ENERGETIKA. 2017. T. 63. Nr. 4. P. 141–145

Cybersecurity of critical infrastructures such as nuclear facilities

Heinz-Peter Berg

Bültenweg 85,
38106 Braunschweig, Germany
Email: bergheinzpeter@gmail.com

In the last years, cybersecurity has become a crucial essential element within the security framework of critical infrastructures such as process industry, railways, hospitals and also nuclear facilities. The types of threats change, and not only organizations requiring money from the affected organization but also nation states seem to be involved. The number of cyber-attacks to all types of critical infrastructure increased and these attacks are seen as a threatening problem.

For the specific aspects of nuclear facilities in Germany, current experiences and future activities regarding these facilities under the German IT Act are discussed. Moreover, respective regulatory requirements recently set in force in Germany are presented. In addition, ongoing international activities in this area are discussed.

Keywords: IT security, cybersecurity, German nuclear regulations, international projects

INTRODUCTION

In general, the protection of critical infrastructures should cover all activities, which shall ensure their functionality, continuity and integrity in order to prevent every type of threats, risks or weaknesses including cyber-attacks affecting the proper functioning. In the last years, the types of threats change and not only single hackers or criminal organizations requiring money from the affected organization but also nation states and more and more national state organizations get involved. It seems that cybersecurity threats have become to some extent part of destabilizing strategies. The number of cyber-attacks to all types of critical infrastructure has increased and these attacks are seen as a real problem in the future.

According to the terminology in [1] cybersecurity is defined as "actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets".

As explained in [2] the development of the digital technology related to instrumentation and control (I&C) systems influences many industries. The importance of cybersecurity in protecting these systems against critical infrastructure attacks is, therefore, of high importance and it is also a challenge to the manufacturers of such systems.

Recent complex attacks to nuclear facilities targeted to I&C systems with all the potential consequences for safety and security resulting from such attacks [3]. In that context, cybersecurity is understood as the adequate protection of any digital equipment or service from unintended access, change or destruction. Against this background, cybersecurity has become an essential part of the entire security framework of nuclear facilities and it is a task of high priority for operators as well as for regulatory and supervisory authorities. Therefore, several reviews of cybersecurity applications, especially in nuclear power plants, are performed [4] showing that it is important to be aware of the evolution of hardware and software and to counter the increasing risk for the facilities regarding cyber vulnerabilities.

GERMAN IT SECURITY ACT

The German IT Security Act (IT-Sicherheitsgesetz) was set in force in July 2015 [5]. Regulations which specify the areas of critical infrastructure covered by the act are needed for its implementation. The first regulation entered into force in May 2016. It covers the critical infrastructure sectors of energy including nuclear power plants, information technology and telecommunications, as well as water and food. The sectors affected must fulfil their obligations under the law six months after the regulations have entered into force.

Initial effects are already being seen as a result of the enactment of the IT Security Act. For example, individual companies in the areas covered are already meeting their statutory obligations for reporting IT security incidents and for protecting IT systems in accordance with state-of-the-art technology ahead of the deadline.

The German IT Security Act places the highest demands on the operators of each type of the critical infrastructures mentioned above. In addition to the requirement of establishing adequate safety and security measures, the operators must undergo an evaluation of the chosen measures every four years.

As a national cybersecurity authority, the Federal Office for Information Security (BSI) has to promote IT security in Germany and is the central IT security service provider for the federal government. Moreover, BSI is the central reporting and supervisory authority, i.e. based on the various requirements defined in the IT Security Act, incidents have to be reported to BSI. The insights gained from these notifications and also from other various information are provided to all operators of critical infrastructures so that they can adequately protect their IT.

The BSI report of 2016 [6] provides, among others, an in-depth description of the current developments in IT security and the German conditions of IT security including outlines of the current exposure in Germany. BSI reported an increase of 20% in the number of known malicious program versions from 2015 to 2016, up to 560 million a year. At the same time, current conventional defence measures are continuing to lose their effectiveness. Hence, overall awareness of cybersecurity threats of the public as well as of legislators, operators and their owners is strongly increasing.

Malicious programs are generally installed with the involvement of the user, meaning that technical protective measures are circumvented and attackers are able to penetrate protected networks. IT security must be considered and implemented as an overarching concept which also comprises user involvement.

CYBERSECURITY ASPECTS FOR NUCLEAR FACILITIES

Many elements or actions in the nuclear area enhance security. For example, the containment structure of a nuclear power plant protects the reactor from a terrorist assault. However, such actions are, of course, ineffective in the case of cyber-attacks. Targeted advanced persistent threats like Stuxnet are the most feared attack scenarios in any business domain and also in the nuclear field. Therefore, the Federal Government has issued the Directive for the Protection of IT Systems in Nuclear Installations [7].

