A NEW INTERNATIONAL STANDARD ON CYBERSECURITY FOR NUCLEAR POWER PLANTS: IEC 62645 – CYBERSECURITY REQUIREMENTS

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

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

Thomas Walter
Process IT Security Manager
PreussenElektra GmbH,
Elektro- und Leittechik (TTE),
Tresckowstr. 5
D-30457 Hannover, Germany
thomas.walter1@preussenelektra.de
+49 511 439-2403

ABSTRACT

This paper provides an overview of the IEC 62645, an actual standard by the International Electrotechnical Commission (IEC) focused on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of cyber attacks against computer-based I&C systems.

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 paper also presents the key issues being considered in the new revision to IEC 62645, currently in process.

1. INTRODUCTION

The purpose of this paper is to provide an overview of the development and content of an actual standard by the International Electrotechnical Commission (IEC), focused on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of cyber attacks against computer-based I&C systems.

It is recognized that this is an evolving area of regulatory requirements, due to the changing and evolving nature of the computer security threats. Therefore, the goal of this standard is to define a common international framework within which the evolving country specific requirements may be developed and applied.

It is also recognized that this subject matter requires protection and limited release of the products derived from application of this standard to country specific requirements to minimize the extent to which malevolent individuals or organizations, intending to access without authorization, a nuclear plant system or systems may benefit from this information.

The increasing use of computers for various functions at nuclear facilities brings forth new vulnerabilities that must be addressed in a rigorous and balanced manner. Nuclear power plant computers are used in non-safety and systems important to safety, where non-availability or malfunction could affect nuclear safety and/or continuity of power. Computers are also used to store important and sensitive data. The complexity of these computer systems makes it difficult to identify comprehensively the potential threats to the nuclear facilities. In particular, industrial control systems, are recognized as attractive targets and vulnerable to cyber attacks (the contrary statements are long lasting myths [8] that Stuxnet or more recently, the Dragonfly operation [9] have proved completely wrong): experience shows that computer systems without proper protection from attack can become unavailable or deviate from their intended function, and must be protected throughout the whole life cycle.

The proposed revision to IEC 62645 is intended to be used for I&C systems of operating and new Nuclear Power Plants (NPP). A revision to IEC 62645 is currently in process. This paper provides and overview of IEC 62645 the key points being addressed in it's ongoing revision process.

2. DESCRIPTION OF THE IEC STANDARD

2.1 Standardization context

As explained on its website, "the International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National

Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations".

The IEC 62645 standard has been developed by the Subcommittee 45A (SC45A) of the IEC, addressing Instrumentation and control (I&C) of nuclear facilities. SC45A has issued many worldwide respected standards on different areas of I&C systems, and more particularly for safety related I&C (e.g, [4-6]). It works in close coordination with the IAEA (International Atomic Energy Agency) on safety-related issues for decades, and more recently on cybersecurity issues.

IEC 62645 is the first document of SC45A targeting mainly cybersecurity, and is the first of a future series dealing with this major issue for NPP I&C (a second document has been recently issued, dealing with the coordination between safety and cybersecurity and referenced IEC 62859 – see [7] for more information.).

2.2 Scope of the standard

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[1], 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. Excluded are all systems which are not important to technical control or operational purposes (e.g. office computers, business IT for procurement, controlling.).

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

[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.

related to accidental failure, which should be implemented even if computer security was not studied;
- natural events.

(Note: the issues related above are addressed by other standards and should of course be addressed by plant operating procedures and programmes.)

2.3 Organization and main principles

Standards such as ISO/IEC 27001 [2] and ISO/IEC 27002 [3] are not directly applicable to cybersecurity of digital I&C systems in NPP, due to their specificities (incl. regulatory and safety requirements). Nevertheless, IEC 62645 has been built to be consistent from a high level perspective with the aforementioned standards: its security life-cycle on the programme level is consistent with the ISO/IEC 27001:2005 standard “Plan Do Check Act (PDCA)” loop, moreover, correspondence with the ISO/IEC 27002:2005 eleven security domains are also reflected in the draft[2].

Globally, IEC 62645 is mainly structured on three layers, corresponding to the three main sections of the standard:
- one dealing with a security life-cycle on the programme level,
- one dealing with a security life-cycle on a system level,
- another one dealing with security thematic areas on a control/requirement level.

According to this standard, the security of computer systems shall be based on a graded approach including consideration of the following:
- three security levels (called security degrees S1, S2 and S3) are defined in the standard. Security measures cannot be defined for each system individually because it would lead to a great amount of studies (and cost) and to many problems to connect communicating systems;
- systems are to be considered from a functional point of view and assigned a security degree according to their possible direct or indirect impact on plant safety and availability;
- generic measures that are given shall be adapted for each level in order to efficiently protect the systems of each considered level.

Some generic features in development of the graded approach include the following:
- similar security programmes shall be drawn up for systems development, involving establishment of a secure development and operating environment during the pre-installation software lifecycle phases;
- similar level of security achievement shall be proven for all systems having a same security degree, regardless of their designer and developer;
- interfaces between systems of different security degrees shall be addressed to enforce

[2] ISO/IEC 27001 and 27002 version 2 (published in 2013) rely on 14 thematic areas, but those versions have been published too late in the standard writing process to be taken into account. IEC62645 is based on the 2005 versions.

restrictions (such as communication pathways);
- interfaces shall be secured but shall not prevent functional transmission.

