IEC STANDARD-FAMILY ON CYBERSECURITY FOR NUCLEAR POWER PLANTS

T. WALTER
PreussenElektra GmbH
Hannover, Germany
Email: Thomas.walter1@preussenelektra.de

E. L. QUINN
Technology Resource Inc.
Dana Point, USA

L. PIETRE-CAMBACEDES
EdF
Lyon, France

J. E. BOCHTLER
Siemens AG
Erlangen, Germany

Abstract

Cybersecurity has become a cornerstone of nuclear security in modern NPPs, considering the place of digital equipment (including reactor control systems and reactor safety systems) in their design and operations. IEC SC45A decided in 2008 to develop an IEC standard on cybersecurity requirements (IEC 62645). The first edition was published 2014. As the development of digital I&C raises, a new edition of this standard was directly started after publishing in 2015. The edition 2 was issued in November 2019, and additional standards, on coordination of safety and security (IEC 62859 started in 2012, published in 2016) and on security controls (IEC 63096 started in 2016), were set on track.

The paper presents in its first part the IEC and its Subcommittee 45A (Instrumentation, control and electrical power systems of nuclear facilities). It explains how the IEC cybersecurity standards fit to the IEC SC45A framework and to other cybersecurity work like ISO/IEC 270xx series and IAEA work (NST045 and NST047).

In the second part, the three IEC SC45A standards focused on cybersecurity are presented in detail.

The standard IEC 62645 gives the high-level requirements and guidance, in particular for development and management of a cybersecurity program, for programmable digital I&C systems. It uses a graded approach and covers the entire security lifecycle on program level and system level, as well as generic aspects of security controls. The revision principles for the second edition (started in 2016) are:

(i) to adapt the structure and high-level principle with ISO/IEC 27001:2013 and ISO/IEC 27002:2013,
(ii) to target a better consistency with IEC 62443 when relevant
(iii) to rearrange the structure to consider the future second level documents on cybersecurity.

The standard IEC 62859 is intended to help coordinating safety and cybersecurity issues. This standard is needed because safety requirements can have impact on cybersecurity measures and vice versa. The safety-oriented provisions are often well established, and the cybersecurity requirements and controls are often added. This can result in interaction and possible side-effects which must be considered on two levels: the architectural level and the individual system level. Additional organizational issues are shown. This standard is, like IEC 62645, also on track to become eu European standard.

The standard IEC 63096 focuses on the process of applying security controls in line with the IEC 62645 requirements and provides a comprehensive security catalogue that is tailored for the nuclear I&C domain. The standard is currently under development and will be published in 2020. The chapters 5 through 18 exactly follow the structure of ISO/IEC 27002 clauses 5 through 18. IEC/ISO 27002 controls have been reconciled with the requirements of the nuclear I&C domain and, if deemed necessary, modified or extended. Additional information on the preservation (confidentiality, integrity and availability) and the control focus (prevention, detection) are given for each control. Their relevance for the security degrees from IEC 62645 and a baseline, and with respect to the different phases (development, engineering, operation), is considered.

As conclusion the IEC SC45A standards for cybersecurity brings a new and regularly updated set of guidance from IEC, in conjunction with IAEA and country specific standards, to the international community with regards to cybersecurity for nuclear facilities.

1. INTRODUCTION

The purpose of this paper is to provide an overview of the International Electrotechnical Commission (IEC) standard framework for cybersecurity. IEC is built by several Technical Committees (TC) with Sub Committees (SC). The cybersecurity framework is handled within the working group WGA09 of SC45A.

It is recognized that cybersecurity is an evolving area of regulatory requirements due to the continuously changing and emerging computer security threats. Therefore, the objective of SC45A cybersecurity standards is to have a framework of standards with IEC 62645 [1] as its top-level document, by focused on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of cyberattacks against digital instrumentation and control (I&C) systems. The nuclear specific safety classification of nuclear I&C systems and associated safety requirements are among the biggest differences compared to typical IT systems and standard industrial automation systems. A new edition is currently being finalized [2]. IEC 62859 [3] deals as one of the first international standards on the coordination of safety and security aspects. An amendment [4] was created to solve some issues by the FDIS vote. The set will be expanded by IEC 63096 [5] with focus on the development of a catalogue of cybersecurity controls that may be applied to prevent and/or minimize the impact of cyberattacks against computer-based I&C systems in NPPs.

