SUNGROW
Clean power for all

BUREAU VERITAS

Cybersecurity Practices for Renewable Energy in Europe

Foreword

By Sonia Dunlop, CEO, Global Solar Council

September 2025

There is no doubt that the solar PV and battery storage industry stands at the forefront of the global energy transition. We are not just scaling up renewable energy—we are reshaping how power is generated, distributed, and secured. In this new era of decentralized, digitalized energy systems, **cybersecurity is no longer optional—it is foundational**.

Solar inverters, as the heart and brains of solar and battery storage systems, sit at the intersection of energy and IT. They play a critical role in grid stability, data communication, and of course, power conversion. But as their intelligence and connectivity increase, so too do their vulnerabilities. Cyber threats—ranging from malware to sophisticated grid attacks—pose real risks to solar's resilience, particularly as we integrate more and more solar into mission-critical infrastructure and national power grids.

This report arrives at a pivotal moment. By focusing specifically on cybersecurity in solar inverters, it shines a spotlight on a rapidly evolving challenge and provides actionable insights for manufacturers, developers, regulators, and grid operators alike. It underlines a vital truth: **resilience in the new energy age requires both electrons and protections**.

At the Global Solar Council, we believe that strengthening trust in solar technology is essential to unlocking investment, achieving just and inclusive energy transitions, and safeguarding energy independence. That is why we are supporting efforts to raise standards, share best practices, and embed cybersecurity into every stage of solar deployment—from design to decommissioning.

SUNGROW has taken proactive leadership in this space, and rightly so. Let this paper serve as both a call to action and a roadmap for industry-wide collaboration. Together, we must ensure that the systems powering a net-zero world are as cybersecure as they are sustainable.

Abbreviations

The abbreviations used in this document and their full forms are shown in the following table.

Tab. 1 Abbreviations

Abbreviation	Full Form
CRA	Cyber Resilience Act
DCS	Distributed Control System
DER	Distributed Energy Resource
DPI	Deep Packet Inspection
EMS	Energy Management System
EPC	Engineering, Procurement and Construction
ESG	Environmental, Social, and Governance
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MFA	Multi-Factor Authentication
NIS2	Network and Information Security Directive 2
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
PERA	Purdue Enterprise Reference Architecture

PII	Personally Identifiable Information
PLC	Programmable Logic Controller
PPC	Power Plant Controller
PSIRT	Product Security Incident Response Team
RBAC	Role-Based Access Control
RED	Radio Equipment Directive
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SSO	Single Sign-On

Contents

1 Introduction

A global renewable energy enterprise, SUNGROW specializes in the research, development, manufacturing, and operation of photovoltaic (PV) inverters and energy storage systems. Secure and sustainable innovation is central to this work, which is why **SUNGROW views cybersecurity not only as a technical function but as a strategic enabler of our solutions**. We fully support the industry viewpoint shared by stakeholders such as the Global Solar Council: cybersecurity is now essential for maintaining grid stability, operational reliability, and data integrity within the renewable energy sector.

Digitalization and connectivity are reshaping how renewable energy assets are designed, deployed, and operated. Advances in digital technologies are bringing residential distributed energy into everyday life, enabling real time monitoring, intelligent O&M, faster product iteration, easier maintenance, and flexible customization, as digitalization and connectivity enhance performance across the entire system. At the same time, greater interconnection widens the exposure surface, and grid-forming stability, distributed coordination, and renewable energy services intensify dependence on digital infrastructure and platforms. Cybersecurity thus provides the foundation for stable, trustworthy renewable energy systems.

What does cybersecurity for the renewable energy sector look like? It requires a holistic approach to protecting digital energy infrastructure and associated data. To do this, sector players must be guided by a comprehensive, integrated cybersecurity framework that encompasses every aspect from security management processes and privacy protection to data compliance and robust product security.

What does this holistic approach entail? This is the question our report seeks to answer, using SUNGROW's practice as a blueprint for building secure and reliable renewable energy infrastructure.

Our report explores **Europe's cybersecurity requirements for the renewable**

energy sector. Throughout the sections that follow, we'll share insights and learnings[1] about security management processes, privacy and data compliance measures, and the end-to-end security framework that's needed across the entire "device–network–platform" chain.

2 Background and Challenges

2.1 Cybersecurity Landscape

Progress on Europe's net-zero transition goes hand in hand with a renewable energy infrastructure that is increasingly digitalized and decentralized. As the PV industry adopts Internet and IoT technologies for monitoring, analytics and operations, it inherits the corresponding cyber risk, which elevates system exposure and can open the door to cyberattacks and disruptive operational failures.

Insights from the *2025 Global Energy Transition Report* by Bureau Veritas (Q3 2025) reinforce this picture: as energy systems become more digitalized, stakeholders are voicing heightened concerns about cybersecurity risks across several areas:

- **Cyberattacks on critical energy infrastructure**: These attacks, may lead to risks such as power outages, with cascading effects on economic activity, national security, and geopolitical stability.
- **Cyberattacks on DERs and IoT devices**: The rapid growth of DERs and connected devices, coupled with limited protective measures, is creating new entry points for attackers to compromise grid operations.
- **Insufficient investment in cybersecurity**: According to the survey conducted as part of the Bureau Veritas report, 47% of respondents believe that current investment

[1] The advice in this report is provided for reference only and does not constitute legal, technical, or investment advice. SUNGROW reserves the right to the final interpretation and update of this document.

in cybersecurity protection for energy projects is insufficient.

The industry has become increasingly aware of vulnerabilities that could be exploited by attackers to remotely access inverters and potentially impact grid stability. Moreover, certain indirect or unintentional actions can also have serious consequences. The sector has since taken these findings on board, implementing stronger security measures to prevent similar issues in the future. This highlights a broader challenge of technological innovation: the rapid pace of change requires cybersecurity to be treated as a continuous process. Constant monitoring, swift detection and response, and robust resilience measures are essential to ensure business continuity and maintain trust.

