Security standards

Effective and efficient security based on international standards

It is not only since the successful cyber attacks on the Ukrainian power supply with 225,000 customers affected by the blackout in December 2015 that we understand our critical infrastructure is vulnerable. The national and international legislatures had initiated suitable regulatory requirements for the protection of the critical infrastructure against cyber attacks before that.

Regulations

The German parliament has passed the IT Security Act on 12 June 2015. The law requires the operator of a critical infrastructure to take on a holistic view when assessing and handling risks. This includes the implementation of a management system for information security for which conformity with ISO/IEC 27001 must be certified.

On a European level, the European Parliament has passed the Directive on the security of network and information systems (NIS directive) on 06 July 2016 which became effective in August 2016.

Dipl.-Ing. *Andreas Kohl* (left), Lifecycle Manager Cyber Security, Energy Management Division, Digital Grid, Siemens AG, Nuremberg

Dipl.-Inf. *Chaitanya Bisale*, Product Lifecycle Manager, Senior Key Expert Cyber Security, Energy Management Division, Digital Grid, Siemens AG, Nuremberg

The member states had to implement the directive into national law until 09 May 2018. The criteria which infrastructures fall under the NIS directive must be defined by the EU member states until November 2018.

The key requirements are:

- Definition of a national security strategy,
- Mandatory reporting of security incidents,
- Definition of measures for securing a high common level of security of network and information systems across the European Union.

Only minor amendments of the German IT Security Act were required in 2017 to fulfill the NIS directive.

The European General Data Protection Regulation (GDPR) on the other hand, became effective on 25 May 2018 across the whole EU and does not require implementation in national law. The GDPR addresses the protection of personal data. This makes the GDPR a basic requirement for the involved roles - operator, system integrator and product supplier - in energy automation.

The common ground of all regulations is the holistic approach which in this case means the considering security across organizations, processes and technologies. The weakest link in the chain is always responsible for the overall security. This weakest link can be a person, a process or technical equipment.

All involved roles must contribute their share for a secure infrastructure (Figure 1).

Operator

The key requirement for the operators in Germany is the mandatory implementation of an ISMS (Information Security Management System) in compliance with ISO/IEC 27001. This process requires the operator to implement infrastructure measures corresponding to the risks.

System integrator

For system integrators and service providers it is also essential to protect their own infrastructure. An ISO/IEC 27001-compliant ISMS is a good solution for this. The protection of the own IT infrastructure is a prerequisite for installation and maintenance of secure solutions for the operator.

If information about a customer plant is disclosed after the system integrator's data storage were to be compromised, cyber attacks on the customer system could be facilitated.

The actual technical security requirements of a system are defined in standard IEC 62443-3-3 (see box). The integration process, i.e. how the system is implemented, is described in standard IEC 62443-2-4.

Product supplier

The product supplier as well has to protect his own infrastructure, ideally ISO/IEC 27001-compliant.

Critical data belonging to the product supplier can include software source files that need to be protected against unauthorized manipulation. Otherwise, such a manipulation could open a "back door" for potential attackers.

The functions implemented in the components should be state-of-the-art and allow for interoperability. This is ensured with an implementation in compliance with the IEC 62351 security standards.

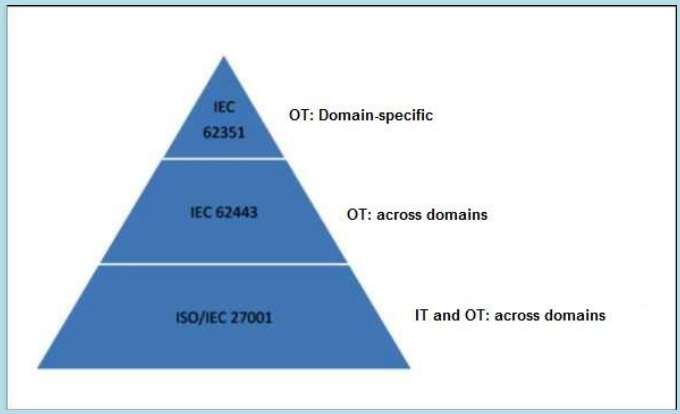
Supplier management

One topic in the ISO/IEC 27001 standard dealing with the protection of interfaces between the involved roles is supplier management.

Technical article / German version published in the magazine "netzpraxis 09-2018"

International security standards:

The standards stated in this article put different emphases depending on the addressee, technical or process orientation and technical depth of the requirements.



Standards building on each other

ISO/IEC 27001 describes requirements for an Information Security Management System (ISMS). Formally, the ISMS covers all information, therefore also printed and written information. In other words: How do I operate infrastructure in order to protect information according to their criticality. It is not important whether the infrastructure is IT or OT (Operational Technology). ISO/IEC 27001 also applies across domains. It can be applied to an office infrastructure of a toy factory as well as to substation automation for power supply as part of the critical infrastructure. ISO/IEC 27001 is therefore a basic standard defining process requirements.

IEC 62443 with 13 parts focusses on the protection of an industrial automation and control system (IACS) and therefore on an OT infrastructure. The recipients here are all involved roles: the operator of the system, the system integrator and the product supplier. Process requirements are also defined as technical requirements for individual components and for the entire system. The technical requirements define generic requirements, i.e. the WHAT, and leave the detailed technical solution mostly open.

