Kurzfassung

Cybersecurity in Kernkraftwerken und ihre Anwendung in weiteren industriellen Infrastrukturen

Stromerzeugung ist verstärkt auf dezentralisierte und vernetzte Rechnersysteme angewiesen, die Begriffe wie „Industrial Internet of Things“ des Internet of Things oder „Industrie 4.0“ bahnen sich heute ihren Weg auch in diese bedeutende Industriebranche. Die Lösungen einer gezielten Ausnutzung von Fehlern und Schwachstellen nehmen mit der Komplexität zu, dem Vernetzungsgrad und mit der dezentralisierten Struktur. Die inhairen strenge Sicherheitsanforderungen des Kernenergiebereiches und die langjährige Berücksichtigung der Sicherheitsanforderungen der Kernenergianwendungen institutionalisiert die Entwicklung von Produkten und in projektbegleitenden Maßnahmen nennt sich Cybersecurity in Kernkraftwerken, sowie auch deren zahlreichen Übertragungsmöglichkeiten auf andere kritische Infrastrukturen, um sie gegen Cyberangriffe und Industriespionage zu wappnen.

Introduction

This technical contribution provides a snapshot of the current cyber security efforts in different industry domains. We argue that stringent security controls (countermeasures) that are already in place for nuclear power plants (NPP) can be ported to other industry domains. A reason for this is that the nuclear domain is more formally regulated, thus graded security requirements were already mandated long before the critical infrastructure debates started and before gradual enforcement of the European and national legislation.

Note: Generally, in the nuclear and industrial automation domain, the term “control” is used mainly to denote Instrumentation and Control (I&C), Industrial Automation and Control Systems (IACS) or SCADA (Supervisory Control and Data Acquisition) referring to control theory tasks. However, in the security context, the term “Security Control” is ubiquitous, and means any countermeasure that can reduce the systems risk due to security threats. Countermeasures are not limited to add-on provisions at the components or systems level. For example, they also include provisions at the software source code level.

In Section 1, we will provide an overview of current international and national cyber security guidance, and how this guidance evolved for IAEA, Nuclear IEC and selected countries. Section 2 summarises the increasing cyber security efforts for Industrial Automation and Industry 4.0 as well as its Chinese “Manufactured in China 2025” and US “Industrial Internet of Things” counterparts. Section 3 provides reasons for the portability of Security Controls from Nuclear to other industrial infrastructure. Summary provides an outlook on the newest cyber security-related activities in the different domains, and concludes with a summary of the main steps that are necessary for achieving and maintaining a target security level.

1 Cyber security and safety requirements for NPPs

In the nuclear domain, for Safety, Human Factors Engineering, Physical Security, Radiation Protection and Cyber Security, the international top-level guidance is provided by the International Atomic Energy Agency (IAEA). The IAEA guidance is regularly updated based on priorities set by yearly or bi-yearly meetings of representatives of all IAEA member states. The overall IAEA Cyber Security guidance is refined, e.g. for Instrumentation & Control (I&C) and Electrical Systems (ES), by the Nuclear IEC subcommittees. However, each country may supersede the international guidance by providing a mandatory higher priority regulation, as will be addressed in section 1.4 for selected countries.

1.1 Stringent and graded security requirements for I&C already since 1986

Safety and security grading are essential when addressing critical industrial infrastructures. Grading by Safety Categories in IEC 61508 and Safety Classes in IEC 61513, were already in place since the first edition of these standards. The software-specific requirements for software implementing Category A or Category B and C I&C functions, are also graded by the respective standards IEC 60880:1996 and IEC 62138. The first edition of IEC 60880:1996 already contained explicit requirements on security during software development and security during software deployment, two essential phases in the software development lifecycle.

1.2 Overall IAEA Cyber security Guidance

The IAEA Cyber security Guidance is published in the IAEA Nuclear Security Series (NSS). Currently the top-level guidance is IAEA NSS 17 from 2011. Developing this guidance took several years with considerable input by member states provided since 2006, and essential agreements being achieved during the first major IAEA cyber security conference in summer 2011. IAEA NSS 17 introduces a graded security approach with 5 security levels and recommendations on security zones.

