Development of a new IEC Standard on Cybersecurity Controls for I&C in Nuclear Power Plants – IEC 63096

Juergen Bochtler
Siemens AG
PG ES IC T2000SOL PN QC
Freyeslebenstr. 1
D-91058 Erlangen, Germany
juergen.bochtler@siemens.com

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

Edita Bajramovic
Friedrich-Alexander-University Erlangen-Nuremberg/AREVA GmbH
Henri-Dunant-Str. 3
91058 Erlangen, Germany
edita.bajramovic@areva.com

ABSTRACT

Standards are promoting the enhancement of cybersecurity in Nuclear Power Plants (NPP). Standardizing processes and procedures are also crucial to achieve successful international collaboration. Many information security standards were developed in recent years; however, not many of them could be directly applied to NPPs. This paper provides an overview of the development of a new cybersecurity standard dealing with cybersecurity controls for nuclear power plants around the world.

For I&C systems in NPPs, the new IEC 63096 standard targeted for issue in 2019, focuses specifically on the selection and application of cybersecurity controls from the included security controls catalogue. The role of selected and applied cybersecurity controls is to prevent, detect and react to digital attacks against computer-based I&C systems.

This standard applies to the I&C of new nuclear power plants and to the I&C modernization in existing plants. It is being prepared and based on IEC 62645 [1], ISO/IEC 27000 series [3] [4], IAEA [2], and country specific guidance in this expanding the technical and the security focus area. The Standard is intended to be used by designers and operators of NPPs (utilities), systems evaluators, vendors and subcontractors, and by licensors.

While the development of international standards is essential it is also a lengthy process, taking multiple years. Especially with regard to cybersecurity, all involved stakeholders have to collaborate.

Key Words: I&C, NPP, Cybersecurity, Security Controls, IEC

1 INTRODUCTION

The purpose of this paper is to provide an overview of the new International Electrotechnical Commission (IEC) 63096 standard development and its content. Focus is 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.

It is recognized that this is an evolving area of regulatory requirements due to the continuously changing and emerging computer security threats. Therefore, the objective of this standard is to extend the SC45A series of documents addressing cybersecurity with IEC 62645 [1] as its top level document, by defining nuclear I&C specific cybersecurity controls for I&C systems of the Safety Classes 1, 2, 3 and for non-classified (NC). 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.

It is also recognized that this subject matter requires protection and limited release of the products derived from application of these standards to country specific requirements to minimize the extent to which organizations, intending to access illegally, improperly or 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 I&C is used in non-safety systems and systems important to safety, where non-availability or malfunction could affect nuclear safety and continuity of power operation (availability). The I&C system also stores important and sensitive data, where any malfunctions could lead to the loss or corruption of important data (integrity) or unauthorized release of sensitive information (confidentiality). The complexity of computer based I&C systems makes it difficult to comprehensively identify 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 that Stuxnet or more recently, the Dragonfly operation 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 new standards IEC 62645 [1], published in August, 2014, and IEC 62859 [5], published in October 2016, as well as this new IEC 63096 standard on cybersecurity controls, are intended to be used for I&C systems of operating and new Nuclear Power Plants (NPP).

2 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 objective 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 standards presented in this paper are developed by the IEC Subcommittee 45A (SC45A), addressing Instrumentation and control (I&C) of nuclear facilities. SC45A has issued many worldwide

respected references on different issues with respect to I&C, in particular for safety-related I&C [6, 7, 8] for instance). SC45A has been working in close coordination with the IAEA (International Atomic Energy Agency) on safety-related issues for decades, and more recently on cybersecurity issues [1].

3 DESCRIPTION OF THE NEW IEC 63096 STANDARD ON SECURITY CONTROLS

3.1 Scope and objectives

For I&C systems in nuclear power plants, this new project, IEC 63096, specifically focuses on the selection and application of computer security controls from the included security controls catalogue, in order to prevent, detect and react to digital attacks against computer-based I&C systems. The security controls catalogue is specifically tailored to I&C in nuclear power plants.

IEC 63096 applies to INSTRUMENTATION, CONTROL AND ELECTRICAL SYSTEMS of new nuclear power plants and to the I&C modernization in existing plants.

