

Cybersecurity in Renewable Energy Plants

How to implement intrusion detection in accordance with NIS2



ENSURE NIS2
COMPLIANCE IN
YOUR OT



DETECT VULNERABILITIES
AND CYBER INCIDENTS
IN YOUR OT



BRIDGE
THE SKILLS GAP IN
OT SECURITY

Executive Summary

Renewable energies are increasingly becoming the decisive backbone of electricity supply. In 2022 the EU-27 states had generated nearly 40 % of the EU-wide energy mix through renewable energy resources¹. It is not only large-scale photovoltaic (PV) and wind plants that play an important role in supplying energy and stabilizing the electricity grid. Smaller PV systems installed privately or on leased roofs have long been combined by aggregators to form larger virtual power plants by means of energy storage fleets.

As a result of this and the digitalization of the energy industry, renewable energy plants (REP) are becoming strongly networked distributed energy resources (DER) with a high degree of automation and remote control. This in turn increases the risk of disruption to the European and national energy supply due to cyber attacks. After all, every single DER represents a vulnerable point of attack. And centralized control centers can become a springboard for adversaries to infiltrate thousands of facilities. There is not only the risk of data leaks and manipulation of consumption data, but also a risk of local and regional blackouts with losses and fines amounting to millions. In the worst case, facilities can be irreparably damaged and human lives endangered.

For this reason, special legal requirements for cyber security apply to players in the European energy supply. The NIS2 Directive and the corresponding national implementing laws significantly expand the requirements for actors in the energy sector and make the management board personally liable.

All large REP operators, aggregators, energy storage operators and electricity suppliers are listed as sectors with high criticality² and at least as »important entities«. Many of these fall under the category of »essential entities« for which stricter requirements apply. Even if the specific requirements are only defined in the respective national implementation laws, all companies affected by NIS2 must implement measures that enable them to deal with security incidents. In addition to preventing incidents, it should also be possible to detect (occurring) security incidents.³

This eBook outlines the different challenges investors, management and operators face with regard to REPs' and DERs' cybersecurity. The document provides a detailed overview of evidence-based cyber risks that exist and, based on this, formulates clear recommendations for ensuring sustainable, efficient cybersecurity measures in renewable energy plants.

Terminological conventions

For critical infrastructures and entities, the term »essential entities« introduced with NIS2 is used.

For industrial IT (industrial control system, control and remote control system, process control technology), the established term operational technology (OT) is used.

Renewable energy plants are abbreviated as REP.

Disclaimer

This eBook does not constitute legal advice regarding applicable cybersecurity laws and regulations in the EU.

¹ <https://de.statista.com/statistik/daten/studie/182159/umfrage/struktur-der-bruttostromerzeugung-in-der-eu-27>

² EU NIS2 Directive, Annex I, 2022

³ ibid., Art. 6 No. 8

Content list

OT security is important for all stakeholders	3
Risk landscape of REPs	4
Attack Vectors in REPs	8
Legal requirements for REPs	10
Intrusion detection in REPs	12
3 Steps for cybersecurity of renewable energy plants	17

OT security is important for all stakeholders

Like no other sector, the energy supply is characterized by a multitude of stakeholders that permeate throughout society. Energy supply systems are the lifeline of our modern society. In short, there are around 746 million private and commercial stakeholders existing in Europe alone. In addition, there are government institutions as well as investors and operators of renewable energy plants (REPs). For all stakeholders, OT cybersecurity represents an investment in the best possible return on investment (ROI) (Table 1).

Despite increasing incidents in which critical assets have been attacked, investing in cybersecurity is often viewed critically.⁴ Cybersecurity does not create value, it preserves value. The return on investment is therefore not directly measurable. The appropriate indicator of the effectiveness of cybersecurity measures is the value of loss prevented. However, this is equally difficult to calculate, as the loss can only be precisely quantified once it has occurred. Therefore, benchmark values are helpful.

For example, a large-scale study found that companies with a solid, holistic cybersecurity approach were able to reduce the costs and losses caused by cyber incidents by 26% annually.⁵ In a previous study, companies with strong cybersecurity reported that they were

able to detect 83% of all security incidents and limit the impact of nearly half of the incidents to less than 24 hours. In comparison, companies with poorer security posture were only able to detect 54%. The share of incidents that impacted operations for more than 24 hours rose sharply to 97%.⁶

The partly negatively perceived impact of cybersecurity investments on the ROI of REPs is therefore an over-simplified calculation if only the expenditure on the measures is considered. As part of risk management, the possible losses that would occur in the event of damage throughout the year should be taken into account. There are now sufficient comparative values from well-documented incidents, such as the WannaCry ransomware, the supply chain compromise at SolarWinds or the attack on the Ukrainian energy supplier Ukrenergo in 2015 and 2016. In all cases, the companies affected faced additional costs in the multi-digit million range.^{7,8} In addition, there are possible fines for non-compliance with cybersecurity laws.

The cybersecurity of renewable energy plants – and in particular the security of the operational technology networks (OT) – is therefore crucial in protecting the return on investment, plant availability and grid stability.













		STAKEHOLDER	OBJECTIVE	RELEVANCE OF OT SECURITY
		State	Internal security, social peace and stability	Defense against hostile state actors, prevention of large-scale blackouts
		Private end users	Peace of mind	Disturbance-free everyday life and feeling of security
		Commercial end users	Successful business	Ensuring security of supply for business operations
		Private and commercial prosumers	Profitability of own REPs	Availability of own REPs
		Investors	Fast, positive ROI	Protection of the investment against failure, damage and fines
		Plant operators, aggregators	Avoiding additional costs	Availability of REPs, integrity of plant data, protection against financial and custodial fines
		Network operator	Grid stability, security of supply	Avoiding large-scale blackouts

Table 1 OT security protects the interests of all stakeholders

⁴ Accenture »Building Greater Cyber Resilience in Renewables«, 2020

⁵ Accenture »State of Cybersecurity Resilience 2023«, 2023

⁶ Third Annual State of Cyber Resilience, 2020

⁷ <https://www.cybertalk.org/5-years-after-the-first-wannacry-attack> accessed 09.17.2024

⁸ <https://heimdalsecurity.com/blog/solarwinds-attack-cost-impacted-companies-an-average-of-12-million> accessed 09.17.2024

Risk landscape of REPs

The risk landscape of renewable energy plants (REPs) is as diverse as their stakeholder groups. It ranges from geographical to technological to geopolitical aspects. Some of the risks cannot be resolved.

They remain as a residual risk and can only be brought under control by monitoring them.

Geographical risk

REPs especially on a large scale, are operated in locations that are sometimes far away from any civilization. However, even private plants in residential areas that are run as virtual power plants are not accessible to operators at all times due to private property boundaries. This makes it impossible to provide watertight physical or cyber security for the REPs. Attackers have all the time in the world to scout out a REP, break into it, and manipulate or damage

equipment. Finally, a large part of the digital control equipment is located on or in the REPs. Intruders in a wind turbine have access to the local programmable logic controllers (PLCs) and programmable automation controllers (PACs) for energy production, meteorological data acquisition and machine control.⁹ At photovoltaic parks, one can access the inverters, local control units and network cables.



So far and yet so close Offshore wind power is hard to reach, but not unattainable.