Observations from the near past show that cyber threats have also been directed on software-based instrumentation and control (SB I&C) systems of industrial processing plants. Thus, cybersecurity has to be applied at the level of I&C and IT equipment while considering the potential impact of manipulations on safety functions and safety objectives.

Because penetration tests on such systems are difficult, an appropriate evaluation model is needed based on prior and posterior information and back propagation calculations. In [2] a methodology is described which uses analytical results from the Bayesian network model in an event tree model.

For implementing SB I&C system internal properties to support cybersecurity or to control the determined security requirements, a general strategy has to be in force which also addresses the mutual impact on safety and security. Some examples where a potential conflict has to be resolved are given in [8], such as:

- The implementation of a cybersecurity feature or control shall not adversely impact the performance, effectiveness, reliability or operation of safety functions supported by SB I&C systems;
- If cybersecurity features are implemented in safety system displays and controls, they shall not adversely impact the operator's ability to maintain the safety of the plant;
- Cybersecurity features and controls included in safety systems should be developed and qualified to the same level of qualification as the systems.

A distinct cybersecurity issue is to develop and maintain a common SB I&C procurement strategy for the system vendor and the component suppliers. Suppliers should meet the same security requirements as the vendor responsible for the final product. Finally, the end-use nuclear power plants have the greatest share of responsibilities to prevent a cyber-attack on their critical digital assets (CDA). Successfully implemented digital instruments regarding access of CDA by network and personnel, tamper prevention and detection as well as cyber-attack identification and response are discussed in [9].

According to the new added § 44b in the German Atomic Energy Act [10], licensees shall report impairments of their information technology systems, components or processes which may lead to or already have led to a threat or disturbance of the nuclear safety of the relevant installation or practice, without delay to BSI. This report must contain information about the disturbance and about the general technical conditions, especially of the supposed or actual cause, and about the information technology affected. BSI shall transfer these reports to the federal licensing and supervisory authorities that are responsible for nuclear safety and security without delay which requires the support by the Incident Registration Centre of the Federal Office for the Safety of Nuclear Waste Management (BfE).

One event of malicious software occurred in a German nuclear power plant [5]: over the course of preparations for inspection work, malicious programs were discovered in a computer system that had been retrofitted in 2008 with data-visualization software accompanying equipment for moving nuclear fuel rods. Viruses had also infected 18 removable data drives associated with computers not connected to the plant's operating systems.

The viruses found on the visualisation computer and on the removable data drives were Ramnit and Concker. Ramnit targets Microsoft Windows software systems and is designed to steal files and allow an attacker to remotely control a system that is connected to the Internet. It is often spread using removable data sticks. Concker which can spread through networks and jump onto removable data drives was designed to obtain login information and financial data. The infection could therefore have been originally transferred onto one of these USB storage devices using a PC connected to the Internet which had been infected with the malicious software online. The USB storage device was then used at a later point in time on the visualisation computer and was thus able to infect the unprotected computer even though it was not connected to any network.

No damage occurred to the nuclear power plant itself, the associated infrastructure or the information technology. However, the operator incurred costs in terms of the working time involved in reconstructing the course of events, the ongoing analysis and the subsequent cleaning of the computers and data storage devices affected.

CONCLUDING REMARKS

Cybersecurity reaches very high importance as the BSI identified a new quality of the nature of this threat for every type of critical infrastructure.

The main gateways for cyber-attacks are unchanged and remain critical:

- Vulnerabilities exist in often used software, in some cases also hardware, which enable attackers to remove information or gain control over systems.
- Attackers have botnets available which have been developed and are executed in an organised manner for distributing malicious software or spam emails on a mass scale.
- Users also often fail to apply conventional straightforward security measures.

In that context, a research project has been performed on cybersecurity at nuclear facilities [11]. This study focuses on characterizing what several countries are currently doing at the national level and introduces a potential model for developing a national approach to cybersecurity at nuclear facilities. One recent example describing the civil nuclear cybersecurity strategy for the United Kingdom is provided in [11].

Nuclear facilities – in operation or being built – have progressively become heavily reliant on digital I&C systems or computer-based information systems. This is a consequence of the disappearance from the market of analogue products as the digitalization of operational functions and working processes increases in quality and efficiency. This development gives rise to new threats confirmed by the publications of security vulnerabilities in the area of process control and automation systems. Thus, further efforts are needed in ensuring that cybersecurity is acknowledged and fully referenced in other domains protecting the operation of nuclear facilities (safety, physical security, nuclear material accountancy and control). In particular, in some fields like instrumentation and control, the interaction between the cyber and physical areas is so strong and inextricable that they are coming into fields of studies and analysis of their own [1].

Current questions about cybersecurity arising from the increasing use of digital I&C systems in nuclear power plants are also being addressed by the research project SMARTEST where a test method for the detection of weak points of software-based control systems should be developed. The project will be completed in June 2018. Some information on modelling of techniques regarding attacks is shown in [12].

