Contribution ID: **31** Type: **Paper**

IEC Standard-Family on Cybersecurity for Nuclear Power Plants

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, 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 fits to the IEC SC45A framework and to other IT security 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 considers 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 be consistent to relevant IEC 62443 controls and (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 also on track to become an EN standard.
- The standard IEC 63096 focuses on security controls and provides a catalogue adapted for nuclear I&C contexts. 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.

Gender

Male

State

Germany

Authors: Mr WALTER, Thomas (PreussenElektra GmbH); PIETRE-CAMBACEDES, Ludovic (EDF); QUINN, Edward (Technology Resources); Mr BOCHTLER, Jürgen (Siemens AG)

Presenter: Mr WALTER, Thomas (PreussenElektra GmbH)

Track Classification: CC: Information and computer security considerations for nuclear security