Architectural risk

Complexity and simplification

REPs are often combined with existing central energy plants and legacy IT/OT systems, which usually provide little or no cybersecurity measures. This historically grown system complexity theoretically requires strict segmentation in order to best isolate the insecure systems. However, local OT networks in REPs are often designed to be relatively flat in order to reduce complexity and enable a more stable communications infrastructure.¹⁰ The flat hierarchy leads to low segmentation and thus increases the risk that adversaries can move more easily through the network (lateral and vertical movement).

Site conditions

In the case of field facilities, the individual circumstances also play a role in how secure the system is from unauthorized access. It is not always possible to accommodate SCADA systems and the OT in a locked station. In photovoltaic systems, it is not uncommon for network cables to be laid freely in the field, where attackers can potentially gain access unnoticed via network taps.¹¹

⁹ Utility Variable-Generation Integration Group, Wind Operating Practices Guidebook, chap. 2.6.2, 2.6.3.

¹⁰ David Ferlemann, »Wind Farm Security Analysis and Attack Mitigation,« (Ph.D. Dissertation., University of Tulsa, 2017), 1–56.

¹¹ ByWa r.e., H. Timm Elektronik, »Cyber Security in the Wind Industry«, 2021

Internet connections

Furthermore, the interface between the REP and the operator's central control room becomes a risk if communication is not carried out via a dedicated cable connection and instead via the Internet. There are still millions of industrial edge devices in remote locations that can be reached via the Internet using the Shodan and Censys Internet platforms. Last but not least, private REPs on residential homes offer an interface through which not only the owners but also attackers can access the system control. This means that attackers can sometimes penetrate the systems regardless of their location.

The Fraunhofer Institute stated in 2021: »This technological complexity, internet-based connectivity and heterogeneous infrastructure landscape create vulnerabilities for malfunctions and incorrect operation by employees, thereby increasing the potential attack surfaces for attackers, and on the other hand make it more difficult to implement security standards such as ISO/IEC 27001 and IEC 62443.«¹²



The OT of remote facilities is typically exposed.

Technological risk

Insecure devices

A large proportion of the currently available and installed OT components such as switches, PLCs, inverters, etc. are still »insecure by design.« One reason is to reduce upfront costs of building REPs. But there is another, more general reason: The focus of industrial digitalization was and is on increasing availability and operational stability. Access to systems and communication between systems are there-

fore often characterized by openness. This is also repeatedly demonstrated by the results of Rhebo Industrial Security Assessments, in which a detailed vulnerability analysis of the OT infrastructure is carried out. On average, Rhebo experts identify 19 security risks and 7 availability risks in each OT network (Figure 1).¹³

¹² Fraunhofer Academy, »Current challenges for cybersecurity in the energy supply«, 2021

¹³ Rhebo, »OT Risks – Insights from Vulnerability Assessments 2023«, (last accessed, 10.02.2024)

TOP 10 SECURITY RISKS IN OT NETWORKS 2023

Results from Rhebo Industrial Security Assessments in 2023

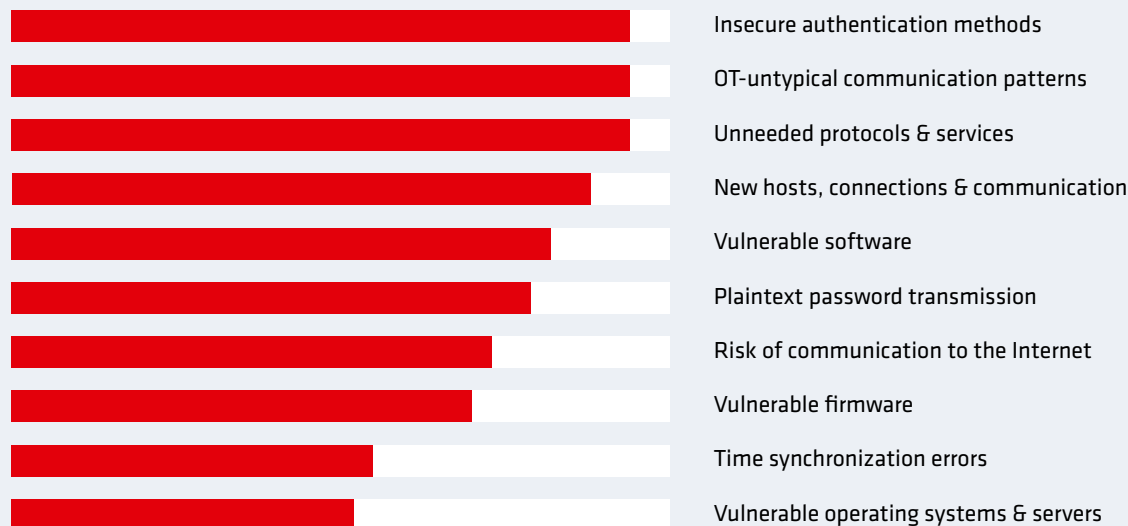


Figure 1 There is no OT without security risks and vulnerabilities as results of the Rhebo Industrial Security Assessments show.

Insecure protocols

The majority of industrial communication protocols do not use authentication or encryption technology. Even in modern systems that follow the IEC 61850 or IEEE 1547-2018 standard, these security gaps remain. Both standards completely ignore protocol security. The international standard IEEE 1547.3 'IEEE Guide for cybersecurity of distributed energy resources interconnected with electric power systems,' published in 2023, even argues that these standards increase cyber risks ¹⁴ see chapter 3. Industry standards such as IEC 62351-4 and IEC 62351-6 define security mechanisms for the MMS, GOOSE

and SV protocols. In practice, however, the additional safeguards are usually not implemented because they require a higher level of administration and a higher runtime memory. The latter conflicts with the requirements for real-time communication in energy infrastructures.¹⁴ Of course, the inherent insecurity of OT components and protocols can only be truly exploited once attackers are in the network. However, they greatly facilitate horizontal and vertical movement within the network as well as the exploitation of the individual systems.



Insecure protocols also pose a risk in hydroelectric power plants.

¹⁴ Rhebo, »360° Cybersecurity in IEC 61850 Infrastructures«, 2023

Insecure security systems

Even devices used to secure the network perimeter of a REP can become a source of insecurity: firewalls. The most prominent example comes from Denmark. In May 2023, a zero-day vulnerability was discovered on a firewall made by Zyxel. Within a few days, 23 Danish energy companies fell victim to orchestrated attacks that specifically exploited this vulnerability. Some energy supply companies had to isolate their OT and switch to manual operation of the plants.¹⁵

AI systems

Applications using artificial intelligence (AI) are also increasing in the energy industry. More than 220 companies with AI products are already active in the energy sector.¹⁶ In a global survey, 74% of energy companies said they were already using AI or were planning to do so.¹⁷ Due to the dependence of AI models on a continuous data stream, AI systems can be exploited for both data theft and data manipulation. The latter can lead to an AI-driven system making erroneous decisions that affect both the REP and grid stability.¹⁸

Supply chain risk

The supply chain is the weakest link in a company's cybersecurity across all sectors. That's because few companies have a significant influence on the cybersecurity of their suppliers.

As the SolarWinds case in 2020 shows, this can have devastating consequences. The network of the IT service-provider had already been compromised in March 2020. The target was SolarWinds' core product, the network management platform Orion. At that time, the platform was used by around 15,000 companies. The attackers

succeeded in implanting malware in an update. This update gave the attackers access to all SolarWinds customers, including government agencies, some US IT security companies, and Microsoft.¹⁹

Such a supply chain compromise can also be easily achieved via a maintenance laptop or a USB drive that is connected to a system by external service personnel, e.g. during maintenance or servicing work. The very first known case of OT malware, Stuxnet in 2010, found its way into the highly secured infrastructure that way.