In Fig. 1 the nuclear specific IEC standards for safety and security are shown and how they are categorized and linked together. The Fig. 1 shows also the links of the security standards to the ISO/IEC standards 27001 [6] and 27002 [7].

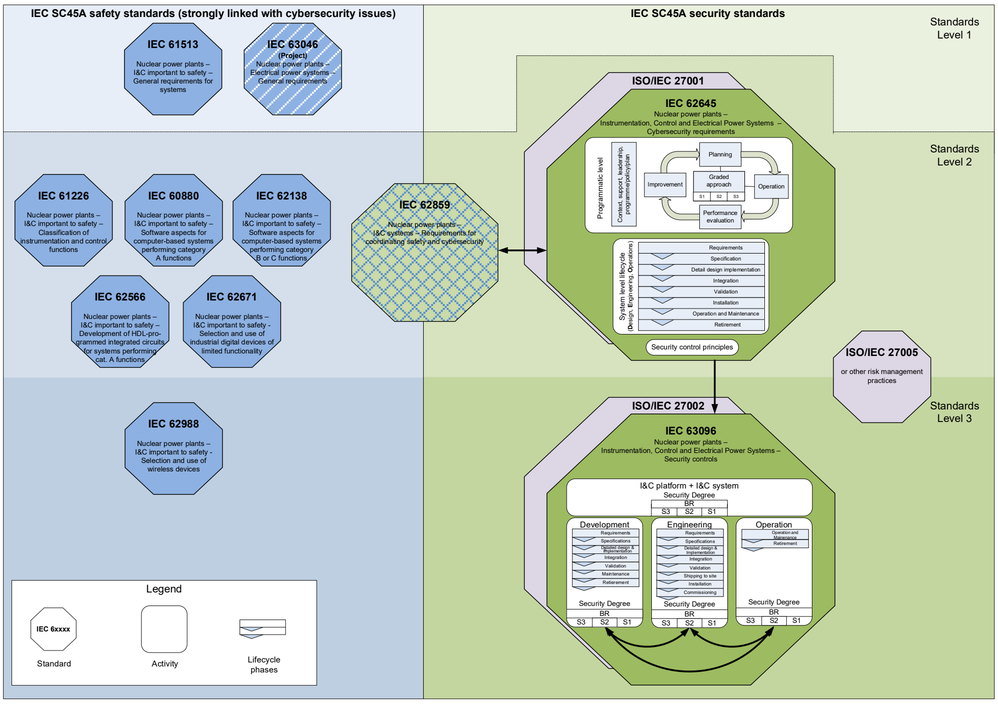

IEC SC45A safety standards (strongly linked with cybersecurity issues)
IEC SC45A security standards
Standards Level 1
Standards Level 2
Standards Level 3
IEC 61513
Nuclear power plants – I&C important to safety – General requirements for systems
IEC 63046
(Project)
Nuclear power plants – Electrical power systems – General requirements
IEC 61226
Nuclear power plants – I&C important to safety – Classification of instrumentation and control functions
IEC 60880
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category A functions
IEC 62138
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category B or C functions
IEC 62566
Nuclear power plants – I&C important to safety – Development of HDL-programmed integrated circuits for systems performing cat. A functions
IEC 62671
Nuclear power plants – I&C important to safety - Selection and use of industrial digital devices of limited functionality
IEC 62988
Nuclear power plants – I&C important to safety - Selection and use of wireless devices
IEC 62859
Nuclear power plants – I&C systems – Requirements for coordinating safety and cybersecurity
ISO/IEC 27001
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Programmatic level
Context, support, leadership, programme/policy/plan
Planning
Improvement
Graded approach
S1
S2
S3
Operation
Performance evaluation
System level lifecycle (Design, Engineering, Operations)
Requirements
Specification
Detail design implementation
Integration
Validation
Installation
Operation and Maintenance
Retirement
Security control principles
ISO/IEC 27005
or other risk management practices
ISO/IEC 27002
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
I&C platform + I&C system
Security Degree
BR
S3
S2
S1
Development
Requirements
Specifications
Detailed design & Implementation
Integration
Validation
Maintenance
Retierement
Security Degree
BR
S3
S2
S1
Engineering
Requirements
Specifications
Detailed design & Implementation
Integration
Validation
Shipping to site
Installation
Commissioning
Security Degree
BR
S3
S2
S1
Operation
Operation and Mainenance
Retirement
Security Degree
BR
S3
S2
S1
Legend
IEC 6xxxx
Standard
Activity
Lifecycle phases

FIG. 1. IEC TC45A safety and security standards.

