VTT Technical Research Centre of Finland

Survey of cybersecurity standards for nuclear instrumentation and control systems

Linnosmaa, Joonas; Papakonstantinou, Nikolaos; Malm, Timo; Kotelba, Adrian; Pärssinen, Juha

Published in:
International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021

Published: 15/11/2021

Document Version
Publisher's final version

Survey of cybersecurity standards for nuclear instrumentation and control systems

Joonas LINNOSMAA[1)], Nikolaos PAPAKONSTANTINOU[1)], Timo MALM[1)], Adrian KOTELBA[1)], Juha PÄRSSINEN[1)]

1) VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, Finland, firstname.surname@vtt.fi

***Abstract*—This survey paper, based on literature and discussions with nuclear stakeholders, identified cybersecurity standards for nuclear instrumentation and control architectures and systems. From among the identified standards, the most significant ones, namely IEC 62443 series, ISO 27K series, IEC 62645, IEC 62859 and IAEA's NSS 17, were recognised and their main topics are further introduced. Additionally, it briefly discusses the importance and role of cybersecurity standards for the domain.**

Keywords—cybersecurity; industrial instrumentation and control systems; standards and frameworks

I. INTRODUCTION

Industrial cybersecurity is a domain governed by standards and guidance frameworks, which generally set forth techniques and methods to defend the cyber environment of the organization. Cybersecurity environment (sometimes referred as cyberspace) generally comprises of the humans (users), systems, components, software, services, processes and data connected directly or indirectly to networks. The goal of these frameworks and standards are to prevent and mitigate the cybersecurity threats and vulnerabilities, thus reducing cybersecurity risks. There are numerous standards and frameworks available, developed and published by various cybersecurity stakeholders, each one introducing their own, often unique, requirements, themes, topics and methods for securing systems and managing cybersecurity. Some of the concepts are shared between them, while some take different paths. This paper surveys and identifies the main cybersecurity standards for industrial control systems, more specifically focusing on nuclear instrumentation and control (I&C) cybersecurity from Finnish perspective. Special focus is on the relations between Finnish YVL-guides (regulatory standards) and other international standards (from IEC and ISO).

Chapter II first identifies nuclear cybersecurity standards focusing on cybersecurity of industrial instrumentation and control systems in the design or operation phase. Then the most relevant standards from the Finnish perspective are recognised. Finally Chapter II gives an introduction to each most relevant cybersecurity standards identified, where their main topics are presented from I&C point of view. Chapter III includes brief discussion and the conclusions from the work.

II. CYBERSECURITY REQUIREMENTS AND STANDARDS

A. Survey of cybersecurity standards

Literature and web was surveyed for relevant cybersecurity standards. The survey was mainly based on author's previous knowledge of the domain, as well as exploring publishers' databases (e.g. IEC/ISO databases) and other cybersecurity survey papers (such as [1], [2], [3], [4]). No exact match for the goal of this research was found from the literature, which would concern cybersecurity standards for nuclear I&C.

The following list presents the results for the cybersecurity standard survey for nuclear I&C systems and architecture. The gathered list is quite broad as our scope was to gather quite extensively all the main standards guiding the cybersecurity design of nuclear power plant. Thus, the list covers large range of design domains and categories from security management, IT and OT, architecture to system and to component design. The list was presented and discussed with Finnish nuclear stakeholders (STUK, the Finnish regulator, Fennovoima and TVO, two Finnish licence-holders) and accordingly it is expected to present quite a comprehensive list of cybersecurity standards in the domain from Finnish perspective. However, it is possibly that the survey has missing some.