In general, cybersecurity concerns should be extended to cover the full lifecycle of nuclear facilities and their components. Therefore, cybersecurity should become a fully incorporated factor in such activities associated with the operation of nuclear facilities like the management of the nuclear supply chain, instrumentation certification procedures, personnel security issues, core training curricula or threat assessment.

In order to protect nuclear facilities and, in particular, nuclear power plants from dynamic, more and more evolving cyber-attacks, an overarching framework guiding cybersecurity, e.g. by institutionalizing cybersecurity, mounting active defence, reducing complexity and pursuing transformation is necessary [13].

In Germany, one is already facing numerous attacks by cybercriminals. Since the introduction of the notification obligation, in total 34 notifications have been received by the BSI until 30 June 2017. 18 of these notifications were in the information technology and telecommunications sector, 11 in the energy sector including the event of malicious software that occurred in a German nuclear power plant, three in the water sector, and two in the food sector. It is to be feared that attacks on hospitals, logistics and energy infrastructure will continue to increase.

A recent report proposed a framework for the energy sector including nuclear in order to address the challenges found [14]. This framework consists of four strategic priorities: management of risks and threats, cyber defence, cyber resilience, as well as the capacity and competences needed to take action in case of a cyber-attack. This report suggests that the European Commission may set up a common European cyber response framework as part of potential future legislative acts.

Received 6 August 2017
Accepted 15 December 2017

References

1. IEC 61226: 2015-08, draft. Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions.
2. Shin J., Son H., Heo G. Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*. 2017. Vol. 49. P. 517–524.
3. *Cyber Security at Nuclear Facilities: National Approaches.* Institute for Security and Safety, June 2015.
4. Khattak M. A., et al. Review of cyber security applications in nuclear power plants. *Journal of Advanced Research in Applied Sciences and Engineering Technology*. 2017. Vol. 7. Iss. 1. P. 43–54.
5. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).* Bundesgesetzblatt Jahrgang. 2015. Teil I. Nr. 31.
6. *The State of IT Security in Germany.* Federal Office for Information Security-BSI, 2016.
7. *Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT).* Federal Ministry for the Environment, Nature Conservation and Nuclear Safety – BMUB. Announcement of July 8th, 2013. GMBl. 2013. No. 36. P. 711 (without text).
8. IEC 62859, Ed. 1.0: 2016. Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coordinating safety and cybersecurity.
9. Spear T., Smith N. Implications of digital instrumentation on nuclear cybersecurity. *Nuclear News*. 2016. Vol. 59. No. 13. P. 32–37.
10. *Act on the Peaceful Utilisation of Atomic Energy and the Protection against Its Hazards* (Atomic Energy Act) of 23 December 1959, as amended and promulgated on 15 July 1985, last amendment of 26 July 2016, corrected on 15 December 2016.
11. *Civil Nuclear Cyber Security Strategy*. Department for Business, Energy & Industrial Strategy, 2017.
12. Fischer R., Clausing R., Dittmann J., Kiltz S., Ding Y. Modeling attacks on critical infrastructure: a first summary of existing approaches. *47th Annual Meeting on Nuclear Technology (AMNT), May 12–14, 2016, Hamburg, Germany.*
13. Van Dine A., Assante M., Stoutland P. *Outpacing Cyber Threats. Priorities for Cybersecurity at Nuclear Facilities.* Nuclear Threat Initiative, 2016.
14. *Cyber Security in the Energy Sector, Recommendations for the European Commission on* a *European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.* Energy Expert Cyber Security Platform (EECSP) Report, 2017.

Heinz-Peter Berg

YPATINGOS SVARBOS INFRASTRUKTŪRŲ KAIP BRANDUOLINĖS ENERGETIKOS ĮRENGINIŲ KIBERNETINIS SAUGUMAS

Santrauka

Pastaraisiais metais kibernetinis saugumas tapo esminis, kai kalbame apie bendrą įvairių ypatingos svarbos infrastruktūrų, pavyzdžiui, pramonės, geležinkelių, ligoninių ir branduolinės energetikos objektų, saugumą. Keičiasi grėsmių tipai, reikalaujama pinigų ne tik iš paveiktų organizacijų, bet į tai įtraukiamos ir valstybės. Kibernetinių atakų daugėja, jos nukreiptos į visus ypatingos svarbos infrastruktūrų objektus, ir šie išpuoliai yra pripažįstami kaip reali problema.

Straipsnyje (kaip pavyzdys) yra pristatoma dabartinė patirtis ir ateities veikla, susijusi su Vokietijos branduolinės energetikos objektais, Vokietijos IT saugumo įstatymu ir kitais atitinkamais reguliuojančių institucijų reikalavimais. Be to, aptariama tarptautinė veikla, vykdoma šioje srityje.

Raktažodžiai: IT saugumas, kibernetinis saugumas, Vokietijos branduolinės veiklos reguliavimas, tarptautiniai projektai