Within the SC45A standard series, IEC 62645 is the top-level document with respect to cyber security. IEC 63096 is located in the second level and will be developed to:

- Ensure consistent understanding of the process of the selection and application of security controls
- Ensure consistent understanding on what security controls are highly recommended and optional for the security baseline and the security degrees S1, S2 and S3 (security controls catalogue)
- Describe a method for crediting/ inheriting existing security controls and safety provisions for I&C systems important for safety
- Describe a method for applying compensatory security controls in case highly recommended security controls cannot be implemented
- Describe a method for handling of legacy systems

Regarding the security objectives it is important to point out that IEC 63096 follows the commonly accepted ISO/IEC 27000 series security objectives:

- Confidentiality
- Integrity
- Availability

3.2 IEC SC45A codes and standards hierarchy and IEC 63096

The following figure shows how the new IEC 63096 standard on Security Controls fits into the existing hierarchy of SC45A IEC standards:

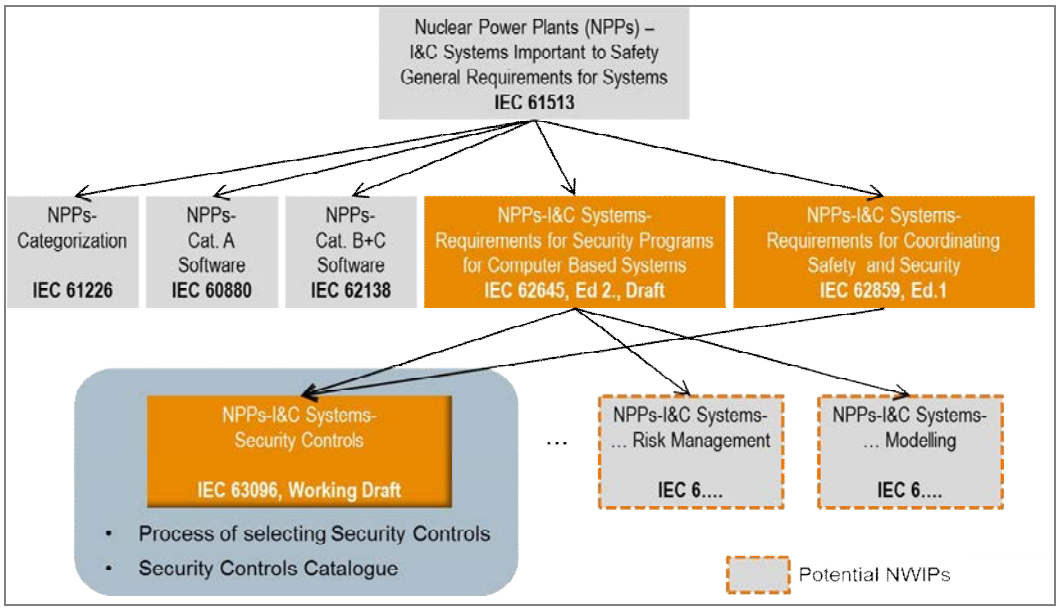

Figure 1. New IEC 63096 Security Controls standard in the SC45A standards hierarchy

An important focus during the development of the IEC 63096 is to assure its consistency with IEC 62645. As a consequence, IEC 63096 is also based on the three security degrees as defined there (Graded approach). In addition to the three security degrees the so called Security Baseline (Basic Requirement) has been introduced. The security baseline is intended for I&C related tools, e. g. diagnostic or engineering systems for the I&C.

Another important aspect is to ensure consistency between IEC 62645 and IEC 63096 on the process of selecting and assigning security controls. Based on the IEC 62645 stipulation IEC 63096 specifies this process in more detail.