2.2 Cybersecurity: The Industry Perspective

2.2.1 Increased Focus

Professional reports and technical vulnerability assessments provided by cybersecurity experts or institutions raise awareness of cybersecurity risks among regulators and industry stakeholders.

On April 29, 2025, SolarPower Europe reported that no major cyberattacks targeting PV infrastructure had occurred to date and urged the industry to respond to risk assessments based on verifiable evidence rather than speculation. Authorities such as the German Federal Network Agency (Bundesnetzagentur) have also called for strengthened resilience requirements and the adoption of common EU-wide standards.

Overall, there are five key focus areas for the industry's cybersecurity:

- **Remote access to renewable energy assets:** Ensuring secure authentication and access rights for PV inverters and energy storage systems.
- **Data exchange with cloud platforms**: Implementing encryption and mutual authentication between devices and cloud service platforms.
- **Supply chain assurance**: Conducting rigorous reviews of firmware, components,

and third-party services.

- **System stability**: Evaluating the potential impact of cyber incidents on grid reliability.
- **Cybersecurity in ESG governance**: Integrating cybersecurity into ESG governance and disclosure frameworks, with management assuming oversight responsibilities.

2.2.2 Pinpointing Risks and Consequences

Are technical protections and communication systems sufficiently strong and reliable? This question lies at the center of public debate — as any weaknesses in these areas could expose critical risks with potentially serious consequences.

(1) **Major Risks**

- **Data leakage**: Connected inverters and storage systems exchange data with cloud platforms. Weak authentication or encryption could expose user information, system status, and power-generation metrics.
- **Remote control by attackers**: Exploiting inverter vulnerabilities, attackers can alter device settings or operating modes, potentially causing abnormal grid loads, frequency instability, or localized blackouts.
- **Exploitation of product vulnerabilities**: Unpatched firmware flaws could be exploited for ransomware attacks or to create distributed "botnets" of compromised devices.
- **Supply chain compromise**: Malicious code injected into OTA update channels or vendor cloud services can rapidly spread across device fleets, leading to systemic risks.

(2) **Potential Consequences**

- **Power system instability**: Large-scale interference with renewable energy infrastructure can threaten grid reliability and national energy security.
- **Reputational damage**: Incidents involving data breaches or compromised control functions can undermine customer confidence and investor trust.
- **Legal and compliance liabilities**: Security incidents may trigger obligations under regulations such as the GDPR, NIS2, and CRA, potentially resulting in penalties or litigation.

- **Financial losses**: Operators may face significant costs from renewable systems downtime, regulatory fines, and revenue losses following cybersecurity incidents.

2.2.3 Regulatory Compliance Requirements

In Europe, regulations around cybersecurity, data privacy and more are tightening, requiring sector businesses to comply. Below, we explore the key requirements relevant to those operating in the renewable energy sector.

(1) **Key Regulations**

- **Establishment of Risk Management Systems:** The EU NIS2 Directive requires operators of critical infrastructure (which includes energy companies) to establish cybersecurity risk management systems and regularly report security incidents.
- **Cross-Border Data Transfer Restrictions:** The EU GDPR imposes strict requirements on cross-border data transfers. Data generated by PV inverters and energy storage systems may contain personal information and energy-related sensitive data. When such data needs to be transmitted to data centers located outside the EU for analysis or storage, the recipient must provide a level of data protection equivalent to that of the EU. Enterprises must conduct thorough risk assessments and implement appropriate safeguards — such as signing Standard Contractual Clauses — before transferring data across borders. Failure to comply may result in significant fines.
- **Remote Access Restrictions:** Laws in some countries (such as Lithuania) require power plants with output above 100 kW to use equipment that complies with national security standards, also mandating that these plants restrict remote access functions. To meet compliance requirements, enterprises must modify systems or implement technical adaptations, such as localized data storage.
- **Cybersecurity Certification Mechanism:** The EU is promoting the creation of a unified cybersecurity certification framework, requiring products to meet security standards throughout their design, development, testing, and deployment.

(2) **Localized Deployment**

Many European countries require energy infrastructure (equipment and related systems) to be deployed locally whenever possible. This means that data storage,

processing, and software development for PV inverters and energy storage systems must comply with localized deployment requirements — presenting both cost and technical challenges. For example, building local data centers requires significant investment in site leasing, equipment procurement, and staffing. Additionally, companies must adapt to local technical standards and regulatory requirements to ensure system security and compliance. Localized deployment also involves cooperation with local suppliers. Selecting reliable partners and ensuring supply chain security are additional challenges enterprises must address.

2.3 Cybersecurity: The Customer Perspective

2.3.1 Awareness Gaps

Security is a strategic enabler of competitive solutions and responsible, robust policy. As such, industry operators and policymakers have had to develop a keen understanding of the topic out of necessity. This is not the case for customers, however. Customers want solutions to be secure but may not fully appreciate what this entails behind the scenes.

(1) **Underestimating Energy Connectivity**

Many customers still view PV inverters and energy storage systems as "mere power generation devices". Some may not realize that these systems require network connectivity, which exposes them to many of the same cyber risks that their IT systems are exposed to. As a result, customers are not being as vigilant as they should be when it comes to "traditional IT" measures like access control, which they may not consider applying to their energy equipment. For example, multiple users might share the same account logins on platforms for managing energy equipment, which leaves the company open to risks like data leakage. Ultimately, it's critical that customers start to view energy infrastructure as "digital technology".

(2) **Overlooking Cybersecurity Scope**

Customers often attribute cybersecurity responsibility solely to equipment providers, disregarding the multilayered structure of cybersecurity in renewable energy systems. Inverter and energy storage manufacturers only cover part of the system's security.