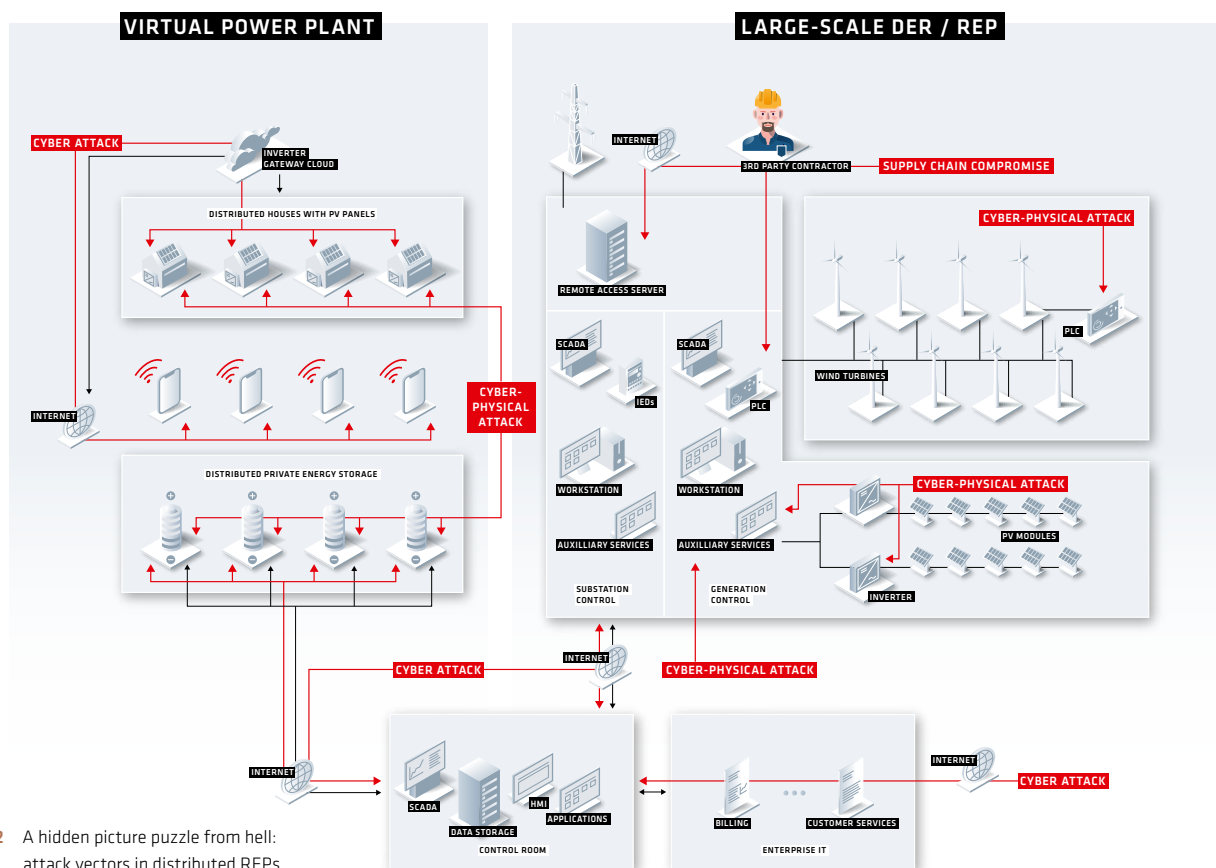


Figure 2 A hidden picture puzzle from hell: attack vectors in distributed REPs.

¹⁵ SektorCERT, »Report: The attack against Danish critical infrastructure«, November 2023

¹⁶ Vladimir Frank et al., »A Comprehensive Review of Artificial Intelligence (AI) Companies in the Power Sector«, Energies 2023, 16(3), 1077

¹⁷ IBM, »New IBM Study Data Reveals 74% of Energy & Utility Companies Surveyed Embracing AI,« 2024

¹⁸ Emily Newton, »The Dual Impact of AI on Power Grids: Efficiency and Vulnerability«, Revolutionized Magazine, 2024

¹⁹ Heise, »Cyber-Attack via SolarWinds«, (last accessed: 02.10.2024)



Most people see an installer. Others see a possible supply chain compromise or adversary in disguise.

Stakeholder risk

As already explained in Chapter 1, REPs have a multitude of different stakeholders. In some cases, they also have access to the plants. Stakeholders have direct and indirect influence on the cybersecurity of their REPs. The indirect risk arises from the decision to invest less in cybersecurity because doing so would (supposedly) reduce return on investment and company profits. The direct risk arises from a certain degree of convenience. Because the day-to-day operation of EEAs becomes easier the fewer restrictions there are, established

security mechanisms and cyber hygiene rules are sometimes circumvented or disregarded. As in any working environment, informal workarounds become ingrained, or work is carried out on the basis of trust (especially with service companies). Furthermore, the number of cybersecurity experts specifically for REPs remains limited. The shortage of skilled labour in this area – among REP operators, grid operators and manufacturers – is the biggest challenge when it comes to implementing OT security in REPs.²⁰

Geopolitical risk

Last but not least, the geopolitical situation is becoming an increasing risk for REPs. For example, the energy transition has made renewable energies the most important energy source in Germany. Accordingly, REPs become potential targets for hybrid warfare. As recently as February 2024, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) warned of activities by the Chinese Advanced Persistent Threat (APT) Volt Typhoon, which has been infiltrating and strategically

positioning itself in critical infrastructure networks for some time.²¹ This so-called strategic prepositioning follows a long-term objective that is less focused on a short-term disruption or ransom money demand. Rather, it is about being able to act immediately in the event of a future conflict, i.e.: To deliberately disrupt the infrastructure. With this in mind, Volt Typhoon places sleeper cells at neuralgic points in the enemy's infrastructure, just waiting for the wake-up call.

Attack Vectors in REPs

REPs provide attackers with a variety of intervention options that allow them to provoke local disruptions to the energy supply, as a 2021 study by the National Renewable Energy Laboratory and Underwriters Laboratories highlights.²² Accordingly, adversaries can:

- change the frequency settings of the grid-interactive inverters,
- change the settings for voltage trip settings of grid-interactive inverters,
- disable the underfrequency load-shedding,
- assume control of the inverter²³,
- assume control of the plant and
- manipulate monitoring data.

Typical attacks on REPs include:²⁴

- **Eavesdropping:** spying on and intercepting communications
- **Masquerading:** access via legitimate user accounts using stolen credentials
- **Man-in-the-middle:** introduction of an additional gateway to send manipulated communication in both directions (actuator, control room)
- **Resource depletion or denial-of-service**
- **Replay:** copying a command and reusing it at a later time to cause disruptions
- **Trojan horse (or supply chain compromise)**
- **Wireless:** circumventing physical security systems via WiFi-enabled components

²⁰ IEEE, »IEEE 1547.3 – IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems,« 2023

²¹ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> (last accessed 10.07.2024)

²² NREL, »Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources,« 2021

²³ Johnson, Jay, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Mathew J. Reno. 2019. »Power System Effects and Mitigation Recommendations for DER Cyberattacks.« IET Cyber-Physical Systems: Theory & Applications. <https://doi.org/10.1049/iet-cps.2018.5014>

²⁴ IEEE, »IEEE 1547.3 – IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems,« 2023, p. 35

Attack vectors and disturbances in photovoltaic systems

In PV systems, the focus is primarily on the inverters as well as the monitoring and control systems. Inverters are often operated with standard passwords, rarely have physical intrusion detection and, due to their long life cycles, sometimes use vulnerable chips.²⁵ Proof-of-concepts have already shown in the past that reference values can be changed via external access in such a way that an inverter absorbs reactive power and thus leads to an energy loss. It is also possible to overcharge batteries.²⁶ Sensor data in monitoring and control systems can be manipulated, among other things, to change the voltage.²⁷ Furthermore, Internet access for data transmission in connection with weak patch management creates a major attack vector.