IAEA NSS 17 is complemented by IAEA NSS 8 on preventive and protective measures against insider threats, and further IAEA NSS guidance, including IAEA...
Cyber security in nuclear power plants

1.3 Nuclear IEC Cyber security Standards

Subsequently, the three major Nuclear IEC cyber security standards will be introduced.

1.3.1 The Top-level Nuclear IEC Cyber security Standard

After initial attempts to structure the top-level nuclear IEC standard according to nuclear safety and other criteria, finally, a core-team devised the alignment with the most popular information security standard ISO/IEC 27001:2005 then in place. This structuring was proposed mainly in order to reduce the initial training needs of security staff already familiar with the mainstream standards, and in order to avoid annexes with cumbersome mappings.

While ISA99 experts were involved in the development of the first top-level nuclear IEC 62645:2013 cyber security standard, an alignment with ISA99 industrial cyber security standards or the corresponding IEC 62443-x-x series were not yet available and because the Security grading follows a different approach, as will be addressed in a subsequent section.

1.3.2 Coordinating safety and cyber security by IEC 62859

Whether safety and cyber security should be considered jointly or subsequently, is a part of ongoing debates in different industry domains. For nuclear, the security grading is directly related to the potential impact of a security attack on nuclear safety. Figure 1 shows the hierarchical refinement from Safety Objectives (level 1) down to I&C Functions (level 3 and 4). Main safety objectives are control of reactivity, residual heat removal and confinement of radioactive material.

Cyber security is applied at the level of I&C and IT equipment while considering the potential impact of manipulations on Safety Functions and Safety Objectives. IEC 62859:2016 [1] specifies the main requirements for coordinating safety and cyber security. In other industries, work on this important topic was just started, e.g. by the new working group WG20 of IEC TC65.

1.3.3 Detailed security controls for I&C by IEC 63096

Similar to the alignment of IEC 62645 with ISO/IEC 27001, the new working draft IEC 63096 is being aligned with the ISO/IEC JTC1/SC27 WG1 standard ISO/IEC 27002:2013. This nuclear IEC standard extends the generic security controls of ISO/IEC 27002 by recommendations for each security level: BR (Baseline Requirements), S3, S2 and S1 (highest security level). It also provides guidance for the main I&C and ES (Electrical Systems) lifecycle phases: Product & Platform Development, Engineering and Operation & Maintenance. Additionally, it provides security control specific guidance for legacy I&C and ES systems.

As a sector-specific standard, similar to ISO/IEC 27009 [3], for non-nuclear utilities, IEC 63096 provides guidance that is structured and formatted in principle in line with ISO/IEC 27009 which provides common guidance on the elaboration of sector-specific security controls and Information Security Management Systems (ISMS) standards.

1.4 International and national nuclear cyber security regulations

Figure 2 lists the international standards discussed above, along with the national standards for Germany, USA and the UK. In Germany, SEWD (Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter/Protection against Disruptive Acts or Other Intervention of Third Parties) is a requirement found in § 6 para. 2 no. 4 Atomic Energy Act. released in 1959.[7]. Licenses for the storage of nuclear fuels are only granted once risks and threats, as a result of SEWD, can be considered as negligible. Created by Congress in 1974, the USA’s NRC regulates commercial nuclear power plants and other uses of nuclear materials. NRC RG 5.71 [4] provides guidelines for the protection of digital computer and communication systems and networks from cyberattacks, against which licensees should provide assurance. The Nuclear Energy Institute (NEI) 08-09 “Cyber Security Plan for Nuclear Power Reactors” provides a generic template for a cyber security plan, which must be used by licensees to develop their cyber security plans to be submitted to the NRC [8]. The HMG IA (Information Assurance) Standard is intended for us by IA practitioners, working especially with UK Government ICT systems, as the foundation for their Information Risk Management Policy. This standard provides a methodology by which these practitioners can “identify, assess and determine the level of risk to an ICT system and a framework for the selection of appropriate risk treatments.”