The assignment of computer systems to different security degrees is based on their relevance to the overall plant safety and plant availability. In addition, computer-based security risk assessment processes is used in the development of the process and detailed controls, corresponding to the high level requirements associated to the different degrees in the standard.

3. STANDARD DEVELOPMENT AND PERSPECTIVES

*3.*1 Development *of the first edition (Issued in 2014)*

A New Work Item Proposal (NWIP) was prepared and submitted by the United States to IEC in 2008, after review by Working Group A9 of SC45A as a new standard to be developed. The NWIP was circulated for voting in 2008 and in 2009 was approved by 19 national committees and 5 national committees designated subject matter experts to work on this new standard: France, Germany, Japan, Sweden and the United States. The first meeting of the working group was in Yokohama in 2009 and significant progress was made on the first draft of the new standard with the assembled subject matter experts. This activity was occurring at the same time that IAEA was preparing to issue a new guideline on computer security [1] culminating in formal issue in 2011. Interim meetings in 2010 in Germany and the full committee meeting in 2012, also in Germany, resulted in a Committee Draft for Vote (CDV) circulated to national committees in 2012. Comments were addressed in the 2013 Moscow full committee meeting and the Final Draft (FDIS) was prepared and circulated to national committees in early 2014. The official standard was issued formally in August, 2014 and a corrigendum in October 2014, to fix some format and reference issues.

In the wake of IEC 62645, several related documents will be developed. As stated before, a second project (IEC 62859) was started in 2012 and was published at the end of 2016:: it focuses on the coordination between safety and cybersecurity. In addition, another daughter standard on security controls, was approved to start in 2015 and is currently in progress. Other specific topics will be covered in the future in other daughter documents: their exact perimeter and the associated timeline of production will depend on the proposals and votes of the IEC SC45A members. Such new documents will provide international reference on what makes the cybersecurity of nuclear I&C a specific area (vs more generic standards like the IEC/ISO 27000 series or the IEC 62443 series). This will be done in consistence with the IAEA international high level guidance (incl. [1]) and the IEC 62645 principles presented in this paper

3.2 Development of the second edition (revision in progress)

IEC 62645 is currently in the revision process. 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 WGA9 recommended IEC 62645 to be revised.
Taking into account the discussions held and the recommendations made, the Project Leaders prepared principles of revision which were reviewed in WGA9 and annexed to a proposal for revision. This record of revision (RR) was circulated in March 2015 in order to open the revision. During the June 2015 Lyon meeting the implementation of the principles of revision was discussed. Considering the discussions held in Lyon the Project Leaders prepared a working draft which was circulated in January 2016 to WGA9 experts as preparatory document for the Gyeongju meeting. The principles of revision include the following major focus areas:

1. IEC 62645 ed. 1 structure and high level principles have been built on the IAEA NSS17, and on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 international standards. The revision shall now take into account 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 shall be reached: this may involve coordination with a future revision of IEC 61513 in order 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 c) with IEC 61513 should be done with IEC 62138 and 60880.

5. The content and structure of IEC 62645 ed. 2 could be rearranged to better take into account the future second level documents with respect to IEC 62645 (IEC 62859 and the NP on security controls).

The revision draft taking into account these principles has been officially circulated in the fall of 2016. It is intended to followup for issue of a CDV in 2017.

4. CONCLUSIONS

In summary, the IEC 62645 standard for computer security brings a new set of guidance from IEC, in conjunction with IAEA and country specific standards, to the international community with regards to

computer security for nuclear facilities. This is the first standard in a new series of IEC nuclear standards to address computer security and respond to the ever growing and expanding threat from electronic means to challenge the protection, control and information systems supporting nuclear plants around the world.

5. REFERENCES

[1] IAEA Nuclear Security Series No. 17, Reference Manual, Computer Security at Nuclear Facilities, Dec. 2011

[2] ISO/IEC 27001:2005, Information Technology – Information Security Management Systems – Requirements

[3] ISO/IEC 27002:2005, Information Technology – Code of Practice for Information Security Management

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

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

[6] IEC 61513, “Nuclear power plants – Instrumentation and control for systems important to Safety – General Requirements for Systems.” 2001

[7] L. Pietre-Cambacedes, T. Quinn "IEC 62859: A NEW INTERNATIONAL STANDARD ON THE COORDINATION BETWEEN SAFETY AND CYBERSECURITY FOR NUCLEAR I&C SYSTEMS," 10*th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC&HMIT 2015)*, San Francisco, USA, June, 2017

[8] L. Pietre-Cambacedes , M. Tritschler and G. Ericsson, "Cyber security myths on power control systems: 21 misconceptions and false beliefs," *IEEE Transactions on Power Delivery*, Vol. 26, Issue 1, pp. 161-172, January 2011

[9] Symantec Security Response, *Dragonfly: Western Energy Companies Under Sabotage Threat*, version 1.21: July 7, 2014