The targets of the attackers will vary with the size of the power provided by the REP. Prepositioning and direct disruptions to grid stability and supply will only have an effect in large-scale plants and larger networks. Even in the case of aggregated virtual power plants, micro-plants will be of less interest to state-sponsored adversaries. Though, criminals could find an optimal base for a bot network such as Mirai in the thousands of gateways. However, the size of a single system might not be necessarily decisive, especially if the feed-in control is operated via a third-party platform that coordinates millions of such small systems and therefore easily scales from megawatt to gigawatt.²⁸

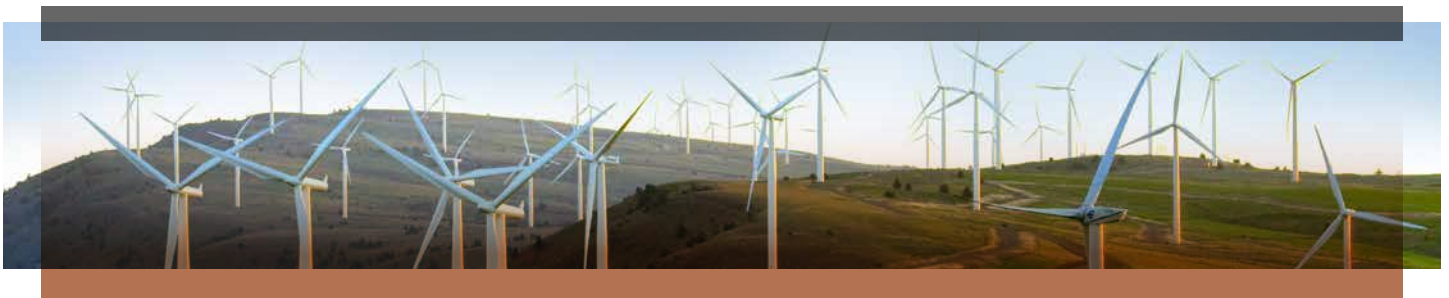


The control technology in PV systems is digital and easily accessible.

Attack vectors and errors in wind turbines

In many wind farms, the OT is characterized by being less segmented and strongly networked. Other vulnerabilities are the often weak authorization on OT devices²⁹ and the lack of encryption of VPN connections. Service and supplier companies often have unrestricted access via VPN to monitor plants, update system software and carry out maintenance work.³⁰ This offers attackers a large attack surface and simplifies lateral movement within the OT of wind farms. Access can

also be achieved via fiber optic connections and Ethernet switches. Due to the remote locations of wind farms, attackers have a good chance of causing damage before an intrusion is noticed or can be investigated. The OPC XML-DA protocol, which is widely used, can be exploited to send false data on operating states and disrupt operations to the point of damaging the plant.³¹



Windparks are quite easily accessible for everyone.

²⁵ Hill, Mark D., John Masters, Parthasarathy Ranganathan, Paul Turner, and John L. Hennessy. 2019. »On the Spectre and Meltdown Process Security Vulnerabilities.« IEEE Micro 39 (2): 9–19. <https://ieeexplore.ieee.org/abstract/document/8634886>

²⁶ Bellini, Emiliano. 2020. »Solar Inverters vs. Cyber Attacks.« PV Magazine, August 17, 2020. <https://www.pv-magazine.com/2020/04/17/solar-inverters-vs-cyberattacks>

²⁷ Watts, Raymond, Brian Kline, and Tom Ridge. 2018. Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors: A Risk Assessment Study of Solar Inverter Technology. <https://www.bitdefender.com/en-us/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states>

²⁸ U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE). 2020. Roadmap for Wind Cybersecurity. Washington, D.C.

³⁰ Staggs, Jason, David Ferlemann, and Fugeet Sheno. 2017. »Wind Farm Security: Attack Surface, Targets, Scenarios, and Mitigation.« International Journal of Critical Infrastructure Protection 17: 3–14

³¹ ibid.

Legal requirements for REPs

In addition to the very specific risks to cybersecurity and the operation of renewable energy plants (REPs), plant operators and owners are now facing another challenge: To implement cybersecurity in their facilities in a legally compliant manner.

- The most important legal documents in Europe for REPs are currently:
- EU NIS2 Directive
 - EU Cyber Resilience Act (CRA)

The legislation often refers to a so-called state of the art. Table 2 lists a selection of national and international cybersecurity standards that apply for REPs.

INTERNATIONAL STANDARDS	ISO 27001 organizational	Requirements for the structure and operation of an information security management system (ISMS)
	IEC 62443 organizational, technical	Basic standard for cybersecurity in industrial infrastructures
	IEC 62351 technical	Security in energy management systems and associated data exchange (protocol security, access control, deep packet inspection, security logging)
	IEEE 1547.3 technical	Guidelines for cybersecurity of distributed energy resources and their connection to electrical energy systems → Currently the latest standard for REP cybersecurity with the aim of strengthening the resilience of cyber-physical systems
	NIST SP 1800-32 organizational	US industry standard for cybersecurity of distributed energy resources as an example of IIoT security
	NIST SP 800-82 Rev.3 organizational	American industry standard for cybersecurity in OT networks

Table 2 Selection of the most important standards for REPs

Critical entity? Yes or no?

The short answer is: This is regulated by the national transposition laws for NIS2. Annex I of the NIS2 Directive defines energy producers, electricity companies and aggregation, demand response and energy storage service providers as high criticality sectors. However,

this is only intended as guidance for national legislation. Operators and owners of REPs should consult the respective national legislation to which extend their plants fall under NIS2.

National NIS2 regulations

The EU NIS2 Directive significantly increases the number of companies for which cybersecurity becomes a legal requirement. Current estimates assume that several hundred thousand companies in the EU will have to comply with the legal requirements in future.

In principle, the NIS2 requirements for cybersecurity risk management pursuant to Art. 1 (2b) apply to all companies in the energy sector, as they:

- are among the sectors with high criticality according to Annex I.
- are often also classified as »essential entities« in accordance with EU 2022/2557 and national regulations.
- are considered regardless of company size and turnover, in accordance with Art. 2 (2c-e).

Many EU countries have long had cybersecurity laws in place, which were implemented on the basis of the first NIS Directive from 2016. NIS2 primarily changes the scope of obligations for players in the energy industry. In addition to the critical facility and its OT, the entire company must now be cyber-secure and include the supply chain. The specific requirements can be found in the respective national transposition laws. However, one thing is clear: In accordance with Article 6 No. 8, »management of cybersecurity incidents« should not be limited to prevention (usually via firewalls and access management at the network perimeter). The detection, analysis and con-

tainment of cybersecurity incidents – i.e. already successful breaches within the networks – must also be implemented. This means – without explicitly stating it – that a multi-level intrusion detection system is mandatory for all companies.

»Even though the NIS2 does not explicitly mention intrusion detection systems, all requirements boil down to exactly that.«

Furthermore, for the first time, the managing board is held personally liable for implementation and compliance.