ISO/IEC Security Standards

Generic

- ISO/IEC 13335-1 Information technology – Guidelines for the management of information technology security
- ISO/IEC 15408 series Information technology – Security techniques – Evaluation criteria for IT security
- ISO/IEC 27000 series Information technology – Security techniques – Information security management systems
- IEC 60870 series Telecontrol equipment and systems
- IEC 61850 Communication networks and systems for power utility automation
- IEC 62443 series Industrial communication networks – IT security for networks and systems
- IEC/TR 63069 Industrial-process measurement, control and automation - Framework for functional safety and security
- IEC TR 63074 Safety of machinery - Security aspects related to functional safety of safety-related control systems
- IEC 62351 series Power systems management and associated information exchange - Data and communications security

Nuclear specific

- IEC 60880 Nuclear Power Plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
- IEC 61500 Nuclear Power Plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions
- IEC 61513 Nuclear Power Plants – Implementation and control systems important to safety – General requirements for systems
- IEC 62138 Nuclear Power Plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions
- IEC 62645 Nuclear Power Plants – Instrumentation, control and electrical power systems – Cybersecurity requirements
- IEC 62859 Nuclear Power Plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity
- IEC 62988 Nuclear Power Plants – Instrumentation and control systems important to safety – Selection and use of wireless devices
- IEC 63096 Nuclear Power Plants – Instrumentation, control and electrical power systems – Security controls

IAEA Security Standards/Guides

- IAEA Nuclear Security Series No. 7 Nuclear Security Culture
- IAEA Nuclear Security Series No.8 Rev.1 Preventive and Protective Measures against Insider Threats
- IAEA Nuclear Security Series No. 10 Development, Use and Maintenance of the Design Basis Threat
- IAEA Nuclear Security Series No. 17 Computer Security at Nuclear Facilities
- IAEA Nuclear Security Series No. 23-G Security of Nuclear Information
- IAEA Nuclear Security Series No. 33-T Computer Security of Instrumentation and Control System at Nuclear Facilities

– IAEA Computer Security for Nuclear Security
– IAEA Computer Security Techniques for Nuclear Facilities
– IAEA Computer Security of I&C Systems at Nuclear Facilities
– IAEA Conducting Computer Security Assessments
– IAEA Computer Security Incident Response
– IAEA Computer Security during the Lifetime of a Nuclear Facility
– IAEA, INSAG-24, The interface between safety and security at nuclear power plants

IEEE Security Standards

– IEEE 7-4.3.2-2016: Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations
– IEEE 1686-2013: Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

NIST Cybersecurity Framework

– NIST Special Publication 800-82 Rev 2: Guide to Industrial Control Systems (ICS) Security
– NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems
– NIST Special Publication 800-53A Rev 1: Guide for Assessing the Security Controls in Federal Information Systems in Organizations
– NIST Special Publication 800-53 Rev 3: Recommended Security Controls for Federal Information Systems and Organizations

Other

– NRC Regulatory Guide (RG) 5.71: Cyber Security Programs for Nuclear Facilities
– NRC Regulatory Guide (RG) 73.54: Protection of Digital Computer and Communication Systems and Networks
– NRC Regulatory Guide (RG) 5.83: Cyber Security Event Notifications
– NRC Regulatory Guide (RG) 1.152 Rev 2 & 3: Criteria for Use of Computer in Safety Systems of Nuclear Power Plants
– Template for the Cyber Security Plan Implementation Schedule
– 10 CFRs: 73.54 & 73.55 & 73.56
– NEI 10-04 Rev 2: Identifying Systems and Assets Subject to the Cyber Security Rules
– NEI 13-10 Rev 5: Cyber Security Control Assessments
– NEI 04-04 Rev 1/NEI 08-09 Rev 6: Cyber Security Program for Power Reactors

Finnish YVL-guides by STUK (nuclear regulator)

– A.3 Leadership and management for safety
– A.4 Organisation and personnel of a nuclear facility
– A.5 Construction and commission of a nuclear facility
– A.11 Security of a nuclear facility
– A.12 Information security management of a nuclear facility
– B.1 Safety design of a nuclear power plant
– B.2 Classification of systems, structures and components of a nuclear facility
– B.7 Provisions for internal and external hazards at a nuclear facility
– C.5 Emergency arrangement of a nuclear power plant
– E.7 Electrical and I&C equipment of a nuclear facility

From the compressive list presented above, the most essential ones were picked for a closer study. The selection was done according to their importance to design of nuclear I&C systems from the Finnish perspective, where the major governing guideline is the YVL-guide A.12 'Information security management of nuclear facility', by Finnish nuclear regulatory authority STUK.