Requirements from these international nuclear Cyber Security standards are applicable for the whole nuclear power plant. Figure 3 shows the scope of applicability.
2 Gradual consideration of information security in Industry 4.0 and IoT

Industry 4.0 and “Manufactured in China 2025” are governed by a “Reference Architecture Model Industry 4.0” (RAMI) or similar which are typically represented by cubes subdivided as 6x6x6 or 5x5x5. The 3 axis of the cube are “Layers”, “Hierarchy Levels” and “Value Streams”. None of the 6 Layers (Business, Functional, Information, Communication, Integration and Asset) explicitly contains cyber security. Similarly along the other two axes, cyber security is not explicitly included. This is due to the fact that security and interoperability are considered as integral components in multiple of the 3D elements that built up the complete cube, see Figure 5.

2.1 Generic information security

One purpose of generic security standards is to be applicable by any size of an organization, e.g. a one-employee service provider or a multinational organization. The ISO/IEC 27000 series takes credit on meeting this criterion. Still, beyond these generic information security standards in the 27000 to 27021 range, additional standards in the 27031 to 27050 and other ranges provide more in-depth guidance.

2.2 IT security for power generating plants

VGB-S-175 addresses generic security requirements, Defense-in-Depth principles, redundancy and diversity, risk management, risk analysis and security countermeasures for both, new built and power plant modernization projects.

Furthermore, VGB provides guidance on intrusion detection and prevention (addressed in more detail by ISO/IEC 27039), patch management (addressed in more detail by IEC 62443-2-3), security gateways (addressed in more detail in ISO/IEC 27033-4), wireless (ISO/IEC 27033-6), documentation of security incidents (ISO/IEC 27035-3) and additional countermeasures.

2.3 Emerging industrial automation security

Cyber security for Industrial Automation mainly builds on the ISA99 specific standards which are published as IEC62443-x-x.
Cyber security in nuclear power plants

The 13 parts of this series are not yet complete. The security grading is based on the risk an attacker imposes and on its strength. This regularly leads to controversy, as the strength of an attacker can change over time, e.g. today’s “script kiddies” have other malicious tools as compared to 10 years earlier.

2.4 Initial Industry 4.0 and IoT proposals

Despite its current incompleteness, IEC 62443-x-x builds a solid basis for cyber security in the Industry 4.0 RAMI framework. Interoperability is a key component of Industry 4.0. The multipart IEC 62541 defines the Open Connectivity Unified Architecture (OPC UA) not just as a communications protocol, but as a communication architecture that supports among other services, interoperability between digital technologies from different vendors. The services, as provided by the layers of the platform-independent OPC UA, include the semantics of an information model, address spaces, discovery services, alarm functions, etc.

AREVA NP implements Embedded OPC UA, for example, in its SIPLUG® family of monitoring sensors, as shown on Figure 6. Hence, it can directly be connected to reporting and trend surveillance systems. This feature drastically reduces the costs for interconnecting the respective sensor devices with equipment from different vendors, as deployed worldwide at NPP sites [6].

3.1 Joint functional safety and cyber security consideration

One benefit of IEC 62859:2016, as compared to generic safety & security related solution, is its well delimited context of the applicability for NPPs. The grading is well defined based on the maximum impact in the nuclear context. The transition between the safety states is also well understood due to comprehensive deterministic and probabilistic safety analyses.

These results from the functional safety experts can directly be leveraged by the security staff. This approach can be transferred and adjusted for other business domains. The security grading has to be adjusted to the possible impact levels in the respective business domain. Similarly, an analysis is needed and feasible on which security events can lead to a similar impact as the respective safety events (like equipment faults, failures of supporting assets, spurious actuations). Based on this mapping, a risk management process can be modified in order to adjust and justify the criticality assignment (assignment of security degrees to systems) and to apply complementary security controls.

3.2 Security grading

The generic information security standards like ISO/IEC 2700x define no security grading: also called security levels or levels of trust. Unfortunately, in some industries the grading may be defined based on criteria that may change over time. Thus, the strength of an attacker may change while the impact will not change or only in well-justified (and easily identifiable) circumstances, e.g. after power up-rating of an NPP.