NIS2 REQUIREMENTS IN OT Challenges and limitations

Download whitepaper



Cyber Resilience Act

The EU Cyber Resilience Act (CRA) is primarily aimed at all manufacturing companies that want to sell components with digital interfaces or applications on the European market. The requirements for integrated cybersecurity (»secure by design«) will become a mandatory aspect for obtaining the CE label and, therefore, a prerequisite for access to the European market.

This also means that manufacturers of PLC components and energy storage systems are obliged to comply. The German company Sonnen GmbH has been actively assuming this responsibility since 2019. As the operator of a virtual power plant in which over 25,000 private households provide around 250 MW of capacity with their Sonnen energy storage systems, Sonnen acts not only as a manufacturer of critical components but also as an aggregator on the energy market. Sonnen has therefore been operating a software-based OT monitoring with intrusion detection from Rhebo on all of its energy storage systems since 2019.

In order to give companies a clear roadmap, the various existing security standards are currently being harmonized. The IEC 62443 standard will most likely play a role, with chapters 4-1 »Secure product development lifecycle requirements« and 4-2 »Technical security requirements for IACS components« explicitly defining cyber security requirements for OT components.

IIOT SECURITY Intrusion detection on Sonnen energy storage systems

Download success story



Intrusion detection in REPs

The standards in Chapter 3 define a multitude of technical measures, but quickly cause affected companies to lose sight of the bigger picture. A collection of tools does not make a REP secure. They must work together to ensure the sustainable cybersecurity and cyber resilience of the REPs.

Cybersecurity should therefore follow three premises:

1. Defense-in-Depth,
2. End-to-end cyber resilience,
3. Continuous improvement process.

Defense-in-Depth in REPs

There is no such thing as 100% cybersecurity. Cybersecurity remains a constant game of cat and mouse for attackers and defenders. A successful cyber attack is not a question of »if« but of »when«. This reality is fueled by two developments:

1. Due to the increasing networking and digitalization of infrastructures, the digital domain will become a lucrative criminal activity in the short term and strategically a decisive arena in state conflicts.
2. Artificial intelligence allows for the faster development of attack techniques.

As already illustrated in Chapter 2, there are always residual risks to cyber security at various levels. Although these cannot be directly repelled, they can be brought under control. The most effective option is to build cybersecurity as a multi-layered strategy from the outside in. This defence-in-depth concept, which is derived

»Defense-in-Depth involves combining multiple heterogeneous security technologies across common attack vectors to ensure that attacks missed by one technology are detected by another.«³³

from the military, aims to still be able to stop the attackers in the event of successful attacks, e.g. external access to the OT network or OT components in REPs. This is not possible with firewalls and a Security Information & Event Management System (SIEM) alone. Das internationale Institute of Electrical and Electronics Engineers (IEEE) warnt entsprechend: »Security for the smart power grid must incorporate a defense-in-depth strategy that layers security features, since any breach could allow attackers or even inadvertent mistakes and failures to cause major impacts on the safety of people and the reliability of the power grid.«³⁴ To use an analogy, a modern, highly in-

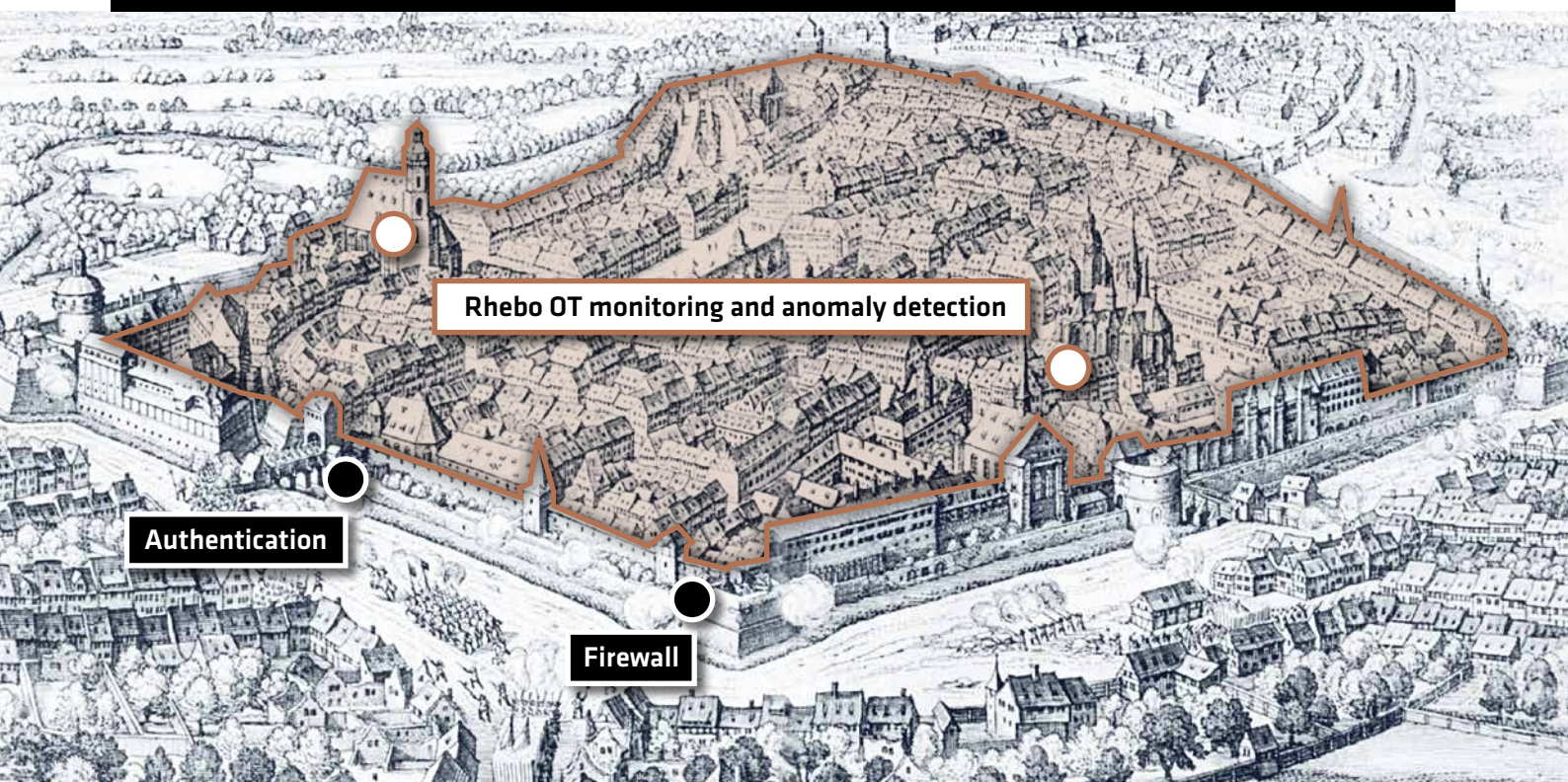


Figure 3 An OT network must be secured like a city state. Besides perimeter security this includes homeland security.

³³ e.g. NIST SP 800-171, NIST SP 800-172, NISTIR 8183

³⁴ IEEE, »IEEE 1547.3 – IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems«, 2023, p. 25

teractive network must be secured like a modern state or a city-state (Figure 3). The city wall, the gateways, and the defense systems (firewalls, data diodes, Authentication, physical access controls) secure the plant from the outside. The residents (employees, service providers) have the legislation as a benchmark (ISMS, compliance and security guidelines). The police and constitutional protection authorities (anomaly detection, network-based and edge device-based intrusion detection system) are responsible for internal security in the country. The external and internal threats are ultimately combined by the intelligence services to form an overall picture of the situation (SIEM). Attackers who manage to sneak into the city-state can be exposed and arrested more quickly. It also makes it more difficult for them to move laterally insight the country.

