AUVESY.
We simplify automation

IEC 62443: IT security for automation solutions

From threats to protection levels

1. General | 2. Policies & Procedures | 3. System | 4. Component

While IT and OT may have similar aims when it comes to security, the way they set their priorities is quite different. So how does one go about harmonizing the risk management approaches of both? One answer, outlined in the IEC 62443 standard, is to segment complex production facilities and to implement a "Defense-in-Depth" approach. In the context of automation facilities, operational safety, and information security, this means data backups, tracking changes, and documentation.

Information Technology (IT) and Operational Technology (OT) – represent two worlds in which the term security is used differently. The differentiation in English between the terms safety and security illustrates this. Security refers to the safeguarding of data (i.e. information security), while safety denotes operational safety, i.e. the safeguarding of people and the environment from physical harm.

IT and OT are in agreement when it comes to how they define their security aims. In both cases, these are confidentiality, integrity, and availability of data and devices. It gets slightly more controversial when it comes to how the security aims are prioritized. While confidentiality is the highest priority for IT, which places the protection of data against unauthorized access above the immediate and constant availability of data to the user, it is not the same for OT. It goes without saying that industrial devices need to be protected from both physical and cyberattacks. However, even if the plant or parts of it are affected by negligence or attack, the continuation of production is what has the highest priority here.

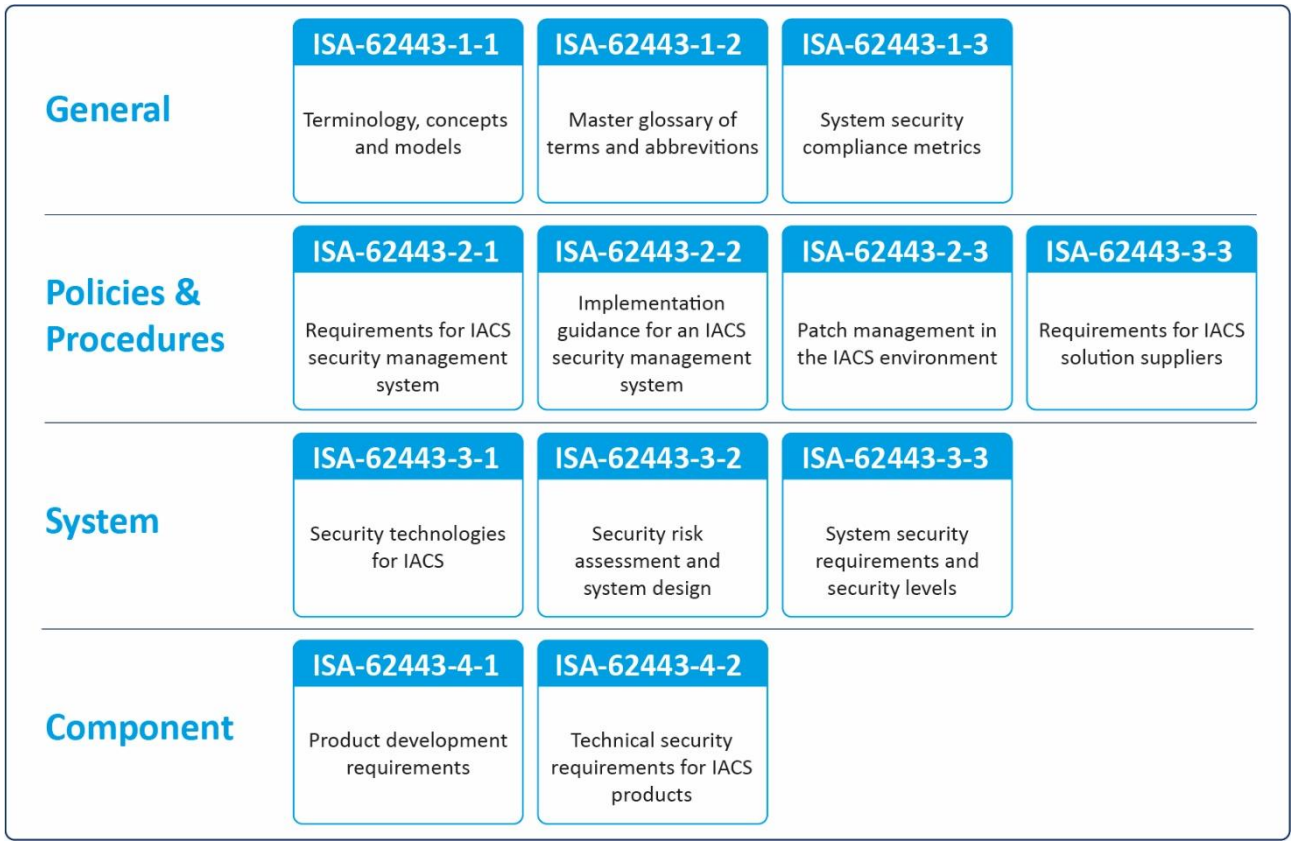
Despite having different rules and regulations, when it comes to risk management, IT and OT follow similar procedures. An analysis of risks and hazards is followed by a risk assessment. Finally, the security concept outlines potential countermeasures. The risk assessment thus follows the same approach; a limit defines which residual risk is accepted and which is not. For those risks which are deemed unacceptable, countermeasures need to be implemented in order to reduce them. The approach differs according to the object in consideration. IT experts, in contrast, take a more straightforward approach; risks are listed, categorized, and finally measures for tackling them are given. In automation, the life cycles of the plant are also listed, including the type and probability of risks, before measures for risk reduction are laid out. The risk assessment is only carried out at the end.