As for nuclear, in implementing a long-term stable impact-based grading approach, the overall risk management and security control adjustment requirements could be considerably reduced.

3.3 Security awareness training

Safety Culture and Security Culture have a long tradition in nuclear, see e.g. IAEA NSS 7 “Nuclear Security Culture” from 2008. With humans as the strongest and also as the weakest link in the security chain, specific security training is essential. Such training can be adapted for other business domains and for different staff roles, like operators, service engineers, physical security staff, cyber security staff and management.

3.4 Strong preventive security controls

Often mimicking the activities of their counterparts in the office IT world, cyber security safety staff deploy network or host monitoring systems, like Network and Host Intrusion Detection Systems (IDS). These detective security controls may be the only option in an office IT environment, where the exact content and frequency and destination of messages sent via communication networks cannot be predicted. However, for nuclear and for many other industries, like process automation and discrete manufacturing, the data exchange is of a periodic nature, e.g. with fixed communication cycle times.

This allows the implementation of strong Preventive Security controls beyond baseline firewall filtering. In many cases, the network architecture may be adjusted to include Data Diodes as (preferably optical) Physically Unidirectional Security Gateways.

Applying these network architecture level improvements ensures reaching and maintaining the required target security degree. An example of preventive security control is provided in Figure 7. On the left half of the figure, an automation system is shown in its standard configuration. On the right half of the figure, the automation system is protected by patented software called OPANASec. OPANASec is both a preventive and a detective measure against cyber-attacks.

Fig. 6. SIPLUG® OPC UA based example.

Part 2 of IEC 62541 provides the security framework for OPC UA, the main aim of which is to provide security for the data exchanges facilitated by this architecture. While there seems to be general acceptance on OPC UA as a part of Industry 4.0 and IoT, the final hard real-time communication protocols and the respective security solutions are still to emerge.

3 Portability of cyber security knowledge and features from nuclear to other industrial infrastructures

The subsequent sections exemplify some domains where solutions from the nuclear domain can be adapted and applied to other domains.

3.4 Initial Industry 4.0 and IoT proposals

Despite its current incompleteness, IEC 62443-x-x builds a solid basis for cyber security in the Industry 4.0 RAMI framework. Interoperability is a key component of Industry 4.0. The multipart IEC 62541 defines the Open Connectivity Unified Architecture (OPC UA) not just as a communications protocol, but as a communication architecture that supports among other services, interoperability between digital technologies from different vendors. The services, as provided by the layers of the platform-independent OPC UA, include the semantics of an information model, address spaces, discovery services, alarm functions, etc.

AREVA NP implements Embedded OPC UA, for example, in its SIPLUG® family of monitoring sensors, as shown on Figure 6. Hence, it can directly be connected to reporting and trend surveillance systems. This feature drastically reduces the costs for interconnecting the respective sensor devices with equipment from different vendors, as deployed worldwide at NPP sites [6].

3.1 Joint functional safety and cyber security consideration

One benefit of IEC 62859:2016, as compared to generic safety & security related solution, is its well delimited context of the applicability for NPPs. The grading is well defined based on the maximum impact in the nuclear context. The transition between the safety states is also well understood due to comprehensive deterministic and probabilistic safety analyses.

These results from the functional safety experts can directly be leveraged by the security staff. This approach can be transferred and adjusted for other business domains. The security grading has to be adjusted to the possible impact levels in the respective business domain. Similarly, an analysis is needed and feasible on which security events can lead to a similar impact as the respective safety events (like equipment faults, failures of supporting assets, spurious actuations). Based on this mapping, a risk management process can be modified in order to adjust and justify the criticality assignment (assignment of security degrees to systems) and to apply complementary security controls.

3.2 Security grading

The generic information security standards like ISO/IEC 2700x define no security grading: also called security levels or levels of trust. Unfortunately, in some industries the grading may be defined based on criteria that may change over time. Thus, the strength of an attacker may change while the impact will not change or only in well-justified (and easily identifiable) circumstances, e.g. after power up-rating of an NPP.