The incident as well as the latest developments and the remaining residual risk clearly speak in favour of the need for inner security in OT networks. Monitoring with integrated anomaly and intrusion

detection analyses OT communication for activities that deviate from the known, established pattern. This is possible in OT because industrial systems are characterized by repetitive, predictable communication. The activities of attackers are therefore relatively easy to distinguish from legitimate communication. As a result, the intrusion detection system can also detect attacks affecting OT that use new attack techniques, unknown vulnerabilities, stolen credentials, and supply chain compromises that use known attack techniques, without having alerted the firewalls and the SIEM system.

As part of the defense-in-depth approach, OT security monitoring forms the “second line of defense” in order to detect both internal perpetrators and successful attacks in the networks at an early stage, thereby strengthening the company’s ability to respond. Perimeter security, a global SIEM system and OT monitoring go hand in hand in the cyber security of REPs (Figure 4).

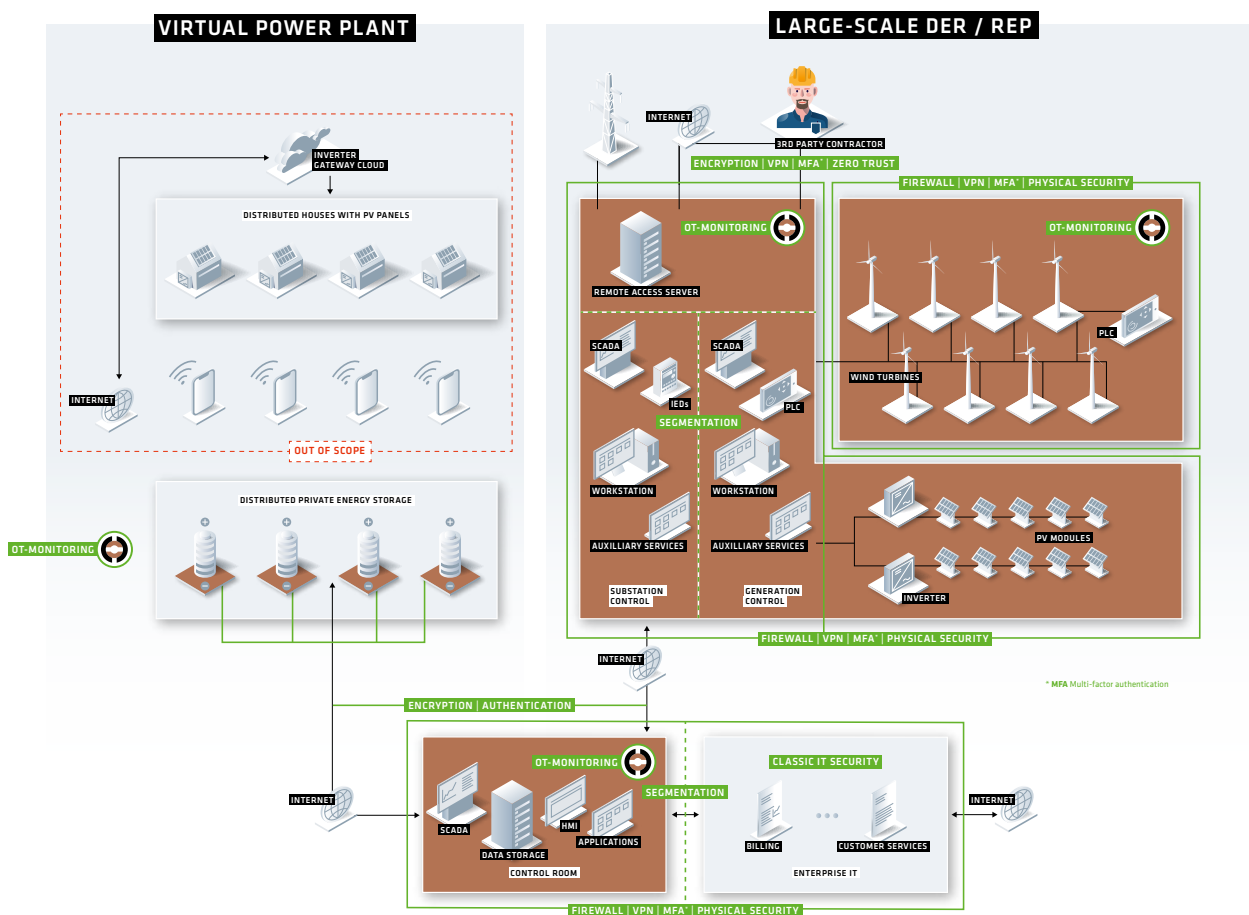
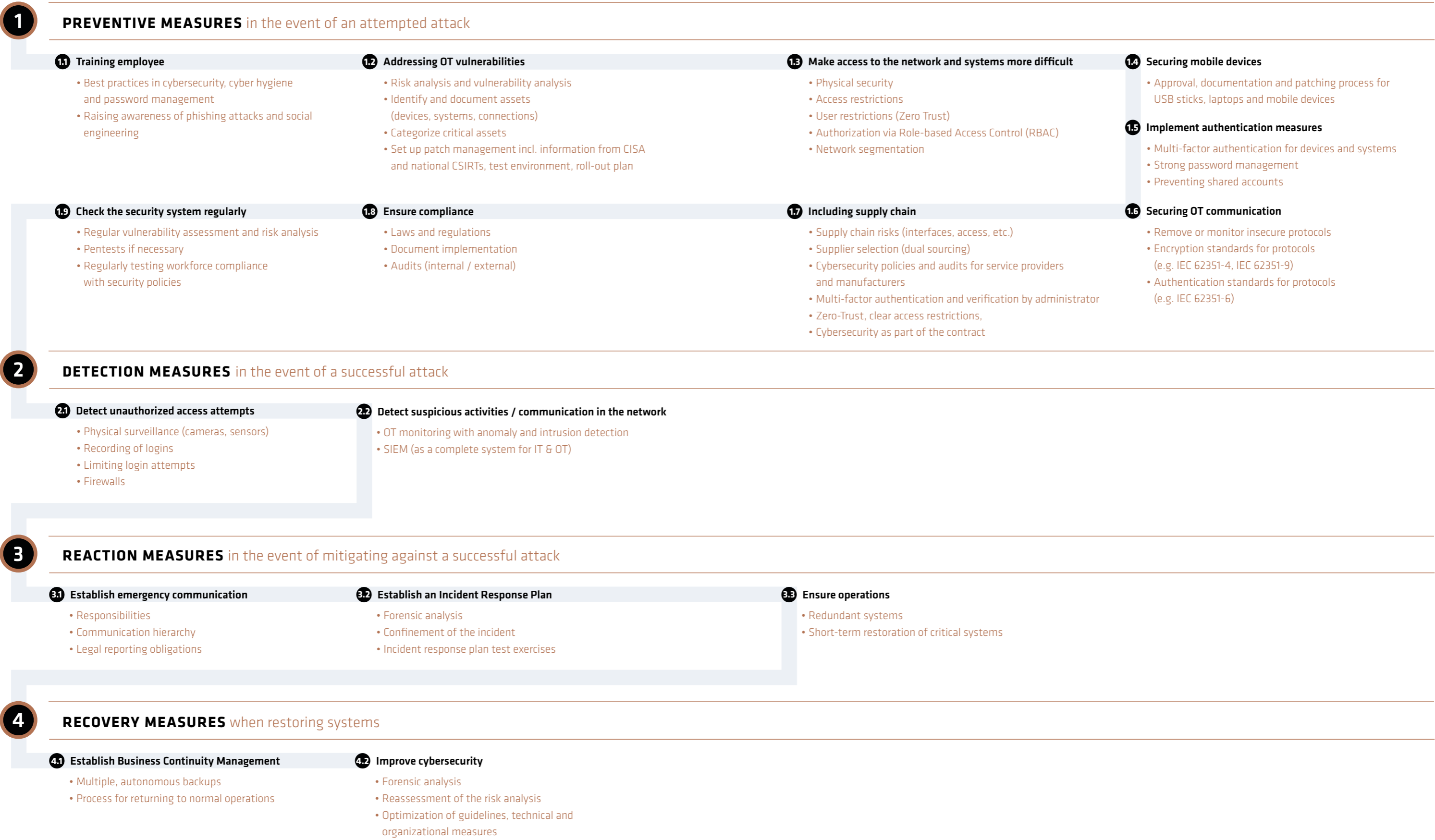