2. IEC 62645 ED2: NUCLEAR POWER PLANTS - INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS - CYBERSECURITY REQUIREMENTS

2.1 Edition 1

Developed since 2009 and published end of 2014, the standard is intended to be used for changing or establishing new security programmes for I&C systems of operating and new Nuclear Power Plants (NPP). This International Standard establishes requirements and provides guidance for the development and management of effective computer security programmes at nuclear power plants. Inherent to the design requirements shall be the criterion that the design of the power plant shall comply with the applicable country's computer security requirements.

This standard is limited to I&C computer-based systems, possibly integrating HPD (HDL – Hardware Description Language - Programmed Devices). It includes those which are used to operate a plant, from the safety and availability points of view, and those which do not run online, in particular configuration management systems as an example. Excluded are all systems which are not important to technical control or operational purposes (e.g. office computers, business IT for procurement, controlling) due to the scope of SC45A.

Also excluded from the scope of this standard are considerations related to:

- human errors;
- site computerized access control and monitoring systems (dedicated studies are made);
- good practices for managing applications and data software, including back-up and restoration related to accidental failure, which should be implemented even if computer security was not studied;
- natural events.

This is situated to the defined scope of TC45A.

During the discussions at the last stage of development of IEC 62645 Ed. 1, it was agreed to publish the results of five years of discussions and state in its introduction its revision would be launched quickly. The stability date for IEC 62645 was set up to 2015, so the responsible working group WG A09 recommended IEC 62645 to be revised as soon as it was published.

2.2 Edition 2

After publishing edition 1 of IEC 62645 the principles of revision were fixed, and they include the following major focus areas:

1. IEC 62645 ed. 1 structure and high-level principles have been built on the IAEA NSS17 [8], and on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 international standards. The revision shall now consider the 2013 editions structure and high-level principles of the ISO/IEC 27001 and ISO/IEC 27002.
2. Although ISO/IEC 27000 series and IAEA NSS 17 remain the main structuring references, a better consistency with the IEC 62443 series (on industrial control systems) should also be sought when relevant.
3. A better consistency and articulation with IEC 61513 [9] shall be reached: this may involve coordination with a future revision of IEC 61513 to modify its clauses presently dealing with computer security (e.g. by pointing towards IEC 62645, providing IEC 62645 Ed. 2 covers correctly these requirements).
4. A similar coordination work as the one mentioned in 3.) with IEC 61513 should be done with IEC 60880 [10] and 62138 [11].
5. The content and structure of IEC 62645 Ed. 2 could be rearranged to better consider the future second level documents with respect to IEC 62645 (IEC 62859 and IEC 63096).

After accepting these revision principles, the work on the new edition started in 2015. A first working draft was issued one year later. The comments were addressed in a full committee meeting (SC45A) 2017 in Shanghai and this results in a committee draft for voting (CDV) by end of 2018. The CDV comments were addressed in a full committee meeting in Paris 2019 and the final draft for international standard (FDIS) was published soon after. This FDIS was accepted with no votes against and IEC 62645 Ed. 2 was published in November 2019. Fundamental concepts of Ed. 1 have been kept (e.g. graded approach and security degrees) but a tighter complementarity with ISO/IEC 27001, and more largely with other relevant standards, has been reached. Wherever it was possible a direct link to ISO/IEC 27001 is stated in the first sub chapter link:

The content of ISO/IEC 27001:2013, *chapter number* applies

In Fig. 2 the important topics to deal with are visualized:

