IEC 62859: TOWARDS AN INTERNATIONAL STANDARD ON THE COORDINATION BETWEEN SAFETY AND CYBERSECURITY FOR NUCLEAR I&C SYSTEMS

Ludovic Pietre-Cambacedes
Senior Engineer
EDF Nuclear Engineering Division
Basic Design (SEPTEN)
12-14 avenue Dutriévoz
69628 Villeurbanne, France
ludovic.pietre-cambacedes@edf.fr
+33 4 72 82 74 10

Edward L. Quinn
ANS Past President
IEC SC45A WGA9 Convenor
Technology Resources
23292 Pompeii Drive Dana Point,
CA 92629, USA
tedquinn@cox.net
(949) 632-1369

ABSTRACT

Cybersecurity requirements and controls for digital I&C systems are increasingly 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. The future international standard IEC 62859 "Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cyber security" aims to optimize the integration of cybersecurity provisions in nuclear I&C architecture and systems, to prevent conflicts between safety and cybersecurity provisions, and to aid the identification and the leveraging of the potential synergies between safety and cybersecurity. The paper presents the state of development of this standard and the main content of the current draft. Presently, the draft 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. The paper also discusses related work in the nuclear industry, and in other sectors.

Key Words: digital I&C, cybersecurity, safety, standard

1 INTRODUCTION

Nuclear I&C systems have evolved from non-digital and close systems to digital technologies and networked environments. This exposes them to cybersecurity risks. Consequently, new cybersecurity requirements and controls now apply to systems already subject 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. The development of a new international standard has been undertaken by the International Electrotechnical Commission (IEC) to tackle this challenge.

The IEC is a worldwide organization for standardization of the electrotechnical and electronic fields. Its subcommittee 45A (SC45A) focuses on I&C systems of nuclear facilities. It has issued several standards used worldwide, in particular on safety-related I&C systems (e.g., IEC 61513 [1], IEC 61226 [2], IEC 60880 [3] or IEC 62138 [4]). In 2008, the SC45A decided to address cybersecurity in dedicated documents. The first and top-level document developed on this issue has been the IEC 62645 "Nuclear power plants – Instrumentation and control systems – Requirements for security programs for computer-based systems" [5]. After six years of development, it has been published in August 2014. An overview of its content is provided in [6]. The second document, directly affiliated to IEC 62645, was initiated in 2010 and is the subject of this paper. Currently under development, it is referenced as IEC 62859 and deals with the coordination between safety and cybersecurity.

This paper presents the state of development of IEC 62859 and its main content. Section 2 deals with the scope and applicability of the document. Section 3 presents its status, from a standardization process perspective. Section 4 describes the structure and main content of the current draft. Section 5 mentions related work in the nuclear industry, and in other sectors. Section 6 concludes the paper.

2 SCOPE AND APPLICABILTY OF IEC 62859

The future international standard IEC 62859 "Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cyber security" aims to provide a rigorous and actionable framework by establishing requirements to:

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

It should be noted that cybersecurity in the context of SC45A is to be understood as prevention of, detection of, and reaction to malicious acts by digital means. It is recognized that the term "cybersecurity" has a broader meaning in other standards and guidance, which often includes non-malevolent threats, human errors, site computerized access control and monitoring systems, good practices for managing applications and data software (including back-up and restoration related to accidental failure); and natural events. Most of those issues are addressed by other standards of SC45A; they should all of course be addressed by plant operating procedures and programmes.

The applicability of the standard is inherited from its parent standard, i.e. IEC 62645: it is limited to I&C computer-based systems[1], possibly integrating HPD (HDL 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. Excluded are all systems which are not important to technical control or operational purposes.

[1] The standard actually refers to I&C CB&HPD systems, CB standing for Computer-Based and HPD standing for HDL-Programmed Device, i.e. integrated circuit configured with Hardware Description Language and related software tools. Such naming aims to cover microprocessor based I&C digital systems, but also FPGAs, PLDs or similar micro-electronic technologies. For convenience, the term "digital systems" is also used in the rest of the paper.

3 STATUS

The initial New work item Proposal (NP) was proposed to the IEC in October 2012. This proposal was previously discussed during an IEC/SC45A meeting held in February 2012 in Garching, Germany, where it received full support of the participating experts. As mentioned in Section 2, its application scope is aligned with IEC 62645, as it aims at becoming a second-level document with respect to IEC 62645. The NP was circulated for voting at the end of 2012 and was approved by 16 out of 18 voting member countries. Seven committees designated subject matter experts to work on this new standard: France, Germany, Japan, Republic of Korea, Russia, Ukraine and United States. The first meeting concerning this document was held in Moscow in June 2013. In its aftermaths, a complete Committee Draft (CD) was written and circulated to the national committees in June 2014. The comments were discussed and solved during the SC45A meeting held in Las Vegas in October 2014. A second Committee Draft (CD2) is currently (2015 Q1) being written to take into account these debates. Once the CD2 circulated and commented, several steps will still need to be fulfilled before issuance (in particular, the CDV stage and the FDIS stage): the publication is foreseen at the earliest for the end of 2016.

It can be noted that the IAEA has also been working on a closely related guidance document since June 2012 [7]. Both documents are developed in coordination, with the IAEA's document focused on guiding principles rather than on requirements.

4 CURRENT DRAFT STRUCTURE AND KEY ASPECTS

4.1 General

In addition to the usual clauses found in IEC standards (scope, references, terms, abbreviations), the CD has three main sections grouping requirements. They are quickly presented in the following subsections. It should be stressed that this document organization and content are still subject to potential important changes, as the drafting process is still on-going.