Figure 4 Exemplary defense-in-depth architectures in large REPs (right) and virtual power plants (left). In addition, all components (PLCs, inverters, energy storage systems, SCADA, IEDs, etc.) should be developed secure by design.

Cyber Resilience in REPs

Almost all standards, including NIS2, follow the escalation process during an attack, which is also inherent in defense-in-depth. Cyber resilience also includes the time after an attack has been repelled, which is about strengthening cybersecurity and restoring systems.

Taking all aspects of cyber resilience into account enables companies to remain capable of acting throughout the entire life cycle of a cyber attack:



Cybersecurity never stops

Cybersecurity is not an end state, but a constant uphill battle. Several years ago, the German Federal Office for Information Security (BSI) reported over 400,000 new malware signatures per day. AI is accelerating the expansion of hybrid warfare and cybercriminal groups and putting more and more pressure on cybersecurity.

Cyber security (posture) and the risk situation must therefore also be regularly reviewed in REPs and follow the continuous improvement process (Figure 5) that has been commonplace in quality management systems. Important steps are:

- Regularly obtain information about newly discovered and exploited vulnerabilities in OT components. For this purpose, we recommend the CISA ICS Security Alerts, which provide daily information about new reports and often make actionable recommendations.³⁵
- Repeated vulnerability assessments regularly analyze the OT for existing and new security gaps (e.g. with the Rhebo Industrial Security Assessment service).
- Analyze anomalies identified by OT monitoring.
If necessary, seek support from the providers' specialists to build up inhouse expertise of OT risks in the company (e.g. with the Rhebo Managed Protection service).

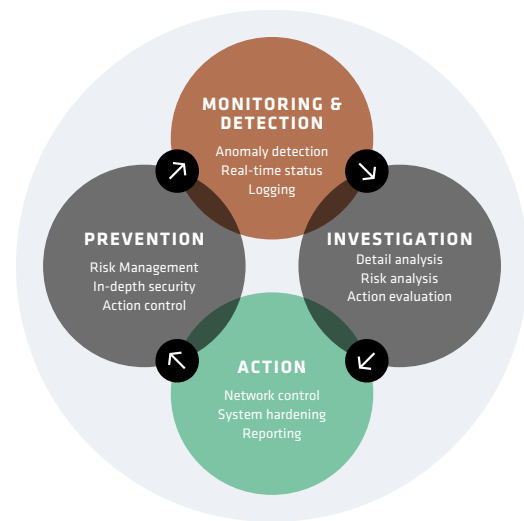
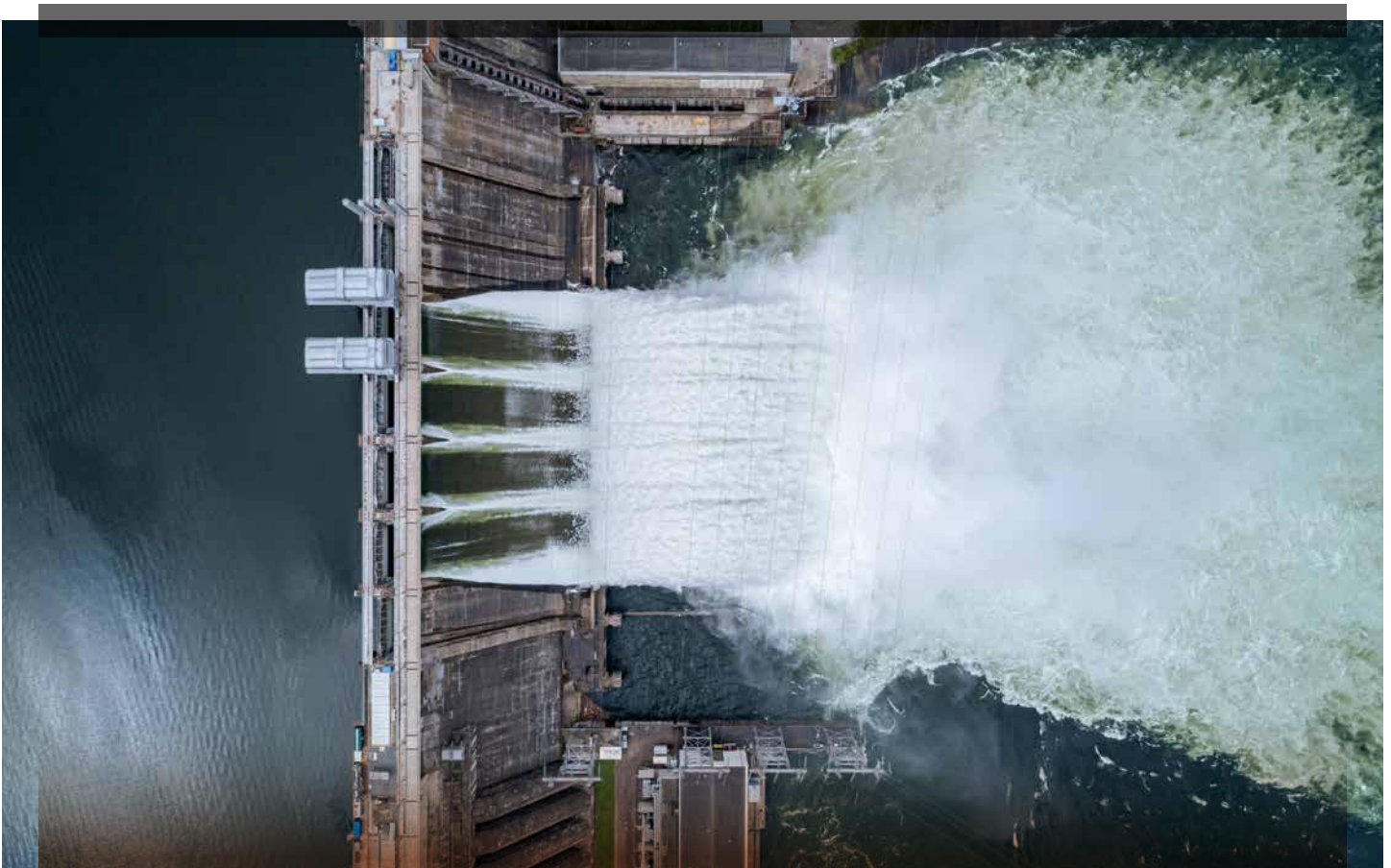


Figure 5 Cyber resilience and cyber security will only be successful if measures are regularly tested for their effectiveness and lessons are learned from incidents.