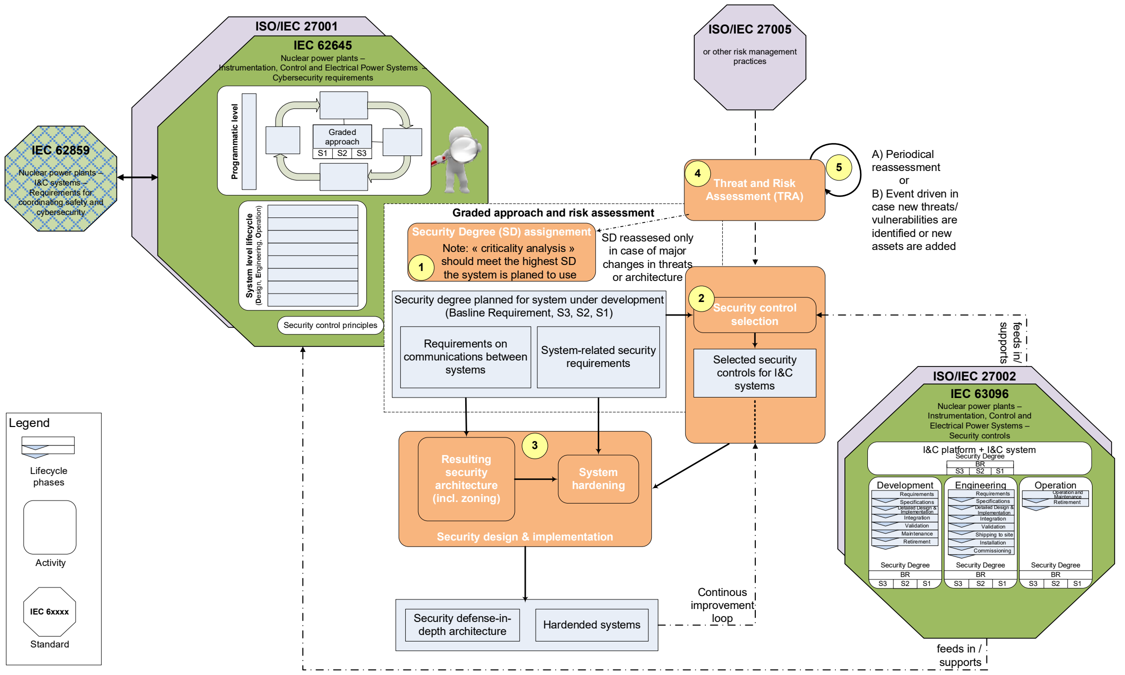

ISO/IEC 27001
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Programmatic level
Graded approach
S1 S2 S3
System level lifecycle (Design, Engineering, Operation)
Security control principles
IEC 62859
Nuclear power plants – I&C systems – Requirements for coordinating safety and cybersecurity
ISO/IEC 27005
or other risk management practices
4
Threat and Risk Assessment (TRA)
5
A) Periodical reassessment
or
B) Event driven in case new threats/ vulnerabilities are identified or new assets are added
Graded approach and risk assessment
Security Degree (SD) assignement
1
Note: « criticality analysis » should meet the highest SD the system is planed to use
SD reassesed only in case of major changes in threats or architecture
Security degree planned for system under development (Basline Requirement, S3, S2, S1)
Requirements on communications between systems
System-related security requirements
2
Security control selection
Selected security controls for I&C systems
feeds in/ supports
3
Resulting security architecture (incl. zoning)
System hardening
Security design & implementation
Security defense-in-depth architecture
Hardended systems
Continous improvement loop
ISO/IEC 27002
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
I&C platform + I&C system
Security Degree
BR
S3 S2 S1
Development
Requirements
Specifications
Detailed Design & Implementation
Integration
Validation
Maintenance
Retirement
Engineering
Requirements
Specifications
Detailed Design & Implementation
Integration
Validation
Shipping to site
Installation
Commissioning
Operation
Operation and Maintenance
Retirement
Security Degree
BR
S3 S2 S1
feeds in / supports
Legend
Lifecycle phases
Activity
IEC 6xxxx
Standard

FIG. 2. IEC 62645 ED2 Work Flow.

3. IEC 62859 ED1: NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – REQUIREMENTS FOR COORDINATING SAFETY AND CYBERSECURITY

3.1 Edition 1

Cybersecurity requirements and controls applicable to digital I&C systems are often added to well-established safety-oriented provisions. Interactions and potential side-effects are possible and must be mastered, taking into account the nuclear I&C system specificities as well as their normative and regulatory contexts. IEC 62859 aims to provide a rigorous and actionable framework by establishing requirements to:

– integrate cybersecurity provisions in nuclear I&C architecture and systems, which are fundamentally tailored for safety;
– avoid potential conflicts between safety and cybersecurity provisions;
– aid the identification and the leveraging of the potential synergies between safety and cybersecurity.

The standard is based on three main sections: one dealing with the overall I&C architecture, a second one focusing on the system level, a third one dealing with organizational and procedural issues.

For the overall architectural level, a set of concise, fundamental and high-level principles when treating cyber security features of digital I&C is given. Among them, one can mention:

– Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realization. It shall not compromise the effectiveness of the diversity and defence-in-depth features implemented by the I&C architecture.
– Cybersecurity requirements impacting the overall I&C architecture shall be addressed after the overall I&C architecture design and assignment of the I&C functions have been first made as per Subclause 5.4 of IEC 61513:2011. The integration of architectural cybersecurity requirements may lead to an iterative design process.
– Cybersecurity features shall not adversely impact the required performance (including response time), 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 and taken into account.