Reconciling the differences between IT and OT

In light of ongoing developments with regard to all things IoT related, it is becoming increasingly important to reconcile the differences between both worlds. This is because internet connection to automation systems opens the door to unwanted network access. The IEC 62443 standard defines protective measures for different network levels.

The IEC 62443 standard differentiates between the roles of product suppliers, system integrators, and operators. The product supplier is responsible for the development, distribution and maintenance of system components used in the automation solution. The system integrator is responsible for composition, configuration, and commissioning. Finally, the operator is ultimately responsible for system operation and maintenance, as well as closing the facility at the end of its life cycle.

The standard comprises twelve documents, divided into four sections:

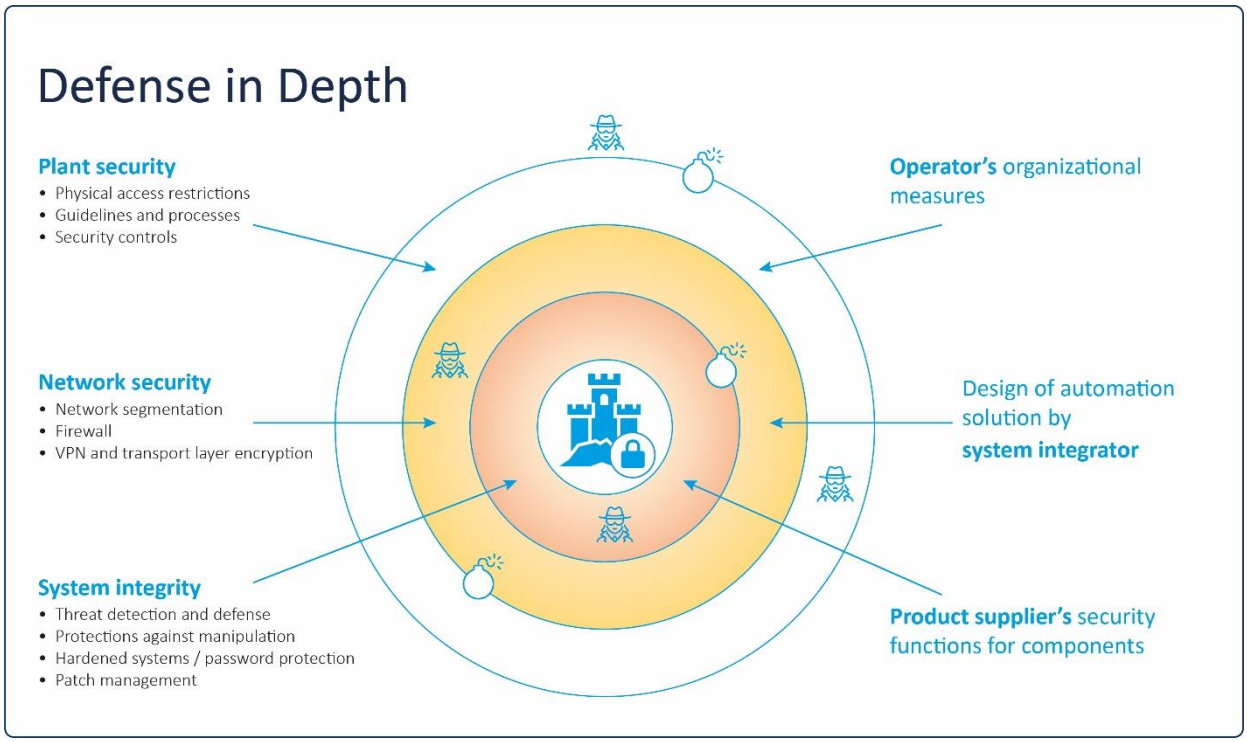


1. **General**
   This section deals with concepts, terminology and models
2. **Policies and Procedures**
   In this section, organizational measures and processes, including recommendations for patch management are presented. The target groups of this section are operators and system integrators.
3. **System**
   The contents of this section include the IT security requirements with regard to the functional capabilities of the system, as well as methods and means of segmenting the solution so that it can be best protected against cyber-attacks.
4. **Component**
   While the section System is aimed at the product supplier of the entire automation solution, the product suppliers of individual components are addressed here. Here too, it is important to develop the components so that they meet security requirements and avoid weak points from the outset. Measures are listed here to ensure the robustness of the components.

Three lines of defense: data security from the outside in

One essential aspect of the IEC 62443 standard is Defense-in-Depth.

While operational safety – as mentioned before – is concerned with ensuring functional safety, information security is much more complex. Numerous measures need to be taken in a coordinated manner. The Defense-in-Depth approach can be likened to a castle: various lines of defense (usually arranged from the outside in) protect the castle from threats and intruders.