Overall security also involves third-party platforms, communication links, and remote operation and maintenance (O&M) systems.

(3) **Overreliance on Security Standards**

During procurement, customers frequently use compliance with specific certifications (such as ISO) as the sole criterion for evaluating cybersecurity. However, this overlooks the inherent limitations of an isolated standard. There are different standards for different aspects — some address management systems or specific technical aspects, without addressing dynamic risks encountered in real-world device operation.

While certification is an advantage, it is only one part of the cybersecurity equation. Certification standards serve as the foundation for building trust, but they cannot replace comprehensive security evaluations and ongoing technical investment. When investing, customers should also consider their chosen supplier's security design philosophy, risk assessment approach, response mechanisms, and commitment to transparency, so they can make an informed decision about their system's security

2.3.2 Market Demand

Customer concerns around cybersecurity have gradually shifted from an abstract awareness about what is needed to "feel safe" to a concrete set of professional requirements for which features they want to have included when they invest. Below, we highlight the areas where we see the strongest market demand.

- **Information Security Management Systems and Certifications:** Establishment of an ISO-compliant ISMS and attainment of cybersecurity certifications recognized by the EU or other international authorities.
- **Security Auditing and Update Mechanisms:** Conduct of regular security audits and frequency against industry standards. Availability of emergency response plans for data breaches, and support for access log tracking and abnormal traffic detection.
- **Data Management and Protection:** Compliance with industry standards and legal requirements for data destruction, desensitization, and isolation.
- **Patch and Firmware Management:** Regular updates of patches and firmware to prevent exploitation of known vulnerabilities.

- **Intrusion Prevention and Incident Response:** Presence of an IPS and an SIEM, as well as an established and regularly evaluated incident response plan.
- **Authentication and Access Control:** Implementation of MFA to enhance account security, and access control mechanisms designed with clear and appropriate privilege allocation.
- **System Monitoring and Log Management:** Compliance of system log retention periods with regulatory requirements.

These feature focal points reflect customers' increasing emphasis on cybersecurity and provide SUNGROW with clear guidance in product-security design and customer-engagement strategies.

3 Cybersecurity Standards and Regulations

3.1 Standards and Regulations

In the context of global energy digitalization, cybersecurity standards have become the fundamental threshold for equipment manufacturers to enter international markets.

This paper addresses regulatory compliance for SUNGROW’s PV inverters and Battery Energy Storage System solutions across residential, Commercial & Industrial, and utility scenarios.

Standards and regulations such as ISO/IEC 27001, ISO/IEC 27701, IEC 62443-4-1, IEC 62443-4-2 and GDPR provide clear frameworks for enterprises to establish information security management systems, privacy protection mechanisms, and secure development processes. These standards play a vital role in enhancing organizational security governance capabilities and meeting regulatory compliance requirements.

- ISO/IEC 27001

ISO/IEC 27001 is an international standard for information security management systems jointly issued by ISO and IEC. This standard covers a series of management activities, including the establishment, implementation, operation, monitoring, review,

maintenance, and continual improvement of information security management systems.

- ISO/IEC 27701

Jointly issued by ISO and IEC, ISO/IEC 27701 is an international standard for privacy information management systems (PIMSs). It covers technical and organizational measures such as encryption, access control, risk assessment, and data breach response to ensure that the handling of PII is both legally compliant and robustly protected.

- IEC 62443-4-1

Titled "Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements", this standard is an important part of the IEC 62443 series of standards. It specifies the requirements throughout the product development lifecycle to ensure product security.

- IEC 62443-4-2

The IEC 62443-4-2 standard, titled "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components", is an important part of the IEC 62443 series of standards. This standard is designed to ensure that the components used in industrial automation and control systems have sufficient security to defend against various cyberattacks and threats.

- ETSI EN 303 645

Issued by the ETSI, this cybersecurity standard for consumer Internet of Things (IoT) products. It aims to address widespread and significant cybersecurity vulnerabilities by establishing a baseline for the secure design of Internet-connected consumer products, ensuring user privacy, and preventing elementary attacks targeting fundamental design flaws.

- RED 2014/53/EU

The RED 2014/53/EU was issued by the EU on May 22, 2014, and came into force on June 13, 2016. The directive introduced a new Article 3.3, which strengthens

compliance requirements for the cybersecurity of radio equipment and the protection of personal data and privacy. These provisions became mandatory on August 1, 2025.

Under Article 3.3 of the RED 2014/53/EU, three technical specifications (d), (e), and (f) are implemented through the EN 18031 series of standards developed by the EU (corresponding to EN 18031-1, EN 18031-2, and EN 18031-3, respectively). The specific requirements are as follows:

(d) Radio equipment shall not harm the network or its functions, nor misuse network resources, thereby causing an unacceptable degradation of service quality.

(e) Radio equipment shall incorporate safeguards to ensure the protection of personal data and privacy of users and subscribers.

(f) Radio equipment shall include features to prevent fraud.

- GDPR

The GDPR, issued by the EU, is a regulation designed to protect the personal data of EU citizens. It establishes explicit requirements for data controllers and data processors in handling personal data. GDPR applies to all EU member states and organizations that collect personal data of EU citizens. As such, it has a global impact on enterprises worldwide.

- Data Act

The EU Data Act is a comprehensive regulation introduced by the EU to govern data access, sharing, and usage. It covers the rights to access, use, and share data generated by connected products and related services, and clarifies the respective rights and obligations of users, data holders, public institutions, and cloud service providers.

- NIS2

Adopted by the EU in 2022, the NIS2 Directive aims to enhance cybersecurity resilience and harmonization across the EU. The regulation applies to fifteen critical sectors, including energy, transportation, finance, healthcare, and digital infrastructure.