Then, it provides more detailed requirements and guidance focused on design aspects regarding the delineation of security zones (completing IEC 62645), provisions for coping with common cause failures, separation provisions, diversity, data communications.

The second major section is dedicated to the individual system level. It also starts by providing fundamental principles, tailored to this level and completing the architectural ones. Then, requirements, recommendations and considerations are given based on an I&C system lifecycle approach. For consistency reasons, the phases considered are those used in IEC 62645. Finally, a set of sub-clauses provides guidance on more concrete aspects, in order to deal with common situations where safety and cyber security technical measures may conflict, depend on or reinforce each other.

The third and last section is dedicated to organizational issues, including governance and responsibilities, coordination between safety and cyber security staff during operations, safety and cybersecurity culture, emergency response and crisis management.

3.2 Amendment

Edition 1 of IEC 62859 was chosen by CEN-CENELEC CLC/TC 45AX as a candidate for an European standard in December 2018. As two major countries voted against edition 1 on the same topic, a simple process was not possible according to the IEC rules. To address the concern of these two countries an amendment was created by TC45A WG09 to solve the issues (possibilities of misunderstanding of two bullets in one chapter). This amendment went fast through the IEC procedures with CD, CDV and FDIS in 2019. There were no votes against, so CEN-CENELEC can go on for establishing IEC 62859 as European standard in 2020.

4. IEC 63096: NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – SECURITY CONTROLS

4.1 Structure of the standard

The chapters 1 to 3, scope, references and terms and definitions follow the IEC standard structure.

Chapter 4 defines the audience, describes the source and structure of security controls and details the process on how to apply security controls in line with the IEC 62645 requirements.

The chapters 5 to 18 cover the chapters of ISO/IEC 27002 [7] on a one to one basis. Some sub chapters with nuclear specific topics were added. In this case NUC is written after the chapter numbering to indicate nuclear specific additions.

The chapters 19 and 20 are nuclear specific additions and marked with NUC after the numbering.

4.2 Structure of each control

Control

This subclause contains a short description of the specific security control. If there is no modification the original ISO/ IEC 27002 text has been taken over.

Preservation of

Description of the objective of the security control in terms of Confidentiality, Integrity and Availability (CIA)

- C = Confidentiality
- I = Integrity
- A = Availability

Control focus

This subclause contains the description of the focus of the security control in terms of prevention, detection and correction

- p = Prevention
- d = Detection
- c = Correction

Implementation guidance

The implementation guidance is described in a standardized table format and depends on the security degree (as defined in IEC 62645) that is assigned to the individual I&C system.

For the security baseline and the security degrees following column headings are defined:

- BR = Baseline Requirement
- S 3 = Security degree 3
- S 2 = Security degree 2
- S 1 = Security degree 1

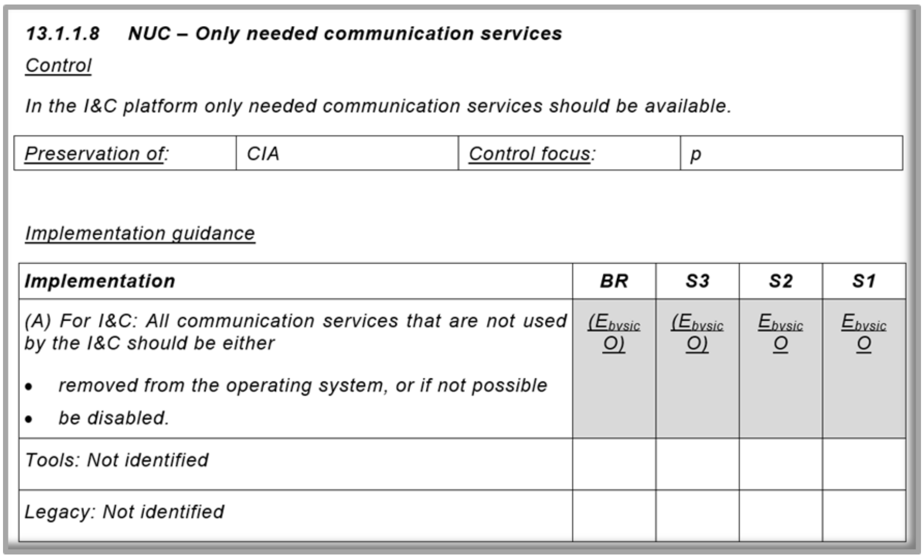
The applicability of the implementation guidance also depends on one or several of the following activities, shown by the following activity letters (See table 1) in columns BR, S 3, S 2, S 1.