The standards selected to be reviewed further were IEC 62443 series, ISO/IEC 27K series, IEC 62645, IEC 62859, and IAEA Nuclear Security Series No. 17, additionally the review included ISO/IEC 15048 'Common Criteria' series. Fig. 1 depicts these standards and roughly their categorisation. Notable, it was discovered that each of them have also been used as referenced standards while the most recent version YVL-guide A.12 was developed (2021 version).

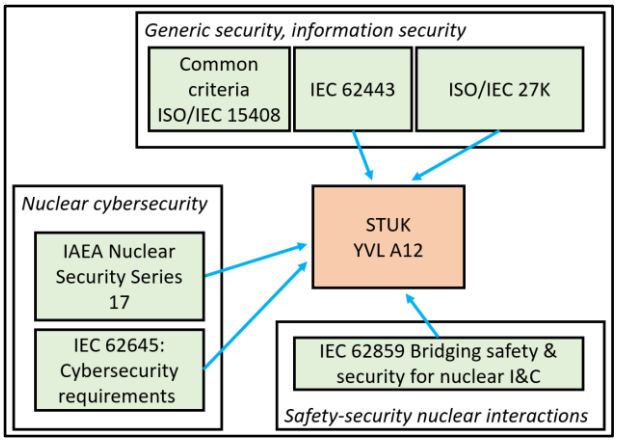

Fig. 1 Most important cybersecurity standards from Finnish perspective.

In the next subchapter, the standards from Fig. 1 are further introduced and their requirement topics are presented.

B. Introduction to selected cybersecurity standards and requirements

IEC 62443-series

The standard IEC 62443 family is developed continuously. Currently published versions can be divided into following groups.

General: General aspects, which are applied throughout the standard series. Including: 62443-1-1: Concepts and Models; 62443-1-2: Master Glossary of Terms and Abbreviations; 62443-1-3: System Security Conformance Metrics; 62443-1-4: IACS Security Lifecycle and Use Cases.

Policies and procedures: focus on people, organizations and processes. Including: 62443-2-1: Security Program Requirements for IACS Asset Owners; 62443-2-2: Implementation Guidance for an IACS Security Management System; 62443-2-3: Patch Management in the IACS Environment; 62443-2-4: Requirements for IACS Solution Suppliers; 62443-2-5: Implementation Guidance for IACS Asset Owners;

System: focus on technology aspects of systems. Including: 62443-3-1: Security Technologies for IACS; 62443-3-2: Security Risk Assessment and System Design; 62443-3-3: System Security Requirements and Security Levels.

Component: focus on requirements related to products and components. Including: 62443-4-1: Secure Product Development Lifecycle Requirements; 62443-4-2: Technical Security Requirements for IACS Components.

IEC 62443 standard introduce the three basic roles that affect in protecting industrial facilities from cyberattacks. These roles are: Product Supplier, System Integrator and Asset Owner. Each of these actors has a unique role to play in the design, development, marketing, operation, and maintenance of industrial cybersecurity solutions. Some parts of the standard family are dedicated to specific role, like asset owner (IEC 62443-2-1 and IEC 62443-2-4). [5]

The security levels defined by the standard represent the confidence that a system, zone, and/or its components can provide the desired level of security. Security levels are defined according to their typology:

– Target - This is the level of protection to be achieved for each area and path using a number of countermeasures (SL-T). This is the minimum target for SL-A. See also part 3-2 of the standard IEC 62443.

– Capability - This is the level of protection specific to a component or subsystem (i.e. part of conduit or zone) that allows the desired level of security to be expected (SL-C). See also part 3-3 and part 4-2 of the standard IEC 62443.
– Achieved: This is the level actually achieved by the intrinsic properties of the components that make up a zone or conduit and the potential contribution of countermeasures (SL-A). See also part 3-2 of the standard IEC 62443.