It classifies companies into "essential entities" and "important entities", requiring them to implement measures regarding risk management, incident reporting, business continuity, supply chain security, etc.

The above content provides an overview of international cybersecurity standards and EU-level security regulations. While the EU sets overarching cybersecurity requirements for equipment manufacturers and its regulations continue to evolve, member states still maintain certain national-level cybersecurity requirements, which this chapter does not cover.

3.2 Division of Responsibilities under Standards and Regulations

With the continuous advancement of digitalization and intelligence, cybersecurity has become a core component in the design and operation of power systems. Multiple regulations issued by the EU — such as NIS2, RED, GDPR, and CRA — indicates the division of responsibilities among stakeholders in terms of cybersecurity compliance. These regulations help stakeholders understand their obligations and establish a clear responsibility matrix. This, in turn, enhances cybersecurity, data protection, and supply chain resilience, ensuring the secure and stable operation of power systems within the regulatory framework.

The following figure illustrates the scope of responsibilities of different stakeholders regarding specific cybersecurity regulations.

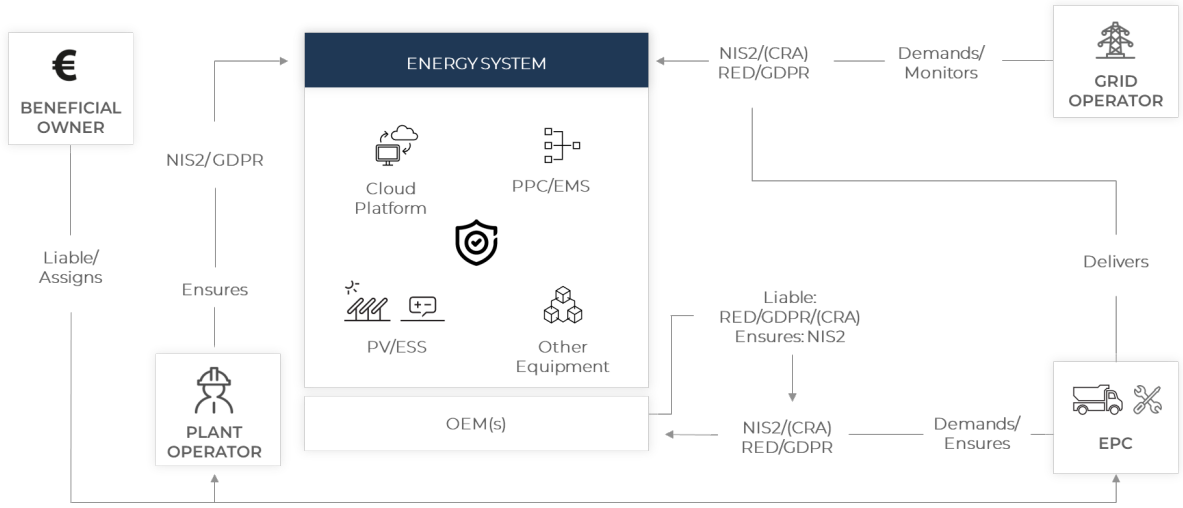

Fig. 1 Stakeholder Responsibilities Under Cybersecurity Regulations

- Beneficial Owner

Project investor or asset owner; responsible for the overall compliance strategy.

- Plant Operator

Responsible for the daily operation and maintenance of the energy system.

- EPC Contractor

Project executor entrusted by the beneficial owner; responsible for equipment procurement and system integration.

- OEM

Responsible for the design, manufacturing, and delivery of equipment and services.

- Grid Operator

Responsible for grid stability and the formulation and supervision of technical interconnection requirements.

The division of responsibilities among stakeholders in the energy system, under NIS2, RED, GDPR, and CRA, is summarized in the table below.

Tab. 2 Responsibility Matrix

	Beneficial Owner	Plant Operator	EPC	OEM	Grid Operator
NIS2	Liable to ensure overall project compliance with NIS2.	Must ensure NIS2 compliance.	Demands and ensures NIS2 compliance of OEMs.	Must ensure NIS2 compliance for its products/services for application in critical infrastructure (supply chain security obligation under NIS2).	Can either directly or indirectly mandate and oversee NIS2 compliance. (Directly by carrying out its own risk management and indirectly by imposing technical connection conditions).
RED	Not directly liable for product RED compliance but must ensure that the equipment used complies with RED requirements.	Not responsible for product RED compliance; It is ensured by the EPC contractor assigned by the Beneficial Owner.	Demands and ensures products' RED compliance from the OEMs.	Liable to ensure products RED compliance and meet CE marking requirement.	Cannot mandate RED compliance directly (as this is manufacturer obligation) but can indirectly mandate it through technical connection conditions to ensure grid security.
GDPR	Liable to ensure GDPR compliance if processing of personal data is involved (which is	Liable to ensure GDPR compliance if processing of personal data is involved (which is mostly the	Demands and ensures GDPR compliance of OEMs.	Liable to ensure GDPR compliance for its services where processing of personal data is involved.	Can demand and monitor GDPR compliance if processing of personal data is involved (which is mostly the case).

	mostly the case).	case).			
CRA	Not directly liable for product CRA compliance but must ensure that the equipment used complies with CRA requirements.	Not responsible for product CRA compliance; It is ensured by the EPC contractor assigned by the Beneficial Owner.	Demands and ensures products' CRA compliance from the OEMs.	Liable to ensure products RED compliance and meet CE marking requirement.	Cannot mandate CRA compliance directly (as this is manufacturer obligation) but can indirectly mandate it through technical connection conditions to ensure grid security.

3.3 Limitations of Existing Cybersecurity Standards

Meeting standards represents regulatory compliance, not the end goal of security. As renewable energy systems evolve rapidly, traditional standards reveal significant shortcomings in terms of technical adaptability, scenario coverage, and end-to-end protection capabilities.