TABLE 1. Activity letters of the live cycle phases for the applicability of controls

Phase	I&C Platform Development	Project Engineering for plant specific I&C system	Operation & Maintenance of I&C system
Main activity	**D** → I&C Platform Development	**E** → Project Engineering for plant specific I&C system	**O** → Operation and Maintenance of I&C system
Sub activities		**E_b** → Project Engineering before "Installation" and "Commissioning" **E_d** → "Requirements", Specifications" and Detailed design and implementation **E_g** → Integration (offsite integration) **E_v** → Validation (factory acceptance testing) **E_s** → Shipping to site **E_i** → Installation (onsite Integration and Acceptance Testing) **E_c** → Commissioning (Commissioning and Acceptance Testing)	**O_o** → Operation **O_m** → Maintenance **O_r** → Retirement

If an activity letter is shown without parenthesis, this security control is highly recommended for the stated security level.

Figure 3 shows an example of a complete control chapter including all the information described above.



13.1.1.8 NUC – Only needed communication services

Control

In the I&C platform only needed communication services should be available.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For I&C: All communication services that are not used by the I&C should be either • *removed from the operating system, or if not possible* • *be disabled.*	(E_{bvsic} O)	(E_{bvsic} O)	E_{bvsic} O	E_{bvsic} O
Tools: Not identified				
Legacy: Not identified				

FIG. 3. IEC 63096 example of a cybersecurity control.

4.3 Overview list of all controls

The annex A of IEC 63096 contains an overview list of all controls with the following fields:

- Clause
- Security Control Name
- Security control by security degree (with the associated activity letters)
- I&C (if the control is to be implemented in the I&C platform or I&C system)
- Preservation of
- Control focus
- ISO/IEC 27002 reference (n = not modified, m = modified, a = added, u = unconsidered)

This annex A will be distributed as attachment to the IEC 63096 PDF-file in two different machine-readable formats (XLXS and CSV).

5. CONCLUSIONS AND FUTURE CHALLENGES

Cybersecurity is now a well-identified challenge and issue for all industries; nuclear I&C have both commonalities, and specificities. Nuclear safety and security are essential aspects of these specificities, in terms of stakes, design and operational approaches, but also in terms of existing IAEA and normative documents and principles, and national practices. The IEC set of standards presented in this paper have been developed to take these very aspects in account, in consistence with IAEA principles, in an industrial normative approach, leaving room for national and particular implementations. Also IEC maintain the standards to be up to date as seen with the Edition 2 of IEC 62645.

IEC work on cybersecurity will be going on with two technical reports. One on “Using Formal Security Models for Design and Assessment I&C Security Architecture” and another on “Cybersecurity – Risk Management”. Both titles are not fixed at the moment and a publication is scheduled within the next two years.

REFERENCES

[1] IEC 62645:2014 “Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems" (2014)

[2] IEC 45A/1289/FDIS IEC 62645 ED2 “Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements” (2019).

[3] IEC 62859:2016, “Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity” (2016).

[4] IEC 45A/1279/FDIS IEC 62859/AMD1 ED1 “Amendment 1 – Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity” (2019).

[5] IEC 45A/1291/CDV IEC 63096 ED1 2 “Nuclear power plants – Instrumentation, control and electrical power systems – Security controls” (2019).

[6] ISO/IEC 27001:2013, “Information Technology – Information technology — Security techniques — Information security management systems — Requirements” (2013)

[7] ISO/IEC 27002:2013, “Information technology — Security techniques — Code of practice for information security controls” (2013)

[8] IAEA Nuclear Security Series No. 17, Reference Manual, Computer Security at Nuclear Facilities, (2011)

[9] IEC 61513:2011, “Nuclear power plants – Instrumentation and control for systems important to Safety – General Requirements for Systems.” (2011).

[10] IEC 60880:2006, “Nuclear Power Plants – Instrumentation Systems Important to Safety – Software Aspects of Computer Based Systems Performing Category A Functions, (2006).

[11] IEC 62138:2004, “Nuclear power plants - Instrumentation and control important for safety Software aspects for computer-based systems performing category B or C functions,” (2004).