Barracuda
Your journey, secured.

Implementation of IEC 62443

with Barracuda CloudGen Firewall

WHITE PAPER

NETWORK SECURITY

Introduction

We encounter digitization with all its advantages and disadvantages in almost all areas of life. The industry in particular has undergone lasting changes due to the arrival of new concepts. While processes have been automated for over 50 years, the advent of Industry 4.0 has brought about a real change. In order to meet modern requirements, it is now essential to permanently analyze data in order to detect even minimal deviations in quality and to exploit new potential for improvements or cost reduction.

Traditional island solutions and air-gaps for sealing off networks and facilities had to make way for real-time data collection and control interventions. Proprietary protocols are gradually being replaced by IP-based communication, as many new concepts require uniform networking. Predictive maintenance, big data and digital twins do not exist without data. Public cloud offerings with their sheer endless scalability and computing power are also pushing into the industry.

At the same time, however, networking of systems means that they are vulnerable and often also vulnerable to attack. Even if the system is not available on the Internet, appropriate protection must still be provided, especially since endpoint security and regular update cycles, as known from IT, are difficult to implement in OT networks operating around the clock and with much longer product life cycles.

Already at the beginning of the last decade, Stuxxnet has shown that it is necessary to react and protect installations efficiently with an upstream defence-in-depth concept.

What is IEC 62443?

The aim of the IEC 62443 series of standards, some of which are still in progress, is to address the gap in IT security in “Industrial Automation and Control Systems”, or IACS for short. Developed by the ISA (International Society of Automation) and the IEC (International Electrotechnical Commission), the standard is intended to help increase the safety, availability, integrity and confidentiality of components and systems in industrial environments. The family of standards provides a framework for addressing weaknesses in IACS. In particular, the comparatively high requirements for integrity and availability in industrial environments are taken into account. Existing standards such as the ISO/IEC 27000 series are used and the characteristic differences in industrial plants are addressed.

Above all, hazards to life and limb and the environment are rarely found in classic IT systems, but are top priority in OT (Operational Technology) networks.

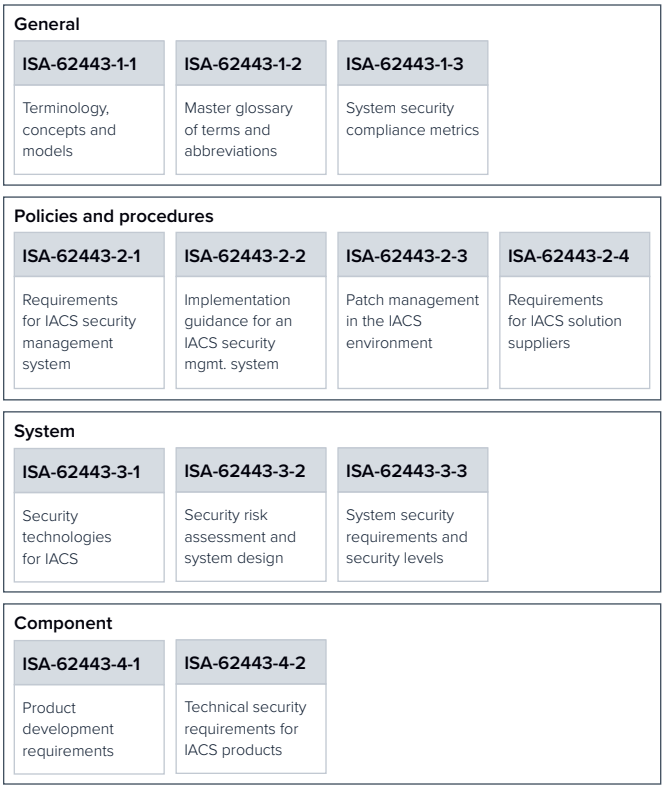
The standards series consists of the following four parts:

Part 1: General - Contains an introduction, basic information, abbreviations.
and terms.

Part 2: Policies and Procedures - Explains technical information on security measures for system operators and owners, as well as service providers. In addition, it primarily deals with requirements for a system for managing industrial IT security. There is also a reference to the ISO 27000 series. The basic objective is the continuous improvement of the security level.

Part 3: System - Specifications for the safety functions of control and automation systems are mainly found in this section. Systems are categorized according to their security level in order to be able to derive appropriate measures for protection.

Part 4: Component - Deals with the requirements for product development of components and automation technology.