Security Level is defined as the measure of confidence that the System Under Consideration, Zone, or Conduit is free from vulnerabilities and functions in the intended manner [6]. The security levels are divided into five levels:

– SL 0: No special requirement or protection provided.
– SL 1: Protection against unintentional or accidental misuse.
– SL 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation.
– SL 3: Protection against intentional misuse by sophisticated means with moderate resources, specific knowledge about industrial automation and control systems and moderate motivation.
– SL 4: Protection against intentional misuse using sophisticated means with extensive resources, specific knowledge about industrial automation and control systems and high motivation. [7]

Foundational requirements (FR) are presented at IEC 62443-4-2, which focuses on components, products and security capability requirements (SL-C). The security levels are defined also for each foundational requirement (FR) based on their criticality within the system. For each foundational requirement there can be also component requirements and requirement enhancements [5]. The security level (SL-C) for the product is the minimum SL achieved over all of these evaluations [7].

– FR 1, Identification and authentication control, identifies and authenticates all users, before granting access into the system.
– FR 2, User control ensures that users have privileges to perform the required actions and monitors them.
– FR 3, Data integrity ensures the integrity of equipment and information in communication channels and storage directories.
– FR 4, Data confidentiality ensures that information flowing through communication channels and storage directories is not disturbed.
– FR 5, Restricted data flow segments the system into zones and conduits to avoid unnecessary data propagation.
– FR 6, Timely response to event, responds to security breaches with timely reporting and timely decision making.
– FR 7, Resource availability ensures system and asset availability during denial of service attacks.

The standard IEC 62443 also presents a maturity model. While security levels are a measure of the strength of technical requirements, the maturity levels are a measure of processes (people, policies, and procedures). Parts 2-1, 2-2, 2-4, and 4-1 use maturity levels to measure how thoroughly requirements are met. The levels from 1 to 4 are initial, managed, defined (practiced) and improving. [6]

Defense of depth strategy is considered good, since attacks come from outside, but a perimeter defence is not sufficient. Several barriers must be established to reduce the probability of bad impact caused by attacker. It means provision of multiple security protections, especially in layers with the intent to delay or prevent attacks. System security becomes a set of layers within the overall network security [8]. The standard defines also concept of essential functions that are required to maintain health, safety, environment and availability of the equipment under control. Part 3-3 of the standard IEC 62443 requires that security measures shall not adversely affect essential functions of a high-availability IACS unless it is supported by a Risk Assessment. [6]

IEC 62443 (ANSI/ISA-99) introduces the concepts of "zones" and "conduits" to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. [9]

ISO 27K-series

The ISO/IEC 27000-series is a set of information security standards, providing best practice recommendations on information security at a generic level but also some publications in the series dive deeper in specific domains like energy, health, financial services, etc. Currently there are 60 different standards in the series.

The goal of the 27k series is to provide a reference to support organizations to identify and manage their risks (financial loss, physical harm, loss of reputation) and establish a process for deploying and updating security controls. This should enable stakeholders to achieve and maintain a basic level of security.

The main topics covered by the ISO 27K series are:

– Information security: requirements, management systems, risk management, governance, controls, incident management
– Network security: design, threat scenarios, security techniques
– Application security: management, validation and verification, controls

The key concepts are:

– Self-assessment of security risks is a good starting point.
– Security threats are dynamic and evolving, there needs to be a continuous effort to update the security controls according to the current and foreseeable environment.
– Establishment of a Plan-Do-Check-Act model implement feedback and update mechanisms.
– Security standards need to be used as references/guidance.
– The security controls need to be appropriate/proportional to the security risk.

