Contribution ID: **9** Type: **Roundtable Member**

Industrial cyber security standard - IEC 62443

Monday, 5 November 2018 16:15 (5 minutes)

At the beginning I will discuss the implementation of the European NIS Directive in Germany, as well as Austria. Operators of critical infrastructure are required to implement appropriate organizational and technical arrangements according to the "state of the art".
In determining the state of the art, particular reference must be made to relevant international, European and national norms and standards, but also to comparable procedures, facilities and modes of operation that have been successfully tested in practice.
I have been working on IT security and IT standards for the last 20 years and have now extended my education to the topics of cyber security and OT standards (Operational Technology). As a Cyber Security Practitioner (CSP), I perform Cyber Security Checks to BSI using ISO / IEC 27001. As an IEC expert of the OVE Austrian Electrotechnical Committee, I work on the IEC 62443 (TSK-MR65) series of standards. Additional I have for the test procedure according to § 8a (3) BSI law, an additional training for the execution of IT security audits with operators critical infrastructure (KRITIS).
As a standard for IT risk assessment and state-of-the-art IT risk treatment, ISO / IEC 27001 is recommended as an information security management system (ISMS). However, this can not be applied 1: 1 for critical infrastructure operators (KRITIS). The assessment of the appropriateness and appropriateness of the risk treatment or measures for KRITIS must not have any impact or disruption on society's security of supply.
In-depth industry-specific industry safety standards are available, with international emphasis on IEC 62443. This standard defines the roles of manufacturers, integrators and plant operators, as well as technology for the design of zones and transitions, ie security design.
I focus on the OVE drafts "Life cycle requirements for safe product development (OVE EN 62443-4-1) and" Requirements for components of industrial automation systems (OVE EN 62443-4-2) and the international standard ISA / IEC 62443 -3-3.
I show afterwards as a practical example of our networksecurity implementation according to IEC 62443 in the pilot factory 4.0 of the Vienna University of Technology.

Topics

CHA2

Primary author: Mr KRONFUSS, Erich (PHOENIX CONTACT GmbH)

Presenter: Mr KRONFUSS, Erich (PHOENIX CONTACT GmbH)

Session Classification: [CHA] Keeping Pace with IT Security - Threat Intelligence for the IAEA/Nuclear Regulatory World

Track Classification: Addressing Growing Safeguards Challenges (CHA)