³⁵ <https://www.cisa.gov/resources-tools/resources>

3 Steps for cybersecurity of renewable energy plants

1



The first easy step
to OT security:

Rhebo Industrial Security Assessment

Cybersecurity starts with visibility.

The **Rhebo Industrial Security Assessment** is an OT cyberrisk and vulnerability analysis that provides a deep understanding of your ICS / OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2



The seamless transition
to comprehensive OT security:

Rhebo Industrial Protector

Cybersecurity does not end at the network perimeters.

The OT monitoring with next generation OT threat and intrusion detection **Rhebo Industrial Protector** provides enterprise-ready OT-dedicated security. It advances the existing perimeter firewall security by integrating holistic anomaly detection that does not interfere with the critical industrial processes. The solution is also available as an agent version for edge devices such as energy storage devices.

You profit from

- real-time visibility of communication behavior of all OT and ICS assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via backdoors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3



The recipe to peace of mind.
We monitor so you don't have to:

Rhebo Managed Protection

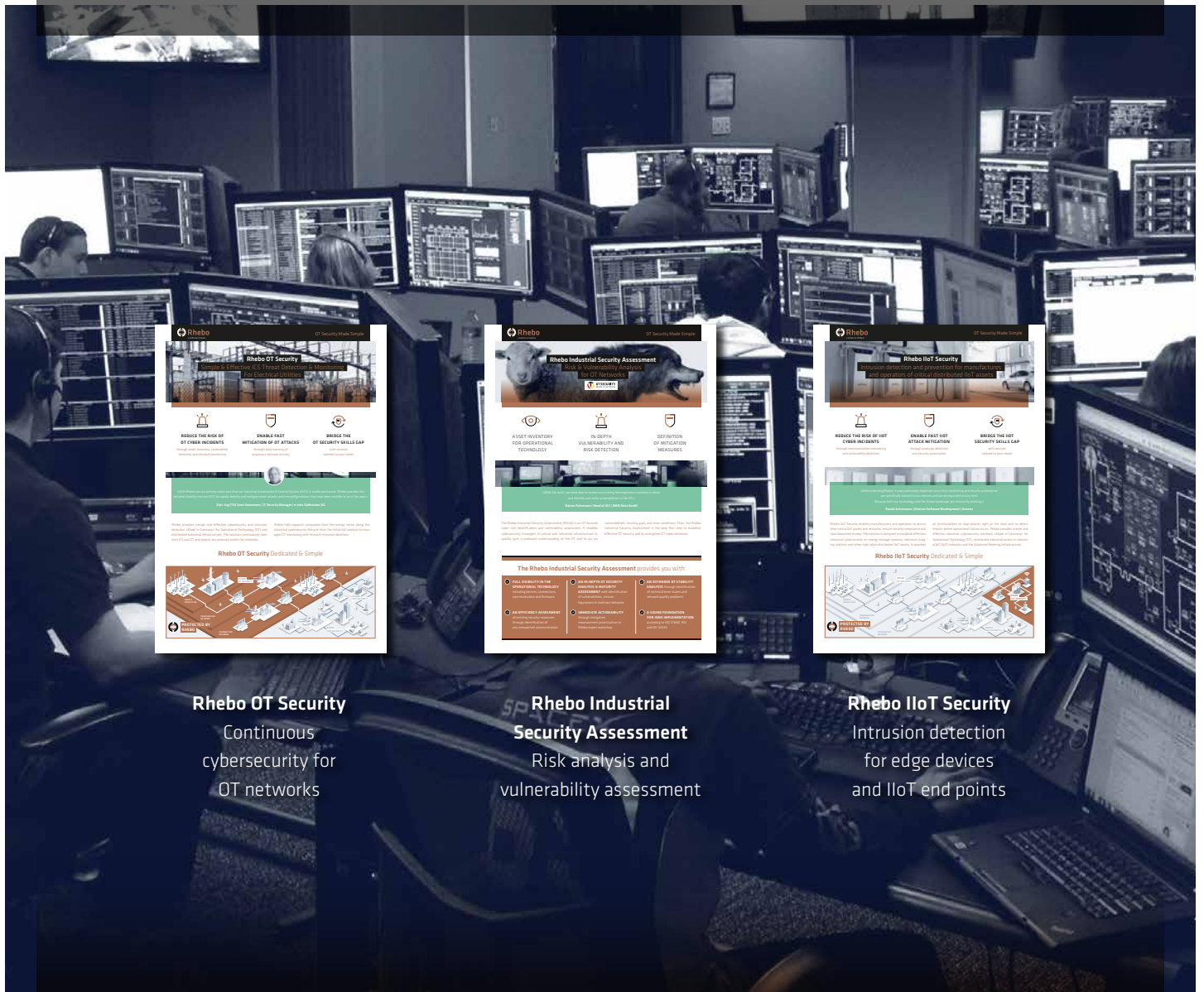
Cybersecurity needs resources and know-how.


With **Rhebo Managed Protection**, we support you in operating the OT security monitoring with anomaly detection, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

You profit from

- expert support for the operation of the OT security monitoring system;
- fast forensic analyses and assessment of OT anomalies;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and maturity assessments for continuous improvement.


Protect your renewable energy plants from cyberattacks and legal fines





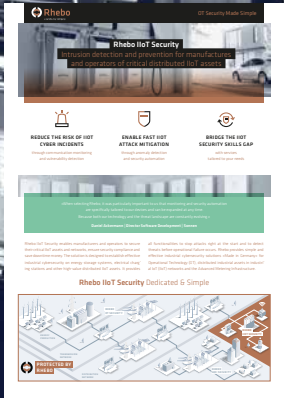
Rhebo OT Security
Continuous cybersecurity for electrical utilities

REDUCE THE RISK OF OT CYBER INCIDENTS
ENABLE FAST MITIGATION OF OT ATTACKS
BRIDGE THE OT SECURITY SKILLS GAP



Rhebo Industrial Security Assessment
Risk & vulnerability analysis for OT networks

ASSET INVENTORY FOR OPERATIONAL TECHNOLOGY
IN-DEPTH VULNERABILITY AND RISK DETECTION
DEFINITION OF MITIGATION MEASURES



Rhebo IIoT Security
Intrusion detection and prevention for manufacturing and operators of critical distributed IIoT assets

REDUCE THE RISK OF IIOT CYBER INCIDENTS
ENABLE FAST IIOT ATTACK MITIGATION
BRIDGE THE IIOT SECURITY SKILLS GAP

Rhebo OT Security
Continuous cybersecurity for OT networks

Rhebo Industrial Security Assessment
Risk analysis and vulnerability assessment

Rhebo IIoT Security
Intrusion detection for edge devices and IIoT end points

www.rhebo.com | sales@rhebo.com | +49 341 3937900



Initiated by ECSO, issued by eurolabs e.V.

Rhebo OT Security Made Simple

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The German company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG, a leading global provider of integrated

energy management solutions for the energy industry with around 7,500 employees in over 30 countries worldwide. As a trustworthy cybersecurity provider, Rhebo is ISO 27001 certified and was awarded the »Cybersecurity Made In Europe« label for its strict data protection and data security policies.

www.rhebo.com