Of special interest is the ISO/IEC 27019 publication which focuses on the energy utilities and covers production, transmission, storage and distribution. It is based on the ISO/IEC 27002 and covers areas of: Central and distributed programming/automation, Programmable logic controllers, sensors and actuators, Data management, Operational Network communications, Metering infrastructure, smart energy meters and other measurement devices (e.g. for emissions), Digital protection and safety systems, Energy management systems, Energy grids

The ISO/IEC 27019 is not applicable to the security of process control of nuclear facilities, the standards point to IEC 62645 for this purpose.

IEC 62645-series

The IEC 62645 standard was first published in 2014 and then updated in 2019. It focuses on the cybersecurity of nuclear I&C and electrical systems, it is aligned with the ISO/IEC 27001 and it is going to be a "parent" for more standards in the topic, like the IEC 62859 (coordination between cybersecurity and safety in the nuclear domain). The three main sections of the standard cover security at programme level, at system level and then specific topics related to control/requirement.

The IEC 62645 introduces cybersecurity concepts such as the graded approach (controls should be appropriate to the level of the threats) with three security levels – degrees (S1, S2, S3) [10]. The function of systems and the impact to safety/security is considered to decide the security measures needed to protect them. The system lifecycle is considered, security measures are applied during also during development and pre-installation phases. Systems that are assigned the same security degree should have a similar level of security measures regardless of subjective parameters (who designed/developed them). The interfaces between systems assigned to different security degrees are of special interest, restrictions (e.g. hardware-enforced one way

communication) may be applied. Security measures applied on the system to system interfaces should not impact the functionality of the system.

IEC 62859

IEC 62859 standard is dedicated to managing the interactions between safety and cybersecurity, specifically in the nuclear domain, taking into account other current SC 45A (IEC nuclear I&C subcommittee) standards. It is aimed at bridging IEC 62645 and IEC 61513 addressing safety-security issues and the specifics of nuclear I&C programmable digital systems (both important to safety and not important to safety). It is intended to be used in the design of new systems and in modernizing the existing ones when safety and cybersecurity provisions converge on the same I&C systems or architectures. Similarly to IEC 62645, it only concerns cybersecurity challenges caused by malicious acts perpetrated by digital means (cyberattacks).

According to the standard, cybersecurity shall not restrict or interfere with safety objectives or performance. It intends to establish requirements and guidance to:

- Integrating cybersecurity provisions in nuclear overall I&C architectures and systems fundamentally tailored for safety
- Avoiding potential conflicts between safety and cybersecurity in system, organizational and operational level
- Help the identification and taking advantage of the possible synergies between safety and cybersecurity

At the architectural level the standards sets the following fundamental and generic principles:

- Cybersecurity shall not interface with the safety objectives of the plant and shall protect their realization. Effectiveness of the diversity and defence-in-depth features shall not be compromised.
- Cybersecurity requirements impacting the overall I&C architecture shall be addressed after the design and assessment of I&C functions have been made.
- Cybersecurity features shall not negatively impact required performance, effectiveness, reliability or operation of functions important to safety.
- The failure modes and consequences of cybersecurity features on the functions important to safety shall be analysed.
- Between equivalently safe architecture designs, the most secure one should be prioritized. However, still avoiding unnecessary complexity.
- If any architectural property or characteristics designed for safety has value as a potential cybersecurity counter-measure, it should be re-examined to confirm its cybersecurity effectiveness.

IAEA NSS 17

Most prominent international guidance comes for IAEA. Mainly through its Nuclear Security Programme, in which the IAEA supports establishing, maintaining, and sustaining a nuclear security regime. The series comprises of fundamentals, recommendations, implementing guides and technical guidance. IAEA categorises overall security to site, personnel, information, computer, and physical security. These disciplines of security interact and complement each other to establish a plant's security posture. Failure in any of these disciplines of security can affect the other domains and cause extra requirements on the remaining aspects.

