that all software-based systems of the facilities, which may be used for malicious actions, must be protected (i. e. potentially also office systems). In order to ensure the protection against malevolent disruptive actions or other interferences by third parties, in the guideline /7/ the compliance with the general nuclear security objectives and the new-defined computer security objective is required.

Furthermore, requirements for specific computer security tasks, responsibilities and powers of selected staff members (i. e. computer security organisation) are given. During the practical implementation, these requirements must be transferred into the existing facility organisation structure. An important issue of this implementation is the appointment of a computer security officer (CSO). This CSO should support and give advice on questions about computer security and should assist in computer security related issues.

Further, this guideline /7/ gives requirements concerning the computer security concept. The basis for this computer security concept is a structure analysis that analyses and documents all existing software-based systems, their structures and the entire network topology. The protection of these software-based systems should be classified according to four graded

computer security levels. The concept allows also grouping these systems into different computer security zones.

Based on this concept, the guideline /7/ presents graded generic requirements for computer security measures. Thereby these requirements are grouped into general requirements, in requirements that scale with the security levels and requirements for the specific security zones. To fulfil these requirements the facilities have to perform a basic security check for each software-based system and if necessary a supplementary security analysis. When determining the necessary computer security measures the results of these analyses are included. These measures can be of organisational, structural or technical manner.

In the guideline /7/, it is also defined that the whole life cycle of software-based systems must be considered for implementing computer security. Furthermore, not only the systems inside the plants have to be regarded, but also in the supply chain, for external services and for remote maintenance access connection there is an obligation for computer security measures.

2.2 GRS Information notice concerning the malicious software “stuxnet” (WLN 2010/07 /2/)

Based on the information available at GRS no German NPP was infected by the malicious software "stuxnet". Furthermore, the analogue reactor protection system, which is operated in German NPPs, cannot be impaired by such a cyber-attack. Nevertheless, why is "stuxnet" so important for the nuclear industry?

"Stuxnet" has shown that cyber-attacks on industrial systems, automation systems, SCADA systems and thus also on NPPs are possible. Therefore in the meaning of the defence-in-depth-idea physical protection and computer security measures are necessary to ensure the nuclear security. Because at the time of the publication of the WLN 2010/07 /2/ in 2010 no legal requirements were available in Germany, GRS has published several recommendations to this topic. These recommendations do not only comply to a "stuxnet"-infection, but also to universally valid procedures. The following main topics are covered by the recommendations:

- Identification and analysis of possible infected software-based and industrial control systems
- Potential "stuxnet"-infection has to be eliminated
- Review and adaptation of user rights (e. g. access control for mobile devices) to a minimum
- No internet access for industrial control systems
- Developing a computer security concept to maintain the nuclear security

2.3 Technical guidance published by the IAEA about computer security at nuclear facilities /1/

Until now, the IAEA has published one document for nuclear facilities which is specific to the computer security topic. This is the technical guidance Nuclear Security Series No. 17 "Computer Security at Nuclear Facilities" /1/, which provides specific guidance to nuclear facilities on implementing a computer security programme and gives advice on evaluating

existing programmes. This is achieved by presenting some approaches, structures and implementation procedures (by applying the defence-in-depth-concept).

In this process, responsibilities and powers are mentioned as well as the graded approach with computer security levels and zones. In contrast to the German guideline, five in contrast to four computer security levels are introduced. Further, a basic concept for the risk assessment and a threat identification method is explained. Special considerations for nuclear facilities, e. g. the difference between software-based systems and industrial control systems, are given. In the annex some information about cyber-attack scenarios and about the role of human errors in the field of computer security is given. These aspects together are crucial for achieving and maintaining the level of protection defined in the facility security strategy and conforming to national security objectives.

For the future, the IAEA has intended to publish some more computer security documents in the categories "Recommendations", "Implementing guides" and "Technical Guidance".

3 EXAMPLES FOR THE IMPLEMENTATION OF COMPUTER SECURITY AT NPPS

In the following, GRS presents assessment principles for different computer security topics. These principles are based on a best-practice-approach. GRS has established this approach in the last years during several assessments in the field of computer security at NPPs. In addition, GRS was involved in the development of the new German computer security guideline /7/. As a result GRS has accumulated an extensive knowledge of the implementation of computer security at NPPs (“GRS-best-practice-approach”).

However, for the implementation of computer security projects at NPPs a team of experts belonging to different areas is required. This team should comprise engineers with the knowledge of the technology and the operational processes of the NPPs, experts who know the safety aspects of the NPPs and of course experts of the computer security sector.

For expanding the existing security management process of the NPPs to computer security aspects, GRS recommends to develop and to introduce at a first step a computer security concept. In addition, the integration of the structure and the roles of a computer security organisation into the existing plant organisation is also an important step, i. e. arrangement of tasks (e. g. tasks of the computer security officer), responsibilities, powers and budgets.