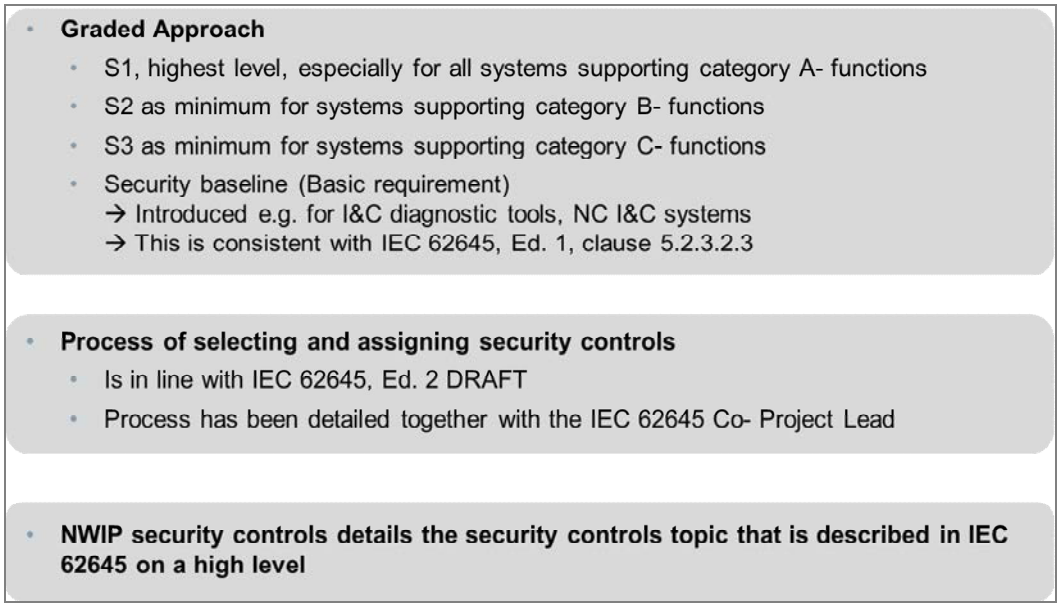

Figure 2. Consistency with IEC 62645 is ensured

3.3 IEC 63096 Structure

In the following, the most important NWIP sections are briefly described

3.3.1 Audience

The first IEC 63096 main section describes the intended audience. It is defined by the parties that are responsible for:

- I&C platform development
- Project Engineering for the I&C system, which also includes installation and commissioning
- Operation and maintenance for the I&C system

The next figure gives more details on the activities assigned to the three groups of audience:

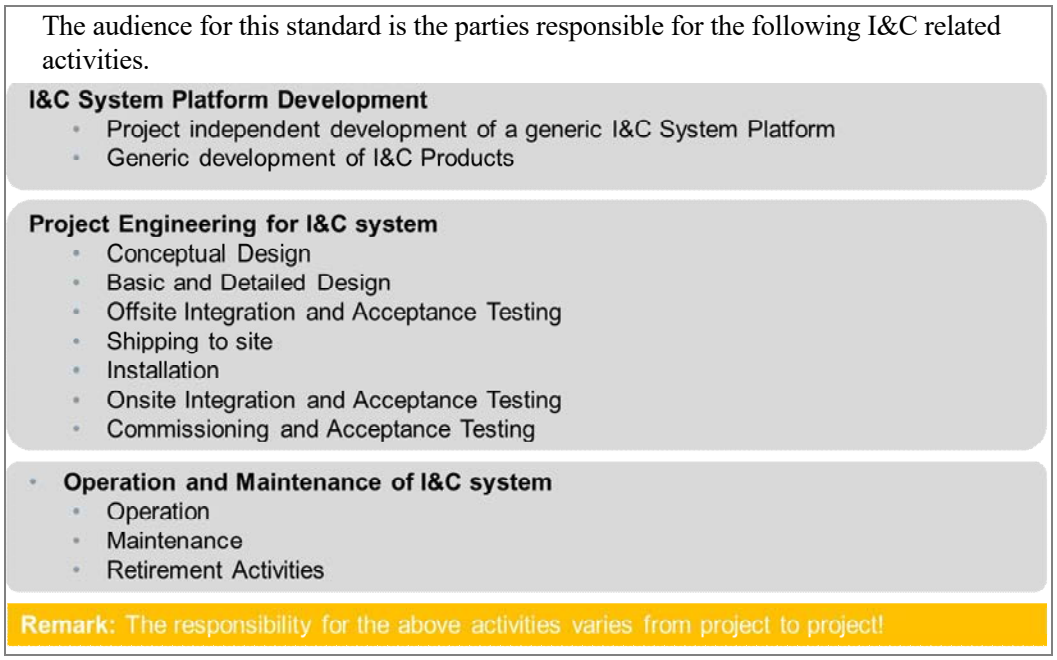

Figure 3. IEC 63096 Audience

3.3.2 Standard security controls catalogue structure and format

Security controls catalogue is based on ISO/IEC 27002

The IEC 63096 security controls catalogue is strictly based on the commonly accepted ISO/IEC 27002 security controls catalogue (ISO/IEC 27002 [4], clauses 5 through 18).

However the ISO/IEC 27002 security controls catalogue is extended and detailed for reflecting the specific security controls needs for I&C in nuclear power plants.