4.2 Coordinating cybersecurity and safety at the I&C overall architectural level

This first main section treats the issue of the coordination between safety and cybersecurity at the overall architectural level. It starts by providing a set of five concise, fundamental and high-level principles when treating cyber security features of digital I&C systems (for instance "*Implementation of cybersecurity features shall not adversely impact the required performance (including response time), effectiveness, reliability or operation of functions important to safety*"). Then, it provides more detailed requirements and guidance focused on design aspects regarding the delineation of security zones (completing what is already indicated in IEC 62645 [5]), provisions for coping with common cause failures, separation provisions, diversity, data communications.

4.3 Coordinating safety and cybersecurity at the individual system level

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 others. For the time being, these clauses cover the following themes: logical access control for HMIs of I&C CB&HPD systems in control rooms; software modifications (this includes patches and updates); logging and audit capability; use of cryptography by I&C systems; system availability and function continuity; emergency response

and crisis management communication systems. Particular attention is also paid to the idiosyncrasies of safety and cyber security. As an illustration, one can cite the following requirement: "*When claimed in cybersecurity-oriented analyses, the cybersecurity benefit of communication or data integrity controls initially implemented for safety or reliability purposes shall be assessed and validated by cybersecurity experts with respect to the relevant malevolent threats*". The driver for such a requirement is that the efficiency of integrity mechanisms differs largely depending on the nature of the threats: for instance, a CRC (Cyclic Redundancy Check) code may be efficient against random failures whereas it would be useless against an attacker, who can change the data and change the CRC. Integrity control or assurance mechanisms specifically tailored for security need to be considered in this case. Several other requirements aim to treat safety and cyber security in close coordination, and to prevent confusion between these two issues, in respect to their specificities. The interested reader might refer to [8] for a general discussion about differences and commonalities between safety and security. As requested by several national committees, an informative annex will be added to the IEC 62859 to recall these differences and commonalities.

4.4 Organizational and procedural issues

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.

5 RELATED WORK

The coordination between safety and cyber security is a subject that has been identified by the academic community for a long time (e.g, see [9] as an early work). A high-level discussion of the state of the art is provided in [8] along with more research-oriented modeling considerations. The convergence of safety and cyber security issues on the same digital systems has now become a reality and a concrete industrial concern. This situation justifies the elaboration of standards applicable to industrial actors, in addition to research efforts. The nuclear industry has already issued several guidance documents about the interface between nuclear safety and nuclear security, but without focusing on the cyber dimension of the subject (see for instance the IAEA INSAG-24 report [10] or the NRC Regulatory Guide 5.74 [11]). This future IEC standard integrates these references as inputs, but will provide a more targeted set of requirements and recommendations for the specific area of digital I&C systems. It should be noted that the topic is not only of interest to the nuclear domain. Other industrial sectors have launched different initiatives aiming at a better coordination between safety and cyber security. In particular, this is the case within the IEC, by the TC65, in charge of the industrial-process measurement, control and automation area [12]. The on-going SC45A work will also consider such initiatives and analyze their work as potential inputs to the standard development process.

6 CONCLUSION

Coordinating cybersecurity and safety is an important issue, as both aspects have long been considered separately, by different people and for different systems, whereas they now have to be considered together. The existing safety culture and provisions in the nuclear industry are a chance to build an efficient cybersecurity posture, however, safety and cybersecurity needs proper coordination to ensure mutual reinforcements and synergies, while limiting interferences and optimizing costs and operations. The future IEC 62859 intends to provide an appropriate framework to tackle this challenge.

7 REFERENCES

[1] IEC 61513 (2011) Ed. 2.0, “Nuclear power plants – Instrumentation and control for systems important to Safety – General Requirements for Systems”

[2] IEC 61226 (2009) Ed. 3.0. “Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions”

[3] IEC 60880 (2006) Ed. 2.0, “Nuclear Power Plants – Instrumentation Systems Important to Safety – Software Aspects of Computer Based Systems Performing Category A Functions,

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

[5] IEC 62645 Ed. 1.0 (2014) “Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems”

[6] Ted Quinn, Leroy Hardin, Ludovic Pietre-Cambacedes, "A new international standard on cybersecurity for nuclear power plants: IEC 62645 - Requirements for Security Programmes for Computer-Based Systems", *9th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC-HMIT 2015)*, Charlotte, USA, Feb 2015

[7] International Atomic Energy Agency (IAEA), NST036 “Computer Security of I&C Systems at Nuclear Facilities”, Draft

[8] L. Pietre-Cambacedes and M. Bouissou, “Cross-fertilizations between safety and security engineering,” *Reliability Engineering & System Safety*, vol. 110, pp. 110-126, 2012. Elsevier.

[9] D. P. Eames, and , J. Moffett “The integration of safety and security requirements,” *Proc. 18th International Conference on Computer Safety, Reliability and Security (SAFECOMP'99), LNCS vol. 1698*, pp. 468-480, 1999, Springer, Berlin.

[10] International Atomic Energy Agency (IAEA), International Nuclear Safety Group (INSAG), “The interface between safety and security at nuclear power plants”, INSAG-24, 2010.

[11] U.S. Nuclear Regulatory Commission (NRC), RG 5.74 “Managing the safety/security interface”, 2009

[12] IEC TC65, Draft For Comment and Call For Experts Ad-hoc group: framework toward coordinating safety, security, Document 65/569/DC, 2014.