For the expanded security management process it is important that this process will be lived by all staff members, i. e. the corporate understanding of the staff members that each individual has to do one’s bit is a major point of a successful implementation. Regarding the computer security aspect for example each individual should report abnormalities, follow the rules, be attentive and so on.

The basis for the computer security concept is the integration of the graded approach of four computer security levels and of the computer security zones. Due to a structure analysis in a NPP all existing software-based systems will be documented and afterwards each system will be assigned to one computer security level. If necessary the systems with the same computer security level can be summarized in one computer security zone. One advantage of this approach is that some computer security measures can be applied to protect all systems in a zone, i. e. some computer security measures can be placed at the zone borders, so that in this case not every system needs all computer security measures separately.

According to the respective computer security level the basic security check and a supplementary security analysis are conducted. As a result the necessary specific computer security measures will be determined. For the highest level the need for protection is the highest and for the other levels the need for protection follows a graded approach.

One example for a measure to protect the highest computer security level is the prohibition of data links into this level. However, for lower levels for example a secured data link may be admissible.

An example for a common protection measure is a regulated access to the software-based systems. Here a strict user identification (e. g. plant ID card and biometric feature) and an user access restriction are thinkable. Another common computer security measure is the requirement to prohibit the connection of private technology (e. g. mobile phones or flash drives) to software-based plant systems and the use of software-based plant systems for private purposes.

An important measure for the protection against an insider attacker is the use of the two-person-principle. This principle can also be applied to control a software development process or a local service process.

In addition to the computer security measures also physical protection measures must be installed to protect the software-based systems, e. g. the entrance limitation to rooms in which the computer security racks are installed.

In the plant specific computer security concept not only the software-based systems of the plant must be considered, but also the software-based systems of possible external services or subcontracted supplies from third parties. In this context the survey of possible remote maintenance accesses also has to be considered.

In the following some examples for the implementation of computer security projects at German NPPs based on the above mentioned GRS-best-practice-approach are given.

3.1 Implementation of a computer security concept at a NPP

During the implementation of a computer security concept at a NPP, GRS has reviewed the appropriate documents, the organisational structure and the derivative of the necessary protection requirements. In addition to this, the common requirements of computer security and the technical realisation of the corresponding computer security measures were checked by GRS. In the following a short overview of the essential principles without making any reference to the established requirements of the physical protection aspects is given.

First, the integration of a computer security organisation into the plant organisation is required. One key factor of this integration is the appointment of the CSO, which has to get the necessary responsibility and powers. Further, the boundary of this CSO to other staff members should be considered. Only with the introduction of this position it is in fact possible to ensure the realisation of the computer security measures.

Furthermore, for the implementation of the computer security concept a generic document is necessary to define and explain its basic requirements. These requirements contain the approach of the structure analysis, the definition and structure of the computer security levels and zones, the different tasks of the staff members (i. e. important aspects of the computer security organisation) and other aspects like life cycle, handling of mobile equipment or regulation of user accesses. In addition, detailed explanations of important topics can be distributed in separate documents.

During the assessment of the above mentioned documents, GRS has verified the included requirements according to the GRS-best-practice-approach. As a result a list with all open points and disagreements with respect to the protection against malevolent disruptive actions or other interferences by third parties was presented. Afterwards the documents were revised by the plant staff in order to meet all GRS recommendations.

In addition to this conceptual assessment, GRS has reviewed the technical realisation of the requirements of the above mentioned computer security concept. Therefore audits at the plant with extensive discussions of different important aspects were necessary. After a final discussion between the reviewers, the related plant staff and the state authority the computer security concept of the plant was approved.

3.2 Displacement of plant applications into an external computer centre

The displacement of software-based plant applications into an external computer centre requires appropriate computer security measures. The determination of these measures was accompanied by GRS in order to ensure the necessary protection against malevolent disruptive actions or other interferences by third parties. At first, the physical protection of the computer centre building was approved. In a second step the computer security organisational and personal procedures as well as their technical realisation in the computer centre were reviewed in respect to the GRS-best-practice-approach.

Because the NPP had an approved computer security concept the appropriate computer security measures of the applications could be equivalently transferred into the computer centre environment. Therefore, the security objectives of the plant were assumed by the computer centre. In addition, the protection requirements and subsequently the specific computer security level and zone of each application were kept in mind. Furthermore, the network area used by the plant but located in the computer centre was well defined compared to the general network area of the computer centre. Thereby also the computer security as well as the physical protection measures against an unauthorised use was included.

The two-person-principle was also integrated in the computer centre procedures just like the integration in the plant. Therefore, technical solutions like electronic locks at the doors to secure that at least two persons go into the rooms, room monitoring systems for a visual control of the entrance, separation locks (barriers that admit only one person at a time access) or specially protected computer security racks were installed. In addition to these entrance security measures the access to the applications was secured. Therefore, among others, restricted user accesses in combination with strict user identifications were implemented. In compliance with the two-person-principle also the different appropriate data administrator rights were separated from each other, i. e. one administrator does not have got an access to two associated networks.