- International Standards

Current general cybersecurity standards exhibit notable limitations when applied to the field of DER. ISO 27001, as a general framework for ISMS, focuses on structured requirements such as risk assessment, documentation, and continuous improvement. However, it lacks technical specifications tailored to industry-specific scenarios — for example, firmware security for PV inverters or encrypted communications at edge nodes. Although IEC 62443 emphasizes security for industrial control systems, including asset identification, zone segmentation, and access control, its primary protection priorities still target traditional industrial equipment such as PLCs and DCSs. It fails to adequately address the emerging needs of DER, including real-time cloud-edge data transmission and large-scale device identity authentication.

- Industry Standards

Existing industry guidelines also face limitations. For instance, IEEE 1547.3 addresses communication security for grid-connected distributed energy systems but does not extend to end-to-end elements such as cloud data storage compliance or supply chain risk management. As a result, equipment manufacturers are often required to comply with multiple fragmented standards, leading to heterogeneous environments with low interoperability.

4 Cybersecurity Solutions

As cybersecurity threats continue to escalate, renewable energy companies are fundamentally re-evaluating the role of cybersecurity. It is now recognized as a cornerstone of energy system security and resilience, rather than solely a technical concern. This evolving recognition highlights the strategic role of cybersecurity in ensuring stable grid operations and advancing the clean energy transition.

In response, renewable energy companies are proactively implementing measures to strengthen their cybersecurity capabilities. These measures include rigorous compliance with international security standards, obtaining certifications from authoritative institutions, enhancing collaboration among regulators, industry peers, and equipment manufacturers, and continuously improving the transparency and auditability of compliance management. Such efforts contribute to building a secure, stable, and sustainable energy ecosystem.

To address customer concerns regarding cybersecurity issues and the limitations of existing security regulations, and to build an end-to-end cybersecurity architecture for energy systems, SUNGROW, sets market access as the minimum requirement. SUNGROW provides security solutions that meet regulatory standards while covering the entire "device–network–platform" chain to build a truly trustworthy energy infrastructure.

4.1 Cybersecurity Governance and Responsibility

SUNGROW integrates cybersecurity into its corporate governance and ESG management framework. Management assumes oversight responsibilities for cybersecurity and ensures orderly governance through annual review mechanisms and continuous improvement processes. The governance framework follows the fundamental principles of "clear accountability, effective management, independent supervision, and transparent disclosure", transforming cybersecurity commitments into actionable management measures and establishing standardized external communication channels.

(1) Cybersecurity Governance Principles

SUNGROW adheres to the following principles in cybersecurity governance:

- Honesty: Accurately disclose cybersecurity capabilities and data processing boundaries, highlight known risks, and specify the scope of application.
- Responsibility: Define roles and responsibilities across the full cybersecurity lifecycle, establish a closed-loop system for issues, and enforce a management accountability mechanism.
- Transparency: Implement routine cybersecurity disclosures and third-party assessment mechanisms, providing verifiable evidence.
- Rigor: Apply international cybersecurity governance frameworks and standards, implement institutionalized internal controls, and pursue continuous improvement.

These cybersecurity governance principles are deeply integrated with the ESG management framework, fostering a sustainable organizational-level system for cybersecurity responsibility and governance.

(2) Core Cybersecurity Values Based on ESG

- Environmental: Cybersecurity governance focusing on availability and reliability helping to reduce risks of unplanned downtime and operational anomalies, ensuring stable output of power plants and equipment throughout their lifecycle. This supports energy efficiency and emission reduction goals, and further advances corporate sustainability practices.
- Social: Protect personal and business data while reducing risks of unauthorized

access or misuse. Incorporate security requirements into supply chain governance to ensure collaboration. Address stakeholder concerns through transparent communication and support localized capabilities in compliance with applicable jurisdictions.

- Governance: Establish a "decision-execution-supervision-disclosure" governance loop to strengthen risk management and compliance. Translate principles into verifiable practices and improve governance maturity.
- Disclosure: Ensure continuity and accessibility of information through annual ESG reporting, regular cybersecurity governance bulletins, and special announcements for major events.

(3) Stakeholder Commitments Based on ESG Principles

- Commitments to Customers

Provide data sovereignty and localized deployment options, respecting jurisdictional requirements and customer choices.

Conduct security response and communication according to established procedures, following the principles of "facts first, legal compliance, and transparency".

Provide verifiable evidence, such as certificate numbers, third-party test/audit summaries, key points from announcements and FAQs, data handling descriptions, and compliance statements.

- Commitments to Investors

Incorporate cybersecurity into key ESG topics and disclose governance progress and long-term value-related information in annual reports.

- Commitments to Regulators and Society

Comply with applicable laws and standards, and support necessary regulatory reviews and third-party assessments.

Participate in the continuous improvement of industry cybersecurity governance rules, promoting a transparent and robust governance ecosystem.

4.2 Organizational and System Architecture Framework

4.2.1 Cybersecurity and Data Protection Office

To meet global compliance and data security requirements and to build a comprehensive, multi-dimensional, and sustainable cybersecurity framework, SUNGROW has established the Cybersecurity and Data Protection Office under the Digital Transformation Management Committee. This Office coordinates and manages the company's ISMS and PSIRT, ensuring efficient and comprehensive implementation of cybersecurity initiatives.

The responsibilities of the Office are as follows:

- ISMS and PSIRT management; develop, execute, and continuously optimize the overall information security plan, covering product information security, privacy, and data compliance.
- Undertake information security and data protection requirements from all business units and promote the implementation of various information security projects.

4.2.2 ISMS

SUNGROW, as an international renewable energy enterprise, has established a comprehensive ISMS. Within this system, a dedicated information security management structure has been deployed from the group level down, playing a critical role in formulating security policies and enforcing security responsibilities.