As for nuclear, in implementing a long-term stable impact-based grading approach, the overall risk management and security control adjustment requirements could be considerably reduced.

3.3 Security awareness training

Safety Culture and Security Culture have a long tradition in nuclear, see e.g. IAEA NSS 7 “Nuclear Security Culture” from 2008. With humans as the strongest and also as the weakest link in the security chain, specific security training is essential. Such training can be adapted for other business domains and for different staff roles, like operators, service engineers, physical security staff, cyber security staff and management.

3.4 Strong preventive security controls

Often mimicking the activities of their counterparts in the office IT world, cyber security safety staff deploy network or host monitoring systems, like Network and Host Intrusion Detection Systems (IDS). These detective security controls may be the only option in an office IT environment, where the exact content and frequency and destination of messages sent via communication networks cannot be predicted. However, for nuclear and for many other industries, like process automation and discrete manufacturing, the data exchange is of a periodic nature, e.g. with fixed communication cycle times.

This allows the implementation of strong Preventive Security controls beyond baseline firewall filtering. In many cases, the network architecture may be adjusted to include Data Diodes as (preferably optical) Physically Unidirectional Security Gateways.

Applying these network architecture level improvements ensures reaching and maintaining the required target security degree. An example of preventive security control is provided in Figure 7. On the left half of the figure, an automation system is shown in its standard configuration. On the right half of the figure, the automation system is protected by patented software called OPANASec. OPANASec is both a preventive and a detective measure against cyber-attacks.

Fig. 6. SIPLUG® OPC UA based example.

Part 2 of IEC 62541 provides the security framework for OPC UA, the main aim of which is to provide security for the data exchanges facilitated by this architecture. While there seems to be general acceptance on OPC UA as a part of Industry 4.0 and IoT, the final hard real-time communication protocols and the respective security solutions are still to emerge.

3 Portability of cyber security knowledge and features from nuclear to other industrial infrastructures

The subsequent sections exemplify some domains where solutions from the nuclear domain can be adapted and applied to other domains.

Fig. 7. Security control using patented software OPANASec.
on the automation system. It protects the system's integrity by detecting any read or write access to the automation system and announces it to the operator in the main control room, by means of a red traffic light for example. It also prevents information retrieval and any modifications of the automation system by locking read and write access.

3.5 Forensic readiness

Reports on system intrusions and manipulations without a trace to the identity and location of hackers or threat agents are, in general, frequently reported in technical magazines, but also more and more by commercial media. Typically, the reason for this is that no forensic readiness specific security controls are in place. Also, the implementation of the forensic readiness security controls (e.g. log files related) may not be adequate for the target security level.

As for nuclear, this can be improved by systematically performing attack tree analyses and assigning appropriate forensic readiness security controls in line with the security grading.

3.6 Incident response

While incident response on Safety related incidents has a long tradition with nuclear, cyber security incident management is currently in the focus of the first IAEA financed cyber security R&D with 14 international partners.

As one of the major partners in the IAEA Coordinated Research Proposal (CRP) J02008, AREVA NP, together with one of its German partner Universities, can leverage the results for other business domains.

3.7 Security testing

The appropriate assignment of security controls based on a continuous risk management, is essential for achieving a high security posture. However, the implementation or configuration of some security controls may be flawed. Even more important, the implementation and configuration of the software and FPGA-based systems may include vulnerabilities, some of which may be security relevant.

This mandates a selective, prioritised, in-depth penetration and fuzz-testing. We are currently working on an extensive R&D together with multiple German partner universities and several Cyber security PhD candidates, as part of the partial-  

3.8 Security modelling

The I&C and ES Architecture of NPPs comprises multiple distributed I&C systems that are built-up from several subsystems and components. Modelling these systems together with models of the physical process (including pumps, valves …) is common practice for several decades. Typically, this includes simulators which run in real-time or faster than real-time. There are modelling approaches which include the security control definitions into exist-  

3.9 Security asset management

Implicit asset identification is unavoidable in order to purchase and install the equipment. However, an asset management in line with ISO 55000 and ISO/IEC 19770-x (4 layers of maturity) is needed in order to leverage the relevant knowledge about assets. This is a precondition for correct patch management. It can be well applied in many industries.