Before commissioning the network area of the computer centre used by the plant the physical protection and the computer security requirements and measures were checked by the plant (“internal audit”). Afterwards, an external verification by GRS (“external audit”) was conducted to approve the entire displacement. To maintain the achieved protection against malevolent disruptive actions or other interferences by third parties, internal and external audits shall be repeated periodically.

3.3 Implementation of a software-based trunked radio system for the physical protection division of a NPP

In this chapter, the basic points of the implementation of a software-based trunked radio system for the physical protection division of a NPP will be presented. To approve this implementation, GRS has applied its above mentioned best-practice-approach on this system. The physical protection requirements and measures are not part of this chapter.

At the initial point of the assessment, the NPP had already implemented a computer security concept.

As part of the structural analysis all components and data connections of the trunked radio system were checked. The result of this analysis has shown that the trunked radio system consists of a main software-based part for the normal operation ("normal system") and a second non-software-based part that is used as backup system ("backup system"). Additionally, a remote maintenance access connection is part of the system.

Based on the results of the structural analysis the trunked radio system was assigned to a computer security level. Because the trunked radio system should be associated to the physical protection division, for the computer security level normally the second highest security level had to be chosen. However, due to structural and organisational defaults this was impossible. As a result the "backup system" was assigned to the second highest computer security level and the "normal system" was assigned to a computer security level with less need for protection. Due to the basic security check and the supplementary security analysis it was decided that in addition to the level corresponding computer security measures for the "normal system" some additional ("higher") computer security measures (e. g. protection of the remote maintenance access connection) had to be implemented.

The necessary requirements of the computer security measures of the "normal system" were fulfilled by the measures due to the existing computer security concept. To fulfil one of the additional "higher" computer security measures decoupling measures for the remote maintenance access connection had to be implemented. Resulting from the fact that the "backup system" is not software-based, the corresponding requirements were also fulfilled due to the existing physical protection measures.

4 CONCLUSION

In the last years the number of software-based electrical and I&C components installed in nuclear power plants (NPPs) increased and a further replacement of the analogue technology (not software-based) by the software-based technology is expected. Subsequently, the threat of malevolent interferences and cyber-attacks via these components to the plants also increased. As a result in addition to the physical protection of a NPP also the computer security for a NPP must be considered in order to maintain the nuclear security.

Based on this trend, since July 2013 in Germany two guidelines with recommendations and requirements for the protection of software-based systems in NPPs against malevolent disruptive actions or other interferences by third parties are available – the German cyber DBT /6/ (confidential) and the German computer security guideline /7/ (restricted). Further recommendations and requirements for German NPPs in the field of computer security can be found for example in the GRS information notice to the malicious software “stuxnet” (WLN 2010/07 /2/). An additional assistance in this field can be found in the technical guidance /1/ published by the IAEA.

In this paper, we have presented the GRS-best-practice-approach for the implementation of computer security at NPPs and some examples of its apllication. Thereby we have outlined a general approach to expand the existing security management process in NPPs to computer security aspects. We have shown, that for the expanded part of this process the integration of a computer security organisation with a computer security officer and the implementation of a computer security concept that contains the analysis of all existing software-based systems including their structures and network topology, the definition of graded computer security levels and zones, the determination of corresponding computer security measures and the approval of the technical realisation, are needed.

In our project examples, we have discussed the essential principles of an assessment of the computer security at NPPs in different contexts. In addition to the general approach of the expanding of the existing security management process to computer security, we have outlined some possible computer security measures (e. g. the prohibition of data links into

the highest computer security level, the use of the two-person-principle, and the restriction of user rights).

5 REFERENCES

/1/ IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities", International Atomic Energy Agency, 2011

/2/ Weiterleitungsnachrichten zu meldepflichtigen Ereignissen in Kernkraftwerken der Bundesrepublik Deutschland (WLN 2010/07), "Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7", GRS mbH, September 2010

/3/ www.heise.de, News "Stuxnet-Wurm kann Industrieanlagen steuern", 16.09.2010

/4/ Siemens - Industry Automation and Drive Technologies, "SIMATIC WinCC/SIMATIC PCS7: Information bezüglich Malware / Virus / Trojaner", online access (http://support.automation.siemens.com) at 20.09.2010

/5/ "Act on the Peaceful Utilization of Atomic Energy and the Protection against its Hazards (Atomic Energy Act)", German Federal Ministry of Environment, Nature Conservation and Nuclear Safety, August 2013

/6/ "Design Basis Threat for the Design of Nuclear Plants and Facilities against Disruptive Actions or other Interferences by Third Parties with the Help of Cyber-Attacks (cyber DBT)", German Federal Ministry of Environment, Nature Conservation and Nuclear Safety, July 2013

/7/ "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 (SEWD-Richtlinie IT)", German Federal Ministry of Environment, Nature Conservation and Nuclear Safety, July 2013