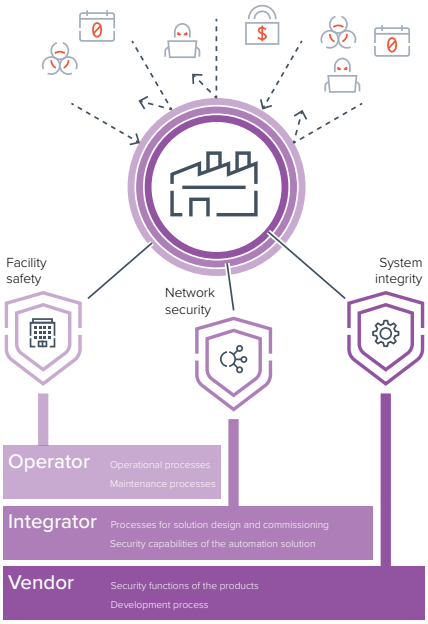


The concept of IEC 62443

The interaction of technical and organizational measures is essential. Optimum security can only be achieved by a combination of both. Technology is essential, but smooth processes, complete documentation and security awareness are also central components. Security is not a one-off measure, but a continuous process. Both the requirements and the measures must be continuously reviewed and, if necessary, adapted. Both probability and impact are taken into account in the decision. Once again, availability and the danger to people and the environment are in the foreground, but a calculated risk is not excluded.

Overall safety in industrial plants can only be achieved by a multitude of coordinated measures. Defense-in-Depth is the basic principle. Security measures are built up in several stages. In order to reach his goal, an attacker must overcome a multitude of different hurdles, which makes the task immensely difficult. Nevertheless, the quality of individual measures must not be neglected. Each individual security level should claim to be insurmountable.

However, maximum security can only be achieved if everyone works together. That is why IEC 62443 in its various parts is aimed at plant operators, integrators, and component manufacturers. The requirements are defined as Security Program Elements for operators, System Requirements (SR) for integrators and Component Requirements (CR) for manufacturers, and they interact very strongly in order to ultimately achieve and cyclically evaluate the appropriate Security Level (SL) for the plant.



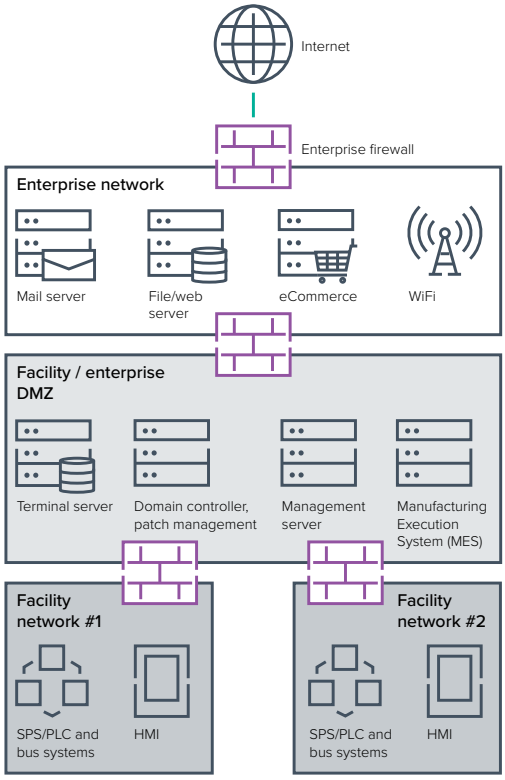
Security risks force to act

Zones and transitions

Chapters 3 and 4 in particular deal with a large number of technical and organizational security measures.

Everything starts with the definition of the system under consideration (system under consideration) and a risk analysis. Then the tolerable risk and thus the desired safety level is determined. The security level describes the desired protection from random or widespread attacks up to targeted attacks by secret services or military.

Based on the result, the system is segmented into zones and conduits. This concept is again derived from the defense-in-depth approach. It provides for logical or physical grouping and segmentation of network devices. This can be based on various criteria, such as physical location, security requirements or functional task. The granularity of the segmentation can vary.



Segmented corporate network

The zones primarily represent areas with different security requirements. A transition stands for a connection between 2 zones. Communication across zones is by no means excluded, but zones must still be separated from each other by safety measures. In order to protect the automation network in the best possible way, it is advisable to restrict cross-zone network traffic as much as possible.

In particular, the following basic principles should be taken into account:

- Separation of OT and IT
- Separation of systems with a safety risk for humans and the environment (safety related assets)
- Separation of temporarily integrated systems, such as laptops
- Separation of WiFi
- Separation of devices that are connected via external networks, e.g., remote maintenance work, business partners, etc.

The segmentation in the model of zones and transitions, as well as the documentation that is also required, can already significantly increase the safety level. This is followed by a detailed safety assessment and the definition of measures at component level. Whereby it is possible that not only technical measures are implemented, but that countermeasures can also be taken by compensatory organizational measures.

This results in technical and organizational measures based on seven different Foundational Requirements (FR). The Foundational Requirements are each specified by System Requirements (SR, 62443-3-3), and Component Requirements (CR, 62443-4-2) and supplemented by Requirement Enhancements (RE) depending on the desired security level.

The essential basic assumption here is that the protection of a machine or plant cannot be carried out by a single actor alone, but that all those involved must work together. Therefore the three essential roles of manufacturers, integrators and operators are addressed.

Basic requirements

In seven different basic requirements, the standard requires extensive measures for the system and component level.