Different roles and organizational units within the ISMS framework carry distinct responsibilities:

- Digital Transformation Management Committee: Responsible for approving and issuing company-level policies, setting cybersecurity management requirements, and supervising the implementation of cybersecurity management across the organization. This function is undertaken by senior corporate management.
- Cybersecurity and Data Protection Office: Centrally manage the ISMS and PSIRT, develop, execute, and continuously optimize the overall information security plan,

covering product information security, privacy, and data compliance. Undertake information security and data protection requirements from all business units, and promote the implementation of various information security projects.

- Cybersecurity and Data Protection Group: Support the Committee by supervising and inspecting the implementation of security policies. It guides the execution of cybersecurity management activities and conducts risk identification, assessment, and monitoring for cybersecurity incidents. It is also responsible for preparing relevant reports.
- Project Team / Information Security Execution Group: The Project Team and Information Security Execution Group operate at the same organizational level. In line with the company's cybersecurity and privacy protection policies and under the guidance of the Cybersecurity and Data Protection Group, they are responsible for implementing cybersecurity and privacy practices within their respective departments.

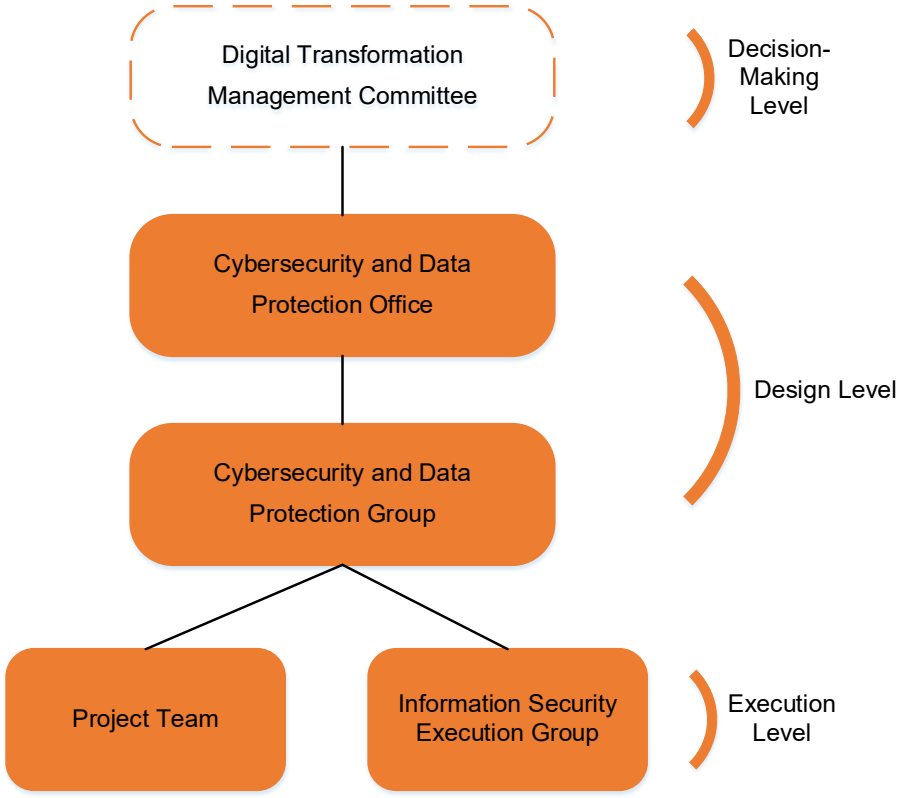

Fig. 2 ISMS Organizational Structure

4.2.3 PSIRT

SUNGROW's PSIRT is a dedicated team responsible for receiving, investigating, and disclosing security vulnerabilities related to SUNGROW products. SUNGROW defines a vulnerability as a security issue that, if exploited by an attacker, may compromise the integrity, availability, or confidentiality of a product.

PSIRT manages security and development processes in alignment with the IEC 62443-4-1 standard. Upon receiving any suspected vulnerability report, PSIRT collaborates with the relevant product teams to analyze and validate the issue. Based on the actual impact on the product, the team assesses the severity, prioritizes remediation, and develops appropriate measures — such as mitigations, patches or updates, or alternative user-side risk mitigation strategies — to reduce or eliminate security risks to users from identified vulnerabilities in SUNGROW products or services.

If a vulnerability is identified in supplier-provided components or services used during product development, delivery, or deployment, PSIRT proactively contacts the supplier to initiate remediation and requires them to fix the issue within a defined timeframe based on the severity level.

Once a vulnerability is confirmed, SUNGROW promptly provides customers with appropriate risk mitigation measures. Vulnerabilities can be reported through the PSIRT section on the SUNGROW official website. Access the reporting page via the following link:

https://en.sungrowpower.com/security-vulnerability-management

Manufacturers should remediate vulnerabilities in their devices while meeting regulatory, standards, and certification requirements. For utility PV plants, remediation is performed through on-site updates. For small distributed systems in remote areas and residential systems, remediation can rely on the manufacturer’s cloud service to deliver remote updates. Manufacturers will clearly inform users of identified vulnerabilities and recommended mitigations. Updates will be deployed only after explicit user approval, following strict security protocols and a staged rollout to minimize risk.

4.3 Implementation and Best Practices

4.3.1 Secure Product Development Lifecycle

High-reliability products are key to ensuring the safe and stable operation of power plant systems. SUNGROW, with reference to and in compliance with the requirements of IEC 62443-4-1, has obtained certification for the secure development lifecycle.

- Threat Modeling, Risk Assessment, and Regulatory Identification

Define product cybersecurity requirements and follow the principle of security by default at the initial design stage. For example, products containing wireless modules comply with the security functions required by EN 18031.