The last level of the security standards are the OT and the domain-specific security standards. IEC 62351 serves as an example, describing the HOW based on the technical requirements of IEC 62443. The standard IEC 62351 addresses requirements for the product supplier and defines how the technical solution shall be realized. The objective here is interoperability. The technical depth is therefore the highest of the various levels described here. IEC 62351 is domain-specific and describes the different procedures for energy automation, for example the protection of the communication protocols used in energy automation, e.g. IEC 61850 or IEC 60870-5-104.

Access control and user administration can serve as an example for the seamless integration of these standards.

ISO/IEC 27001 requires a process implemented by the operator which ensures the “Need-to-Know” principle.

IEC 62443-3-3 requires a technical solution for user authentication and authorization on system level. Whether access is granted within a secure zone or via unsecure networks defines the severity of the requirement.

Part 8 of IEC 62351, on the other hand, describes how to implement the technical solution of RBAC (Role Based Access Control) to achieve interoperability.

This is a possible categorization of the security standards in order to better understand how to use them. More information can be found in [1].

The use of these standards covers the requirements of the BDEW whitepaper [2] and exceeds them in many areas.

The system integrator acts as the supplier for the operator. The operator must not only describe the requirements for the technical solution when selecting a supplier, but also define the requirements for the supplier processes. The same applies to the relationship between system integrator and product supplier and of course also for the relationship of the product supplier to suppliers providing modules or software components.

After all, a compromised module or software component determines the total security of the solution.

Supplier management should continuously cover the whole supply chain from the module or software of a component up to the entire system.

Suppliers and sub-suppliers which already hold certification in compliance with ISO/IEC 27001 can build trust, and efforts for own supplier audits can be reduced.

Summary

Applying international security standards is efficient and ensures effective security. Why? International standards provide harmonized requirements. This means that fewer gaps can be expected when using the standards compared with requirements defined in-house.

Security standards

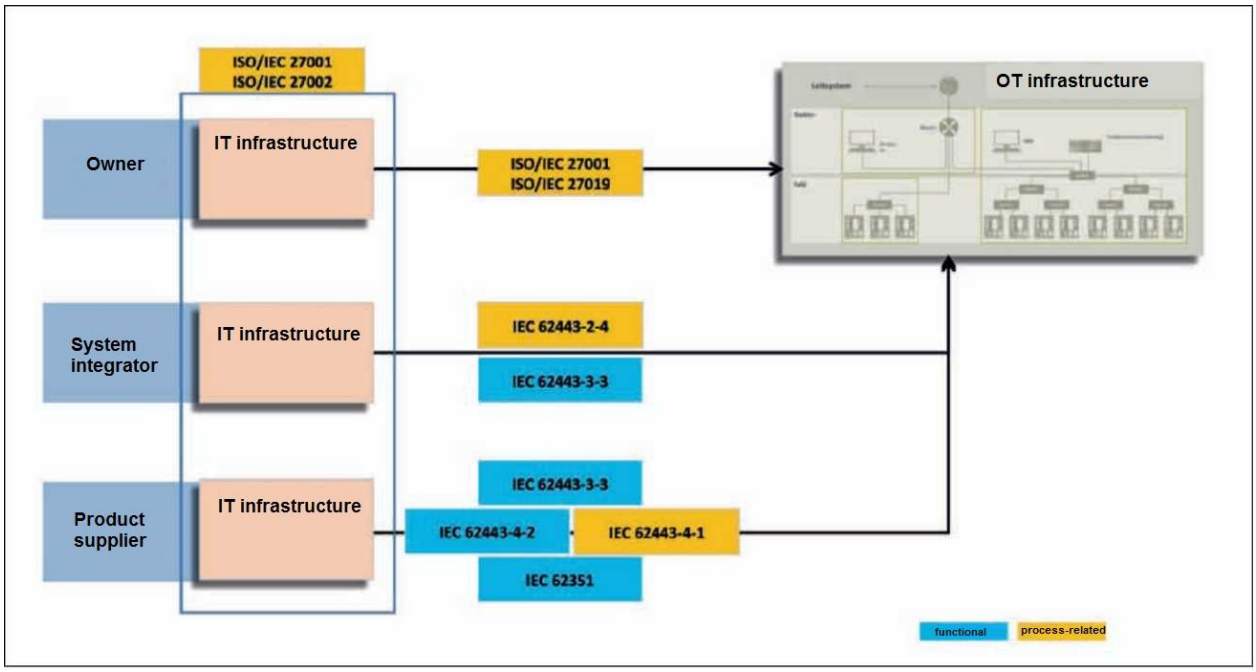


Fig. 1: Using standards for the involved roles

Standards ensure interoperability. Referring to standards like IEC 62443 and IEC 62351 in a tender ensures fewer errors, avoids misunderstandings and therefore saves time and money. Nobody would think of defining the environmental requirements of components without using standards.
The international standards build on each other, see also the box "International security standards". Standards provide a clear basis. A supplier with his own, ISO/IEC 27001-compatible infrastructure is better able to understand the requirements of an operator who has to operate his OT infrastructure in compliance with ISO/IEC 27001.
In addition, only certification based on international standards is meaningful and comparable. The ISO/IEC 27001 certification of suppliers, increasingly demanded by operators in the scope of supplier management, can build additional trust.

Literature

[1] Cyber Security & Privacy; CEN-Cenelec-ETSI Smart Energy Grid Coordination Group; 2016-12

[2] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V; Österreichs Energie: Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Vollständig überarbeitete Version 2.0, 05/2018

andreas.kohl@siemens.com

Chaitanya.b@siemens.com

www.siemens.com