The following three cases on the nuclear I&C specific refinement/extension of the ISO/IEC 27002 security controls are considered:

- Security control is taken over from ISO/IEC 27002 without modification. In any case, the details required by the standardized structure are added.
- ISO/IEC 27002 security control is modified or described in more detail to better meet the specific requirements from the nuclear I&C domain.

- A new security control has been added and embedded into the best fitting ISO/IEC 27002 clause (5 through 18) in order to meet the specific requirements from the nuclear I&C domain. This is the case where the ISO/IEC 27002 does not describe needed nuclear I&C specific security controls. As recommended by ISO/IEC 27009, new security controls will be marked by the acronym "NUC" for Nuclear.

The IEC 63096 security controls catalogue therefore represents the domain specific ISO/IEC 27002 extension for I&C systems in nuclear power plants.

This approach also considers the guidance provided by the new Draft ISO/IEC 27009 on sector specific security controls, while no full compliance is intended.

Standardized format for the description of each single security control

In IEC 63096 the ISO/IEC 27002 security controls description format has been extended.

The standardized format for the description of each single security control structured representation, clearly defines for what Security Degree the specific control is either 'highly recommended' or 'optional'. In addition, further description indicates whether the control preserves the security objectives confidentiality, integrity and/or availability. The control focus in terms of prevention, detection and correction is also part of the standardized format.

The main section of each security control description gives precise implementation guidance on how to implement the control for the nuclear I&C domain. In case there is no domain specific extension of the ISO/IEC 27000 guidance needed, this is indicated by the text "No additional implementation guidance".

The implementation guidance can be specific for the three groups of audience, I&C platform development, project engineering and operation and maintenance.

The following figure shows the security controls description format:

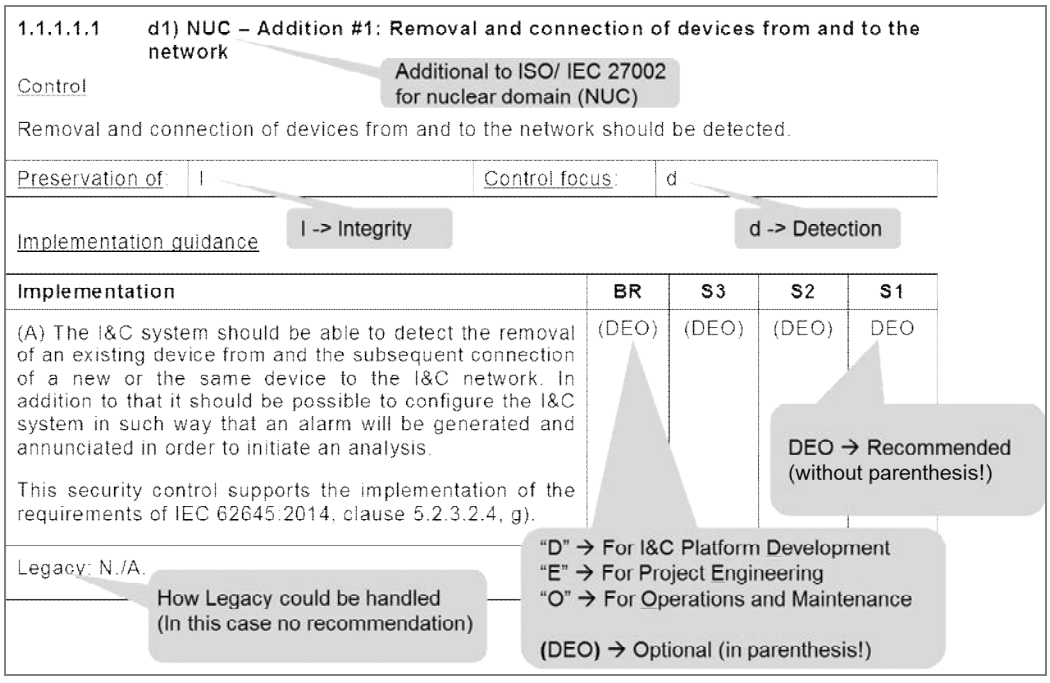

Figure 4. Standardized format for the description of each single security control

3.3.3 Process of selecting security controls

Security degree assignment according to IEC 62645

IEC 62645 [1] defines the process and rules for assigning security degrees to individual I&C systems.

