Progress in Nuclear Energy 84 (2015) 103–107

Contents lists available at ScienceDirect

Progress in Nuclear Energy

journal homepage: www.elsevier.com/locate/pnucene

Implementation of computer security at nuclear facilities in Germany

André Lochthofen*, Dagmar Sommer

GRS mbH, Schwertnergasse 1, D-50667 Cologne, Germany

ARTICLE INFO

Article history:
Received 20 February 2014
Accepted 29 December 2014
Available online 28 January 2015

Keywords:
Computer security
Nuclear facility
Implementation
Germany

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 modernized 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 optimization 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 (GRS mbH, 2010). “Stuxnet” exploits different vulnerabilities of Microsoft products to manipulate SCADA (Supervisory Control and Data Acquisition) systems with SIMATIC WinCC or SIMATIC PSC7 from Siemens (News, 2010). In doing so “stuxnet” cannot only spread information but can also manipulate industrial processes and operational sequences (Siemens, 2010). 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 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 realized 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)” (German

* Corresponding author.
E-mail address: andre.lochthofen@grs.de (A. Lochthofen).

[1] In our paper we use “computer security” as established in (International Atomic Energy Agency, 2011): “*[…], 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 […].*”

http://dx.doi.org/10.1016/j.pnucene.2014.12.016
0149-1970/© 2015 Elsevier Ltd. All rights reserved.

Federal Ministry of Environment, 2013a). 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) (German Federal Ministry of Environment, 2013b) and the German guideline for the protection of software-based systems in nuclear facilities (German Federal Ministry of Environment, 2013c) – 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 (GRS mbH, 2010) concerning this topic. In addition, since 2011 an international technical guidance published by the IAEA about computer security at nuclear facilities (International Atomic Energy Agency, 2011) is available.

2.1. German guidelines for computer security at German NPPs

The German cyber DBT (German Federal Ministry of Environment, 2013b) 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 (German Federal Ministry of Environment, 2013c) 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 organizations including the Gesellschaft für Anlagen-und Reaktorsicherheit (GRS).

In the guideline (German Federal Ministry of Environment, 2013c), 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 (German Federal Ministry of Environment, 2013c) 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 organization) are given. During the practical implementation, these requirements must be transferred into the existing facility organization 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 (German Federal Ministry of Environment, 2013c) 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 (German Federal Ministry of Environment, 2013c) 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 organizational, structural or technical manner.

In the guideline (German Federal Ministry of Environment, 2013c), 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 (GRS mbH, 2010))

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 defense-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 (GRS mbH, 2010) 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 with 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 (International Atomic Energy Agency, 2011)

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” (International Atomic Energy Agency, 2011), 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