The first line of defense serves to protect the production facility itself. The standard requires that certain steps be taken, such as physical access restrictions, guidelines and processes concerning the use of the facility and controls to ensure that these are adhered to.

The second line of defense concerns network security. Network segmentation creates a production cell that is protected from the outside and that can only be accessed by authorized persons. It is the job of the system integrator to take appropriate measures, such as the use of firewalls, passwords, or the protection of external access via VPNs.

The inner lines of defense can be observed in the security functions found on devices or components. These can be encrypted or protected via a virus scanner. It is the task of the product supplier to ensure this.

Zones and channels: the task of segmenting complex facilities

When it comes to functional safety of a production facility, the requirements are divided into levels. Each level corresponds to a number that describes the ability of the facility or device to prevent harm from occurring to the environment or to personnel.

Information security is multidimensional and cannot be described simply by using a number. One possibility to segment complex production facilities is to separate them into zones and to create channels between zones.

The first zone is always the entire production facility and how it connects to the surrounding infrastructure. The organizational measures taken by the operators are of importance here.

Finally, the solution is separated into individual zones, between which interfaces are constructed. The component product supplier is responsible for these individual zones; however, the interfaces need to be coordinated with the operator. The system integrator is obligated to consider the security and safety requirements of the facility when selecting components.

The goal is to create a protection level for each zone. This helps to reduce the complexity of creating a risk analysis for the entire plant and is sufficient to evaluate the functions performed in each zone and the channels between zones.

From threat to protection level

The starting point for determining a protection level is a fundamental requirement (FR). This may, for example, require authorization of a system, such as a key switch on a device or write protection.