	Abbreviation	Title
FR1	IAC	Identification and authentication control
FR2	UC	Use control
FR3	SI	System integrity
FR4	DC	Data confidentially
FR5	RDF	Restricted data flow
FR6	TRE	Timely response to events
FR7	RA	Resource availability

The aim is complete control of all processes, access and changes to the control system (Industrial Control System, ICS), not only during normal operation but also in exceptional situations. Of course, the risk management also considers the probability and determines the acceptable risk.

How Barracuda can contribute to compliance

Industrial network security

Micro-segmentation allows you to achieve a safety level where, in case of doubt, each plant or machine is isolated individually. The starting point is the clean separation between IT and OT. However, according to the concept of zones and transitions, segmentation must also continue within production. Each plant is isolated individually with an industrial firewall, or groups are formed based on security requirements or location.

Only through consistent sealing off can potentially vulnerable environments be protected from attacks and malware. Application and protocol detection ensures that only legitimate network traffic can get through to the system. The detection of industrial protocols can even be limited to individual commands or sub-protocols. In addition to these mechanisms, antivirus, Intrusion Prevention System and Advanced Threat Protection ensure reliable detection of intruders. Firewall rules with authentication ensure that network accesses are linked to corresponding authorizations and all activities are logged in a traceable manner. This protects the system and establishes an effective defense-in-depth concept to prevent outages. Even if malware or an attacker can penetrate the OT area, for example via USB thumb drives or laptops, the spread within the infrastructure is effectively contained.

The special feature of the Barracuda implementation is the transparent commissioning of industrial firewalls. This allows machines and plants to be sealed off without having to convert the existing networks. IP address changes, which are often associated with failures or cause technical difficulties at the plant, can thus be avoided. Firewalls for micro segmentation in the OT can be implemented without disruption of operations and can even be integrated into the switch network via the RSTP protocol. Nevertheless, each network access must overcome up to 14 security levels of the Barracuda CloudGen Firewall.

Barracuda rugged firewalls are used in harsher environments with special requirements regarding vibrations, dust, or temperature. For all other applications without special hardware requirements, for example in the medical environment, you can choose from the complete Barracuda CloudGen Firewall range.

Remote access management

The networking of machines and systems also offers great advantages for maintenance work. Many things can be analyzed or even repaired remotely. Without control mechanisms, however, there is an unmanageable proliferation of maintenance accesses.

The dynamic firewall rules on the Barracuda CloudGen Firewall allow secure maintenance accesses to be predefined. The release is time-controlled by an operations technician via mobile apps or by integrating the firewall API into another application. This ensures that accesses can be activated as required on site in production and can also be closed again after work has been completed. Several factors can of course be used for authentication.

Logging and visualization

Especially OT environments with a large number of firewalls for micro-segmentation and a unique set of rules each can quickly become confusing. Barracuda Firewall Insights is an advanced security analytics platform that automatically collects, aggregates and analyzes data from any CloudGen Firewall deployed on your corporate network. This allows you to analyze in one central location. A choice of hundreds of pre-defined analysis options helps visualize and detect problems and anomalies.

Threat management

In combination with the SCADAfence security platform, an even higher level of security can be achieved. SCADAfence is a threat management solution with automated incident response. By analyzing network traffic at firewalls and switches, anomalies and malicious processes can be detected. Through integration with Barracuda CloudGen Firewall, network rules are created and malicious access is blocked in real-time and automatically.

SCADAfence also offers significant advantages in asset discovery and in establishing the baseline for legitimate network traffic by creating a firewall policy.

Central management and deployment

With Barracuda Firewall Control Center, even thousands of firewalls can be efficiently administered on one management platform. Whether configuration, updates or analysis, everything can be done with one application. A granular authorization concept allows different teams to administer the system in their own area of responsibility. Due to the flexible pool licensing, licenses are not bound to the hardware, which makes the rollout faster and more efficient, and the exchange of hardware can be carried out easily on site.

Conclusion

With IEC 62443, IT security has finally arrived at OT. Despite the abstractness and complexity caused by the different viewing angles, it is clear that a significant security gain can be achieved by applying it in production environments and other OT networks. Concrete and realizable measures can be derived from the standard, which offer a very good structure for the implementation of technical and organizational security measures. Security is an ongoing process, which is constantly being developed and can only be achieved if all parties involved cooperate.

Disclaimer

Individual products such as Barracuda CloudGen Firewall can help implement standards. However, full compliance can only be achieved by an organization or company as a whole by implementing a large number of technical and organizational measures and their documentation. Furthermore, the level of security achieved also depends on the individual configuration of the solution.

Glossary

Abbreviation	Term
CR	Component requirement
DC	Data confidentiality
FR	Foundational requirements
IAC	Identification and authentication control
ICS	Industrial control system
RA	Resource availability
RDF	Restricted data flow
RE	Requirement enhancements
SC	System under consideration
SI	System integrity
SL	Security level
SR	System requirement
TRE	Timely response to events
UC	Use control

Barracuda
Your journey, secured.