The computer security at nuclear facilities reference manual [11] gives guidelines especially to management. Security management lifecycles model describes the security management tasks and it emphasizes continuous improvements. The difference between information technology systems and industrial control systems is pointed out and different cybersecurity requirements are needed for them. Security levels are described in the manual and they define the degrees of security protection required by various computer systems in a facility. The security levels differ from IEC 62443 security levels (SL). Unlike in IEC 62443 series, the security level 1 has the strictest rules and rules become lower up to security level 5. Generic security level is required from all computers. The security levels of the reference manual are associated to required safety of the computer system. For example, security level 1 is required from protective circuits and security level 5 from office automation systems, which have low severity level for various cyber threats. This kind of classification gives an overview of potential combined safety and cybersecurity severity, without going deep in security details.

The reference manual shows list of threats, which are associated to individual attackers or organizations. Also, the list of vulnerabilities is associated to human mistakes.

ISO/IEC 15048 'Common Criteria'

The Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO/IEC 15408) for computer security certification. Its current version is 3.1 revision 5. [12]

The Common Criteria (CC) was developed to facilitate consistent evaluations of security products and systems. The theory behind CC, is that CC will advance the state of security by encouraging various parties to write Protection Profiles (PPs) outlining their needs and desires, and this will push vendors to meet the resulting Protection Profiles and make claims about the security attributes of their products. Independent certified laboratories evaluate the products to determine if they actually meet the claims. [13]

In other words, CC provides assurance that the process of specification, implementation and evaluation of an IT security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. The certification of evaluation results can provide a sound basis for confidences that security measures are appropriate to meet a given threat, and they are correctly implemented. However, it is not an absolute guarantee of security. [13]

CC maintains a list of certified products, including operating systems, access control systems, databases, and key management systems [14].

Key concepts of CC are:

- Target of Evaluation (TOE) is the product or system that is the subject of the evaluation. The evaluation serves to validate claims made about the target's security.
- Protection Profile (PP) is a document, typically created by a user or user community, which identifies security requirements for a class of security devices relevant to that user for a particular purpose.
- Security Target (ST) is the document that identifies the security properties of the target of evaluation. The ST may claim conformance with one or more PPs.
- Security Functional Requirements (SFRs) specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions.
- Security Assurance Requirements (SARs) are descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.
- Evaluation Assurance Level (EAL) is the numerical rating describing the depth and rigor of an evaluation. Common Criteria lists seven levels, with EAL 1 being the most and EAL 7 being the most stringent. Higher EALs do not necessarily imply better security, they only mean that the claimed security assurance of the TOE has been more extensively verified.

The CC documents are [12]:

- Part 1 - Introduction and General Model: This part defines general concepts and principles of IT security evaluation and presents a general model of evaluation.

– Part 2 - Security Functional Requirements: This part establishes a set of security functional components as a standard way of expressing the security requirements for IT products and systems.
– Part 3 - Security Assurance Requirements: This part presents establishes set of assurance components that can be used as a standard way of expressing the assurance requirements for IT products and systems. Part 3 defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs). Part 3 also presents the seven Evaluation Assurance Levels (EALs), which are predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems.

The application of CC in nuclear industry is discussed, for example, in [15] and [16]. The author of [15] lists key advantages of the use of CC in nuclear industry:

– The CC is the only well established and internationally recognized standard for IT product security evaluation and there is tremendous value in the worldwide network of certification schemes and accredited labs that can be used for security evaluations.
– The CC provides a flexible but structured framework that can be customized and adopted for a variety of industry vertical use cases, threat models and assurance levels.
– To get real value from CC, industry participants must collaborate to create tailored requirements to address the specific needs of nuclear industry. For example, nuclear industry can establish relevant technical communities that are focused on sharing threat intelligence and specifying security requirements, both functional and across the product life cycle, for technologies that are critical to your industry via relevant protection profiles and security targets.
– The CC allow for scaling of device testing thanks to use to standardized and automated test, which in turn leads to demonstrable reduction of time, cost and reduction of risk.