- Source Code Security Detection During Development

At the software development stage, SUNGROW conducts source code security scans using multiple advanced tools, such as static analysis tools, software composition analysis tools, and interactive analysis tools. These tools automatically detect and identify security vulnerabilities and risks in the code, thereby improving code quality, reducing remediation costs, ensuring compliance, and enhancing software security and resilience against attacks.

- Comprehensive Security Testing

Upon completion of product development, SUNGROW performs functional tests, threat mitigation tests, black-box scans, penetration tests, and full vulnerability security tests to verify whether the product meets defined security requirements and quality standards.

- Continuous Vulnerability Management

SUNGROW has the capability to rapidly respond to cybersecurity vulnerabilities, with clearly defined policies, procedures, and incentive/penalty mechanisms. From the company level to the product level, vulnerability management processes are established. Products are regularly scanned for vulnerabilities, and identified issues are managed through a defined workflow, including vulnerability reporting, severity

assessment, distribution and remediation, and fix verification.

- Security Training for Technical Personnel

SUNGROW organizes regular cybersecurity awareness training sessions for all employees each year, helping them understand global cybersecurity compliance requirements and trends, recognize the impact of security incidents on the enterprise, and interpret the content of the ISMS. Targeted training is also provided to equip employees with the specific cybersecurity skills required for their respective roles.

4.3.2 Data Security

(1) Data Confidentiality and Integrity

To ensure the confidentiality of power plant data during transmission and storage, prevent leakage or tampering, and safeguard privacy and security, the following best practices are recommended:

- Server–Client Communication

Data exchange between servers and clients uses the HTTPS protocol. During communication, encryption algorithms are applied to secure power plant data in transit. Additionally, WebSocket technology is used to achieve real-time, bidirectional communication between client and server, ensuring low latency and high efficiency in data transmission.

- Communication Between EMS/PPC and SCADA

The northbound communication protocol between EMS/PPC and SCADA adopts Modbus TCP/IEC 104, with encryption algorithms applied to ensure data confidentiality and integrity during transmission.

- Cloud Communication

Cloud platform uses MQTTS protocol, which supports SSL encryption for all data transmitted to the cloud, ensuring data completeness and accuracy upon receipt.

(2) Data Availability

- Redundant Storage Hardware

In EMS/PPC systems, redundant configurations are provided to eliminate single points of failure. If one unit fails, the other continues to operate independently. Each server also includes redundant components (e.g., dual power supplies).

The EMS/PPC network topology incorporates two or more switches to eliminate network-level single points of failure. Servers are equipped with redundant connections to different switches, ensuring uninterrupted operation even if one switch or link fails.

- Business Data Backup

In EMS/PPC systems, device data is stored on the SCADA server. The active server collects data and writes raw records to the SCADA database. In parallel, over the link between the active and standby servers, the active server automatically replicates SCADA data to the standby server, ensuring rapid recovery in the event of a failure.

- Configuration Data Backup

Configuration file backups are performed on SCADA servers and controllers, with dedicated backup strategies established to ensure rapid system recovery in the event of a disaster.

During system operation, configuration data is synchronized between the active and standby servers as needed. In the event of a primary server failure, the standby server can take over while maintaining the original configuration state, thereby ensuring stable operation of the plant equipment.

(3) Data Destruction

As a cloud-enabled user platform, iSolarCloud provides dashboards for performance insights and maintenance alerts, helping users manage PV and energy storage systems securely while ensuring compliance with data protection standards. For operational data stored, retention rules are defined according to the type of site, ensuring users' rights to access, correct, and delete stored data. Once the retention period expires, data is deleted in accordance with applicable laws to prevent sensitive information leakage and to maintain secure and reliable cloud data management.

(4) Secure Data Access

Sustained data security requires disciplined data exchange. When third parties access data via APIs, interfaces must enforce robust controls to ensure that only authorized parties obtain appropriate data and that all activities are auditable. Ultimately, manufacturers must continuously harden cloud platforms, safeguard firmware distribution and integrity, and secure end-to-end communication channels against malicious intrusion and tampering.

4.3.3 Security Protection Across All Scenarios

Faced with increasingly complex and diverse cyberattack methods, traditional single-layer security measures are no longer sufficient to address the sophisticated threats targeting modern renewable energy power systems. To effectively reduce security risks and ensure the stable and reliable operation of power plants, SUNGROW has designed a systematic, dynamic, and coordinated defense strategy, establishing an end-to-end cybersecurity architecture to safeguard the energy system.