A detailed technical system requirement (SR) is defined based on the functional requirements. Security levels are defined in the process. As mentioned before, a number is assigned which describes the ability of a system or device to prevent harm to the environment or to personnel.

Opposite the organizational level is the maturity level, or the means of implementing functional measures. In comparison to the functional measures in place, it is important that organizational measures are implemented by personnel and lived. This requires for processes to be documented, personnel to be trained, and implementation to be monitored.

By combining the evaluation of the functional measures and the degree of maturity in the corresponding organizational measures into a two-dimensional matrix, a protection level can be assigned to each field of the matrix. The ability to protect is contrasted with the protection that can be achieved.

To summarize: the IEC 62443 standard uses the advent of the introduction of information security in the world of automation as an opportunity to connect two worlds between which there are not only significant differences in complexity, but also with regard to protection aims and priorities. Various concepts are used in order to manage the complexity of information security in an automation facility by dividing the facility into components, introducing different levels of security and, most importantly, ensuring those persons involved (i.e. product suppliers, system integrators, and operators) implement this security within their area of responsibility.

Three areas in which OT security is present

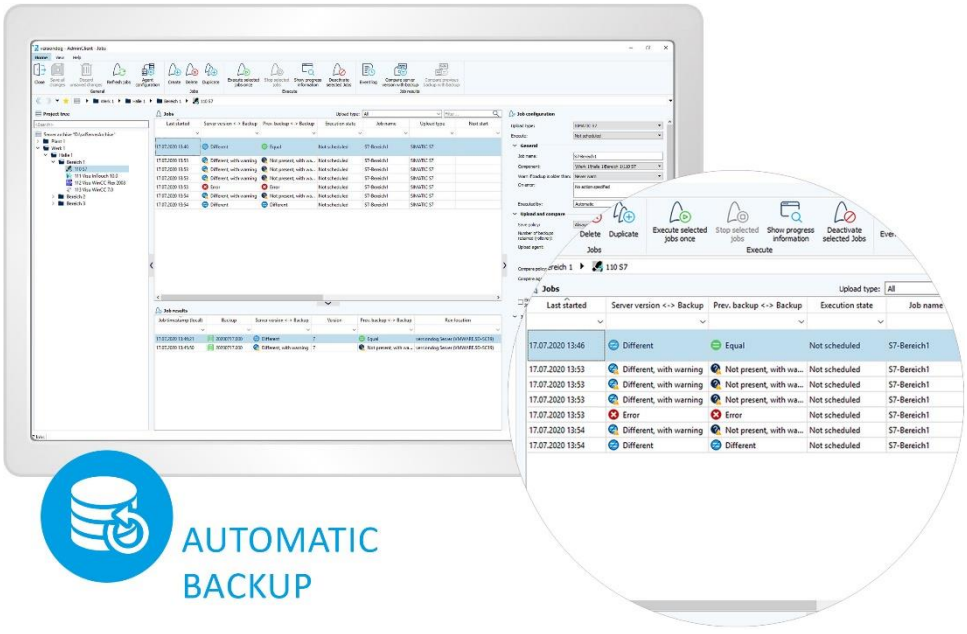
The required measures can be divided into three main areas:

1. Data backup in the form of backups and versions
2. Tracking changes by comparing data sets
3. Documenting changes in an event log