I&C programmable digital system security shall be based on a graded approach. Therefore all I&C programmable digital systems shall be assigned to security degrees S1 through S3.

The three safety categories defined in IEC 61226 are to be taken into account to define the security degrees. I&C systems processing safety category A functions are to be assigned the most stringent security degree (security degree S1). I&C programmable digital systems processing safety category B functions are to be assigned at least to an intermediate security degree (security degree S2). The initially assigned security degree of an I&C system might ultimately need to be adjusted based on the assessment of the maximum consequences of a successful cyber-attack on this I&C system in terms of plant safety and performance. As a result an I&C system can be assigned to a higher security degree as originally defined by the safety category the I&C system is performing.

The assignment of security controls to individual I&C systems is clearly outside the scope of the new IEC 63096.

Security controls assignment according to the I&C system security degree

The third IEC 63096 main section details the process of assigning security controls to each individual I&C systems from the IEC 63096 security controls catalogue.

The process of assigning security controls to individual I&C system starts with the results from the IEC 62645 based phase, where the security degrees have been assigned to each of individual I&C systems.

The IEC 63096 security controls catalogue defines for each single security control whether the security control is ‘highly recommended’ or ‘optional’. Highly recommend security controls are considered a shall requirement. As a result, if a highly recommended controls is not selected, a justification is needed. There might be technical, economical or other limitations for not selecting highly recommended controls. If feasible a compensatory security control shall be defined instead.

Another reason for not being able to implement a highly recommended security control could be that the security control negatively impacts the safety of the I&C system. It can be the case that a specific security control has negative impact on the predictability or the reliability and availability of the I&C system. IEC 62859 [5] provides guidance on requirements for coordinating safety and cybersecurity. In any case safety prevails security.

Inheritance of or crediting existing security controls is permitted and encouraged. Tools and Legacy systems are also considered in this standard.

Each security control selection shall be documented. The resulting documentation then forms the basis for security design & implementation audits and for verification and validation activities.

The implementation of the security controls shall be traceable for each phase of the I&C project:

- Each step of the I&C System Platform Development
- Each step of the I&C system Project Engineering
- Each step of I&C system Installation and Commissioning
- Operation and Maintenance of I&C system

After completion of the Installation, the Cold Commissioning, and the Hot Commissioning it needs to be checked on whether the respective security controls are still in place. This check is also necessary at the end of an outage.

Threat and risk assessment

The security controls catalogue defines a comprehensive set of security controls that provide a good level of cyber protection of individual I&C systems.

However it might be the case that not all cyber security threats and resulting risks are sufficiently mitigated by simply applying the IEC 63096 security controls catalogue.

Therefore after the completion of the security controls selection, a threat and risk assessment is needed to detect the cyber security risks that are not yet properly mitigated and require the implementation of additional specific security controls.

The threat and risk assessment (TRA) is outside the scope of the IEC 63096. One possible practice for risk management is standardized in ISO/IEC 27005 [11].

Each I&C project phase (e. g. acceptance testing, installation, cold commissioning) has its own threat scenario and could therefore require additional phase specific security controls. As a result the TRA should be performed for each major project phase.

The threats to be taken into account depend on the project phase, the associated environment and also depend on the design basis threats that are defined by the local authorities or codes and standards.

Before performing a TRA the acceptable risk level is to be defined by the parties responsible for the TRA for the respective I&C project phase. The acceptable risk level could be based on the local codes and standards and the requirements of the local authorities.

As part of the continuous improvement it is recommended to regularly update the risk assessment, especially in the case of

- new or modified I&C system assets or
- new regulations to be met and also to
- reflect the fact that the cybersecurity threat landscape continuously changes.

Process overview and interaction of IEC 63096 with SC45A cybersecurity standards

The following drawing gives a high level overview on the process of implementing security controls for I&C for nuclear power plants. It also shows on where the IEC 63096 connects with the other SC45A cybersecurity standards, IEC 62645 and 62859.

The main process steps from a high level perspective are (see yellow numbered circles in figure 5):

1. I&C system security degree assignment according to IEC 62645
2. For each individual I&C system selection of the security controls according to the new IEC 63096
3. Definition of the final security architecture including zoning and assigned security controls for system hardening
4. Execution of the Threat and Risk Assessment for each individual I&C system for detection and mitigation of potential remaining security risks. This includes the definition and implementation of additionally needed suitable security controls for mitigating newly surfaced unacceptable cybersecurity risks.