Son et al. [16], on the other hand, discusses common points of various cyber security schemes used in nuclear industry. The CC is one of the analysed cyber security schemes. The authors recognize a few additional advantages of CC schemes. Namely, the CC schemes additionally require that devices undergo: 1) Periodic vulnerability analysis 2) Penetrating testing 3) Patch update against recently effective cyber-attacks 4) Cryptographic module validation 5) Secure coding, and 6) Security suitability. The first, second and the third points are elements that should be considered in light of ever-evolving cyber-attacks. Vulnerabilities could always be discovered and exploited. Thus, for example, as the CC receives an assessment, it sets a maximum certification period, and when the term expires, re-certification should be performed for cyber security. The fourth point states that the cryptographic module implemented for the security function should be verified according to the methods of Cryptographic Module Validation Program (In FIPS 140-2, Security Requirements for Cryptographic Modules by NIST). The fifth points is a scheme that analyses whether the developed codes are implemented in compliance with the recommended secure coding guidelines. The sixth point is requirement to analyse the suitability of security functions and products for a given application. Finally, the authors propose a nuclear cyber security evaluation system with reference to a CC assessment system.

A.12 – Information security management of nuclear facility

Relevant YVL guides to cybersecurity are A.12 (Information security management of nuclear facility) and A.11 (Security of nuclear facility), which together with The Nuclear Energy Act (990/1987) and the Government Decrees on Security in the Use of Nuclear Energy (734/2008) form the basis for security arrangements in Finnish nuclear facilities. A.11 focuses more on the physical security of the plant but brings up important concepts such as security zones. Some additional requirements are also given in guides B.1 (Safety design of a nuclear power plant) and E.7 (Electrical and I&C equipment of a nuclear facility). Guides give picture of the overall implementation of nuclear security consisting of several actions and systems.

Guide YVL A.12 is from Finnish perspective the most important cybersecurity guideline. The guide sets out requirements for the management of information security at a nuclear facility in all stages of its lifecycle. The main topics the guide addresses are related to information security management, protecting information, managing resources (sufficiency, competence, training, expertise), protecting system that are important to safety and security (separation, data transfer limitation, however YVL A.12 doesn't directly required information security zones, as NSS-17 does, for example), access control and security testing. In the explanatory memorandum it mentions the most significant references to be the IAEA NSS 17, the ISO/IEC 27000 series, and the IEC 62443 series. Other noteworthy being IEC 62645 and IEC 62859.

III. Discussion and Conclusion

Increased level of automation, gained by more sophisticated algorithms for control and data analysis, brings increasing complexity and introduction of a new cybersecurity risk for the systems and the plant at whole. In general, synthesis for I&C architecture requirements during design stage is still an open issue. This paper surveyed the cybersecurity standards for nuclear I&C from Finnish perspective. However, the list of standards introduced are expected to cover the landscape of nuclear I&C builds quite generally in other countries too. The list is long, as many different organisation progress the cybersecurity domain with their efforts. We considered the most significant standards to be IEC 62443 series, ISO 27K series, IEC 62645, IEC 62859 and IAEA's NSS 17, in addition we reviewed ISO/IEC 15048 and Finnish cybersecurity YVL-guide A.12.

The work also included discussion with Finnish nuclear stakeholders. The main comments from the industry were such that from the designers/licence holders' point-of-view the standards are not detailed enough, or too ambiguous, and it is often unclear how the security requirements are meant to be fulfilled. When the list of current cybersecurity standards were gathered for the paper; it was noticed, that more related standards are being prepared to fulfil gaps and integrate different security design components together to form more overarching approach to security architecture design, similar to quite matured safety standardisation.

Many safety related requirements turn easily into security requirements and vice versa, at least when software is considered. For example, in YVL B.1, there is requirement that states that '*no single common cause failure (CCF) of any individual component type shall prevent the nuclear power plant from being brought to a controlled or safe state*', in a broad sense all software in the plant can be considered as a single component and thus designers need to consider a situation were all software is lost to a CFF, for example because of a cyberattack. As a future research, the next steps will focus on categorisation of the cybersecurity standards and the safety – security interplay [17], which is approached already promisingly in the standard IEC 62859.