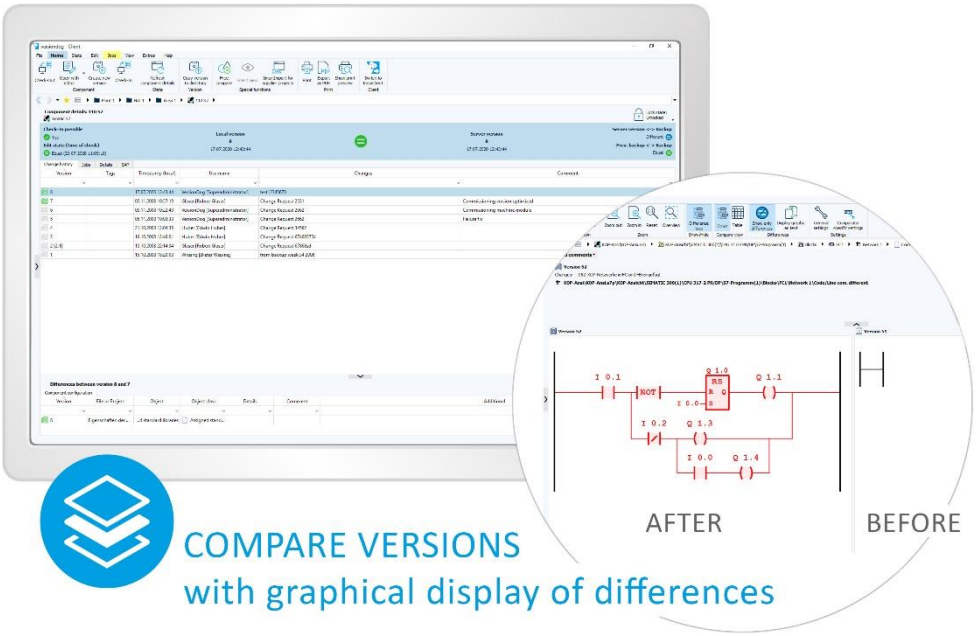
An urgent preventative measure for emergency situations can be assigned to several of these areas: the quick and reliable recovery of data.

The data management system versiondog demonstrates how the interaction between these three areas can work together to maximize the information security of automation systems.

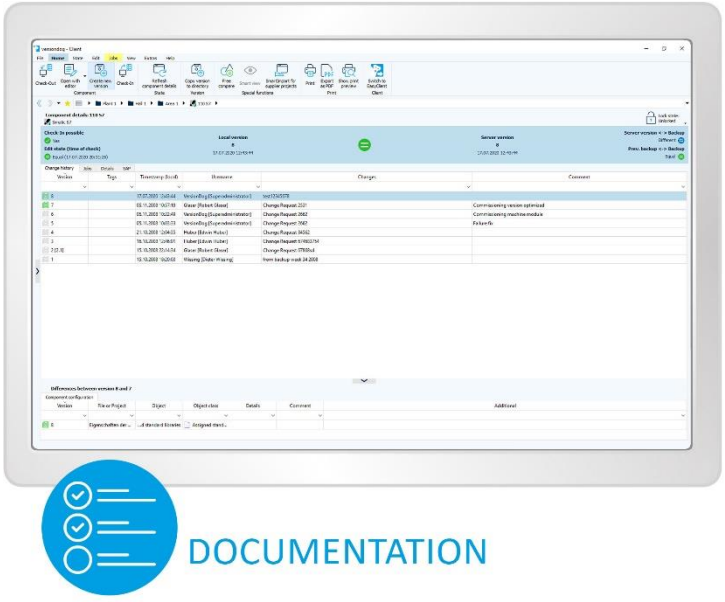
The solution supports many automation components and devices from different manufacturers. Integrating all components into versiondog allows for centralized, regular, and automatic data backups and allows you to compare them with the status of the server. This not only ensures that the data is always up to date, but it also allows for trouble-free disaster recovery.



Changes between different versions are displayed graphically, in a table and in text. This enables the operator of the facility to see at a glance who changed what, where, when and why to a project. This gives him requisite transparency to see whether the person who made the changes was authorized to do so or whether he is dealing with manipulation or a hacker attempt.



In order to track discrepancies retrospectively (as well as to meet legal and regulatory requirements) versiondog automatically documents all changes in the form of a change history. This allows for change logs to be quickly and easily generated for audits.



For more information about the concrete measures needed for safeguarding critical infrastructures, take a look at our article on IT baseline protection requirements https://auvesy.com/de/leitfaden-it-grundschutz#c3206.

www.versiondog.de

Author:
Monika Biedlingmeier
Technical writer,
AUVESY GmbH