Due to potential additional or modified I&C system assets and the continuously changing threat landscape:

5. Periodical reassessment of the Threat and Risk Assessment. As a consequence for newly surfaced unacceptable cybersecurity risks, new risk mitigations and security controls respectively might need to be defined and implemented into the 'secured I&C architecture' and the 'secured individual I&C systems'.

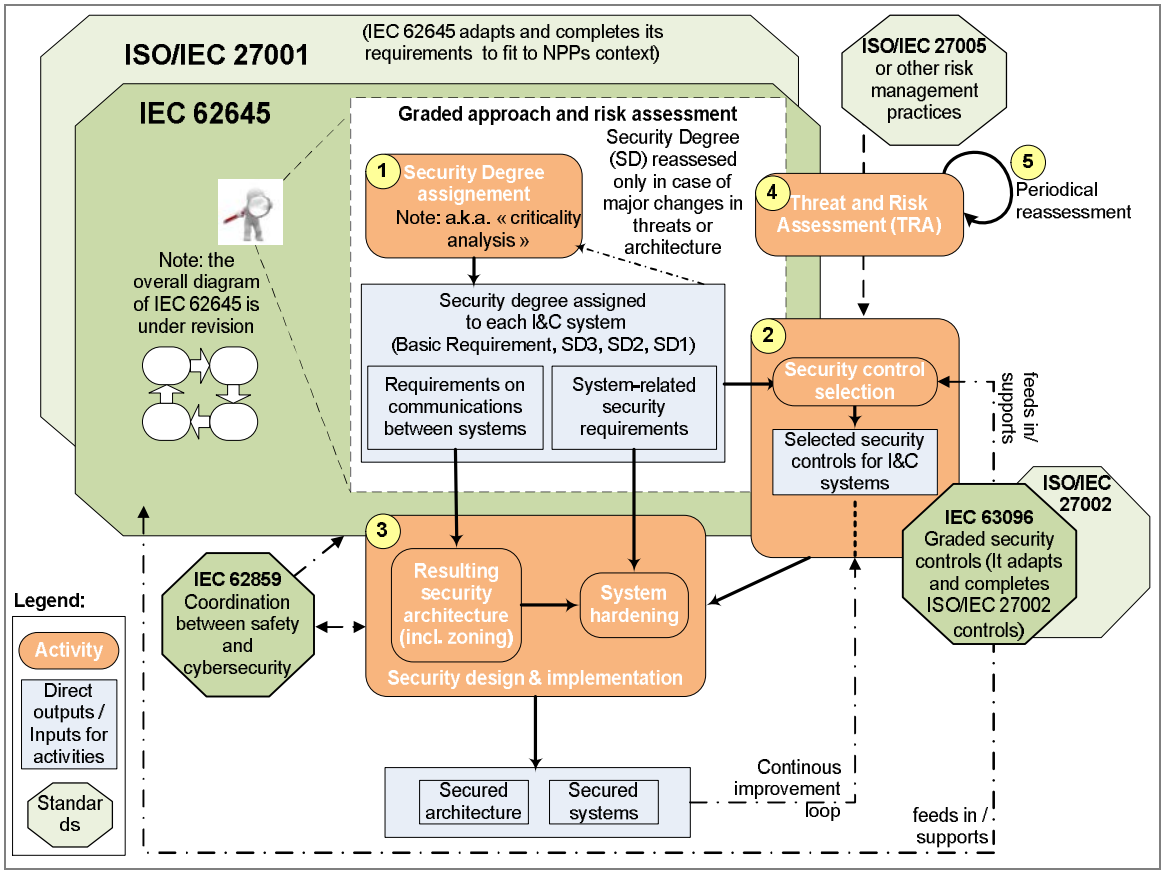

Figure 5. Process overview and IEC 63096 interaction with SC45A cybersecurity standards

Security controls catalogue

The fourth IEC 63096 main section consists of the security controls catalogue. It mirrors and extends all security controls defined in ISO/IEC 27002 for the nuclear domain. Each security control is described in the standardized structure as described above.

3.4 IEC 63096 development schedule

The NWIP was developed by a small core team and was submitted to IEC for voting in the middle of May 2016. At this point of time the main body of the NWIP was already fully worked out in a first version. The NWIP also contained a variety of fully developed security controls. This was to give the voting IEC community a maximum of clarity on the path going forward to a fully developed IEC 63096.