Acknowledgement

The Finnish Research Programme on Nuclear Power Plant Safety 2019-2022 (SAFIR2022) funded this research. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

References

[1] Ehrlich, M., Trsek, H., Wisniewski, L., & Jasperneite, J. 2019. "Survey of Security Standards for an Automated Industrie 4.0 Compatible Manufacturing." IECON Proceedings (Industrial Electronics Conference) 2019-

October (October): 2849–54. https://doi.org/10.1109/IECON. 2019.8927559.

[2] Arinze, U. C., Longe, O. B., & Eneh. A. H. 2020. Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues. International Journal of Nuclear Security. Vol. 6. https://doi.org/10.7290/ijns060103.

[3] Sommestad, T., Ericsson, G. N., & Nordlander, J. "SCADA System Cyber Security - A Comparison of Standards", *IEEE PES General Meeting*, 2010.

[4] Shan L., Sangchoolie B., Folkesson P., Vinter J., Schoitsch E., Loiseaux C. (2019) A Survey on the Applicability of Safety, Security and Privacy Standards in Developing Dependable Systems. In Computer Safety, Reliability, and Security. SAFECOMP 2019. Lecture Notes in Computer Science, vol 11699. Springer, Cham. https://doi.org/10.1007/978-3-030-26250-1_6

[5] Amirault, A. & Ferreira dos Santos, I. 2021. Securing industrial networks: What is ISA/IEC 62443?. Cisco IoT Security Research Lab. 13 p.

[6] ISA Global Cybersecurity Alliance. 2020. Quick Start Guide: An Overview of ISA/IEC 62443 Standards - Security of Industrial Automation and Control Systems. 14 p.

[7] Giaconia, M. & Bignalet, X., 2021. Demystifying ISA/IEC 62443 and Secure Elements. AN3983. Microchip. 17 p.

[8] Hauet, J-P. 2012. ISA99/IEC 62443: a solution to cyber-security issues? ISA Automation Conference – Doha (Qatar) - 9 & 10 December 2012. 52 p.

[9] Toffino. 2012. Security White Paper 2012. Using ANSI/ISA-99 Standards to Improve Control System Security. 11 p.

[10] Quinn, E.L., Hardin, L. & Pietre-Cambacedes, L., A New International Standard on Cybersecurity for Nuclear Power Plants: IEC 62645 - Requirements for Security Programmes for Computer-Based Systems. http://www.technology-resources.com/docs/IEC_Cyber_Standard_FINAL_12192014.pdf

[11] IAEA. 2011. Nuclear security series no. 17 - Computer security at nuclear facilities - Reference manual. International Atomic Energy Agency. Vienna

[12] Common Criteria webpage. 2021a. Publications: CC Portal. Available at: https://www.commoncriteriaportal.org/cc/ (Accessed: 23 August 2021)

[13] Aizuddin, A. 2021. The Common Criteria ISO/IEC 15408 – The Insight, Some Thoughts, Questions and Issues. SANS Institute white paper. https://www.sans.org/white-papers/545/

[14] Common Criteria webpage. 2021b. Certified Products: CC Portal. Available at: https://www.commoncriteriaportal.org/products/ (Accessed: 23 August 2021)

[15] Turner, L. 2020. Common Criteria for nuclear cyber security. In Report of Contributions of International Conference on Nuclear Safety, IAEA, p. 182

[16] Son, J. Choi, J. & Yoon, H. 2019. New complementary points of cyber security schemes for critical digital assets at nuclear power plants. In IEEE Access, vol. 7, pp. 78379-78390, 2019, doi: 10.1109/ACCESS.2019.2922335

[17] Papakonstantinou, N., Linnosmaa, J., Bashir, A. Z., Malm, T., Van Bossuyt, D. 2020. Early combined safety – security defence in depth assessment of complex systems. In Reliability and Maintainability Symbosium IEEE RAMS 2020. USA. California. 7 p.