3.10 Secure human-machine interaction

Main control rooms and I&C maintenance rooms equipped with HMI equipment are common for power plants and stringently regulated for NPPs, e.g. with regard to the explicit documentation for plant operators. Different solutions exist for secure human-machine interaction. An example of it is a Qualified Display System (QDS), which limits functionalities accessible to the operator. The respective security provision may be transferred or adapted for other HMI related user activities.

3.11 Domain specific application security controls

The semi-formal approach of the up-coming ISO/IEC 27034-x is applied to the nuclear context. A key concept is the Application Security Controls (ASCs). An ASC provides a semi-formal definition of a security control. It also includes the indication of the security grade that the ASC can meet, the status of the ASC implementation (e.g. whether verification and validation were completed), the role assignment according to RACI (Responsible, Accountable, Consulted, Informed) and the specification of links to other ASCs.

Summary

Monitoring agencies like the “US Industrial Control Systems Cyber Emergency Response Team (ISC-CERT)”, the “French National Agency for Information systems’ security” and the “German Federal Office for Information Security” (BSI) all record steep increases in cyberattacks on companies and institutions in general, and on critical infrastructures in particular. For example, the BSI reported an increase of 20% in the number of known malicious program versions, from 2015 to 2016, up to 560 million a year. Hence, overall public awareness of cyber security threats, as well as of legislators, of power plant operators and of their owners, is also on a steep rise. Preemptive cyber security measures not only avoid loss of revenues, costs of crisis management, costs of reimbursements and higher insurance premiums. They also avoid upcoming legal penalties for

siders advanced features, like ASC inheritance, not yet included in the current ISO/IEC 27034-x standard versions.

As an example of the adaptation of the ASCs concept, the default grading of 10 levels of trust has to be adjusted to the domain specific grading, or a grading has to be introduced for the target domain. Additionally, the accompanying concepts of an Organization Normative Framework and an Application Normative Framework can be adapted.

This is in line with the key concepts of ASCs, which promote the development and delivery of high-quality specialised ASCs by standards-conforming sub-suppliers.

3.12 Advanced persistent threats

Targeted Advanced Persistent Threats (APT), like Stuxnet, are the most feared attack scenarios in any business domain. The combination of several of the aforementioned approaches, including a comprehensive asset management, semi-formal modelling of the assets and supporting assets, semi-formal description of the Application Security Controls, targeted security testing, Forensic Readiness Security Controls and further security controls related to the secure software development will support in systematically increasing the security posture and thus, the effort needed to be spent by an APT agent.

Similar APT analysis can be performed for other business domains, provided the above listed preparations, like asset management and semi-formal modelling are already in place or are implemented.

The knowledge areas described above should be organised in different products and services offered to selected critical industries for efficient application. An example of how to implement this is shown in Figure 8.

Cyber security in nuclear power plants
infringement of an increasingly intransigent legislation.

AREVA NP’s long-standing expertise in nuclear cyber security relies on in-depth knowledge of industrial and legislative requirements and of the corresponding companies’ protection needs. As shown above, it applies to a great extent to any industrial infrastructure using control systems. Not only the energy sector, but also the manufacturing sector, the water and wastewater systems sector and the defense industrial base sector benefit from such an expertise.

References


Yes, I would like order a subscription of VGB PowerTech. The current price is Euro 275.– plus postage and VAT. Unless terminated with a notice period of one month to the end of the year, this subscription will be extended for a further year in each case.

Return by fax to
VGB PowerTech Service GmbH
Fax No. +49 201 8128-302

or access our on-line shop at www.vgb.org | MEDIA | SHOP.
VGB PowerTech DVD 1990 bis 2016:
27 Jahrgänge geballtes Wissen rund um die Strom- und Wärmeerzeugung
Mehr als 27.000 Seiten Daten, Fakten und Kompetenz

Bestellen Sie unter www.vgb.org > shop

Jetzt auch als Jahres-CD 2016 mit allen Ausgaben der VGB PowerTech des Jahres: ab 98,- €