In July 2016 the NWIP was approved with a 100% approval rate. The working group commenced work in August 2016. In the meantime the original small NWIP team has grown to about twenty members from North America (United States, Canada), Asia (India, China, South Korea, and Japan), Russia and

Europe (France, United Kingdom, Sweden, Bosnia Herzegovina, Germany), which helps to reach a wide acceptance of the new IEC 63096.

The first complete proposal of the Committee Draft (CD) will be reviewed and improved at the next IEC TC45A conference that takes place in Shanghai, China, in October 2017. The circulation of the first CD (Committee Draft) for official review by the IEC world community is targeted for the end of November 2017. According to the current planning, this IS (International Standard) is expected to be formally issued end of September 2019.

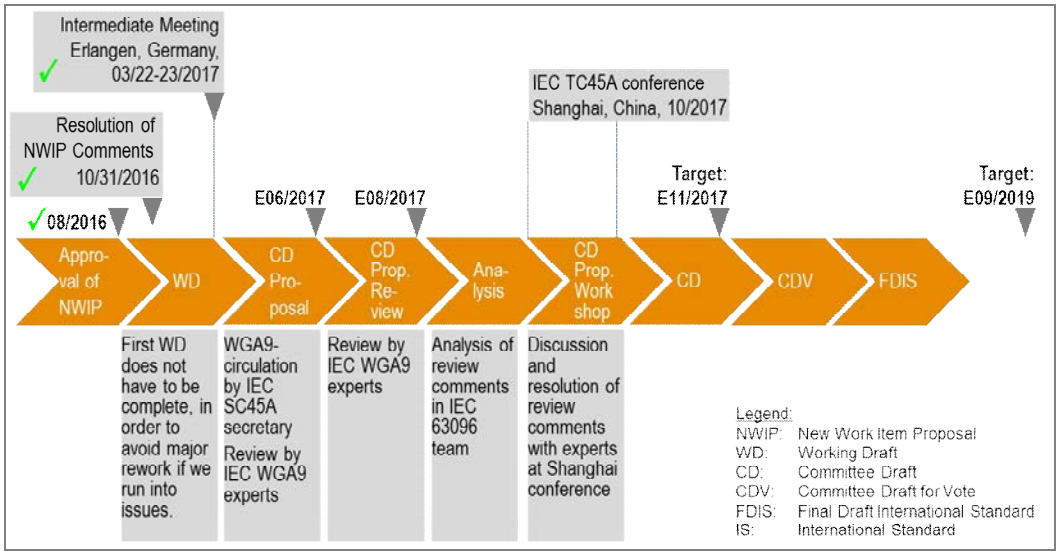

Figure 6. IEC 63096 development schedule

4 CONCLUSIONS

In summary, the IEC 63096 SC45A 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.

For I&C systems in nuclear power plants, this new IEC 63096 standard on security controls, is part of the IEC 62645 family of standards and specifically focuses on the selection and application of computer security controls from the included security controls catalogue in order to prevent, detect and react to digital attacks against computer-based I&C systems.

Other initiatives and documents will also complete the series, depending on the needs, interest and proposals from the nuclear community and the IEC national committees.

5 REFERENCES

1. IEC 62645, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programs For Computer-Based Systems, 2014
2. IAEA Nuclear Security Series No. 17, Reference Manual, Computer Security at Nuclear Facilities, Dec. 2011
3. ISO/IEC 27001:2005, Information Technology – Information Security Management Systems – Requirements
4. ISO/IEC 27002:2005, Information Technology – Code of Practice for Information Security Controls

5. IEC 62859, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity, Edition 1.0, 2016-10
6. IEC 61513, “Nuclear power plants – Instrumentation and control for systems important to Safety – General Requirements for Systems.” 2001
7. IEC 60880, Nuclear Power Plants – Instrumentation Systems Important to Safety – Software Aspects of Computer Based Systems Performing Category A Functions, 2006
8. IEC 62138, “Nuclear power plants - Instrumentation and control important for safety Software aspects for computer-based systems performing category B or C functions,” 2004.
9. IAEA Nuclear Security Series No. 036 (NST 036) [Draft]: Computer Security of I&C Systems at Nuclear Facilities, Technical Guidance, IAEA, 2011
10. ISO/IEC 27009:2013, Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements (DRAFT)
11. ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management