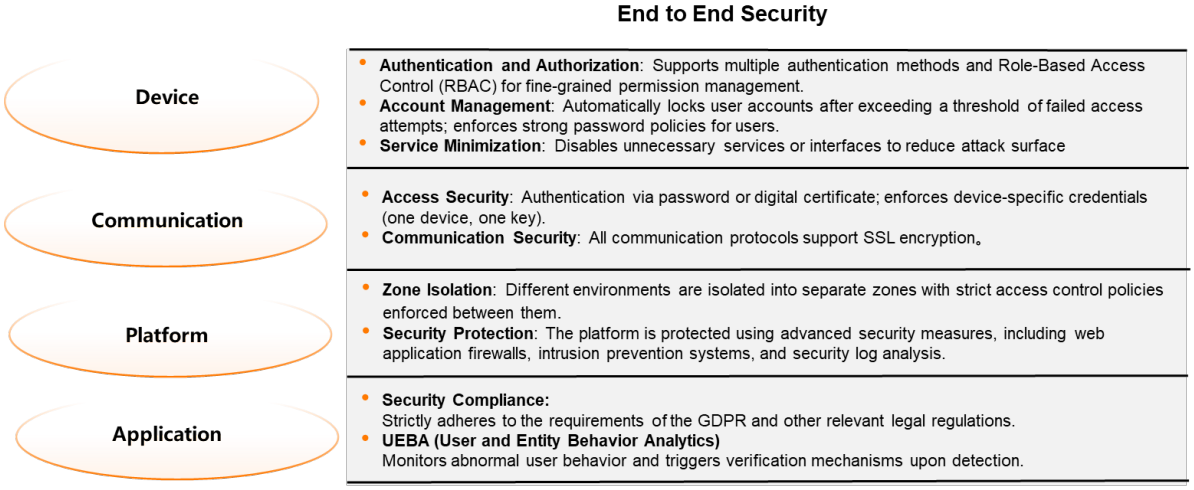

Fig. 3 End-to-End Security Architecture

- Application Layer

The system strictly complies with GDPR and other European regulatory standards. It leverages User and Entity Behavior Analytics (UEBA) to monitor and analyze behavior patterns of users and devices, enabling the identification of potential anomalies or

security threats such as insider threats, account abuse, and abnormal login activities. This ensures the security of assets within the power system.

- Platform Layer

The system isolates development, testing, and production environments based on their respective implementation types. By default, public network access is prohibited (only essential ports are open). Security technologies such as firewalls, intrusion prevention systems, and security log analysis are employed to prevent security risks from spreading across environments. This ensures that data, configurations, and access rights at each stage remain independent, thereby reducing the potential attack surface and safeguarding system security and stability.

- Communication Layer

To ensure the security and stability of communication links and to protect the confidentiality and integrity of data during transmission, the system employs password authentication, digital certificates, or digital signatures for user identity verification, preventing unauthorized or malicious logins. All communication protocols used support encryption algorithms (such as SSL encryption). By encrypting data, the system effectively prevents tampering, theft, or forgery.

- Device Layer

The system implements RBAC to associate access permissions with roles, thereby preventing unauthorized access. It also supports account management functions, including setting thresholds for failed login attempts and enforcing strong password policies. Accounts are automatically locked if login failures exceed the defined threshold, mitigating risks from brute-force attacks and weak credentials. In addition, the system follows the principle of least privilege (PoLP), restricting accounts to only the resources and functions necessary to perform their tasks, thereby reducing potential security risks and minimizing the attack surface.

Given that renewable energy power plants are mainly divided into commercial plants and utility plants, SUNGROW has established differentiated security architecture systems for these two types of plants in order to achieve comprehensive cybersecurity

protection across various application scenarios of renewable energy power systems.

The specific frameworks are as follows:

(1) Security Architecture for Commercial Scenarios

Device Security: All hardware devices within the security architecture comply with internationally recognized security standards such as IEC 62443-4-2 or EN 18031, and are audited and certified by authorized certification bodies.

Cloud Platform Security: iSolarCloud leverages a wide range of cloud security tools to enhance application security.

- Regional Isolation

  iSolarCloud implements physical regional isolation through localized deployment across regions such as China, Europe, and Australia. Data from each region is stored independently, ensuring operational independence of the cloud platform and data isolation.

- Tenant Isolation

  Within each server, iSolarCloud enforces logical isolation for tenants. Each tenant operates in a logically isolated environment with authentication, authorization, and encryption mechanisms applied to prevent unauthorized access, ensuring that tenant-specific data and operations remain securely protected.

- Human-Machine Verification

  iSolarCloud employs advanced risk control engines to provide real-time risk assessments for high-risk device operations, brute-force attacks, replay attacks, and other malicious activities.

Device-Cloud Connection Security: Devices communicate with the cloud platform through secure encryption methods, ensuring the confidentiality and integrity of data transmission.

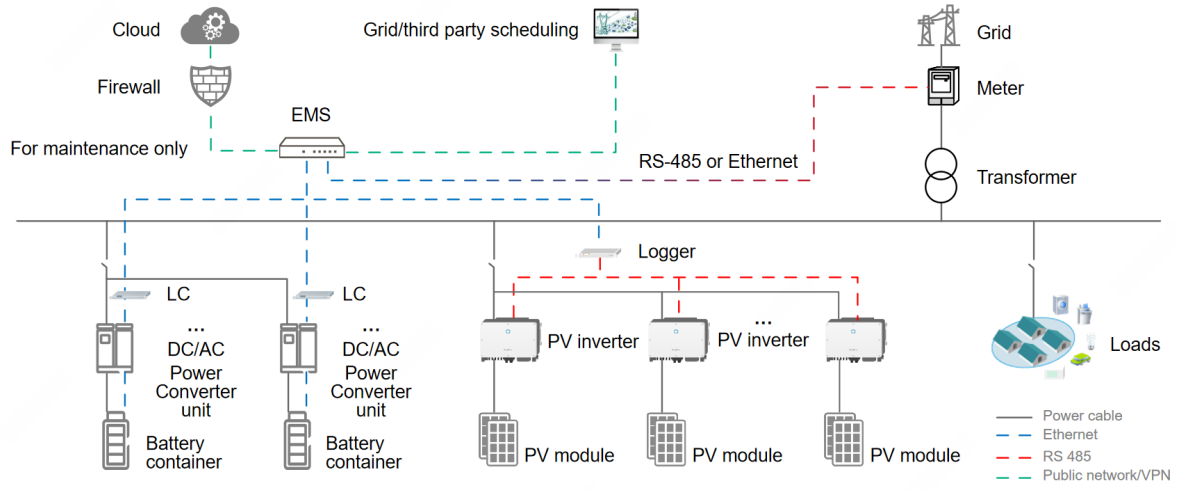

Fig. 4 Security Architecture for Commercial Scenarios

(2) Security Architecture for Utility Scenarios

Cybersecurity architecture for utility systems adopts a layered security strategy based on the PERA model. It integrates the Zero Trust Architecture (ZTA) and the PoLP to ensure secure system design. The layered structure is as follows:

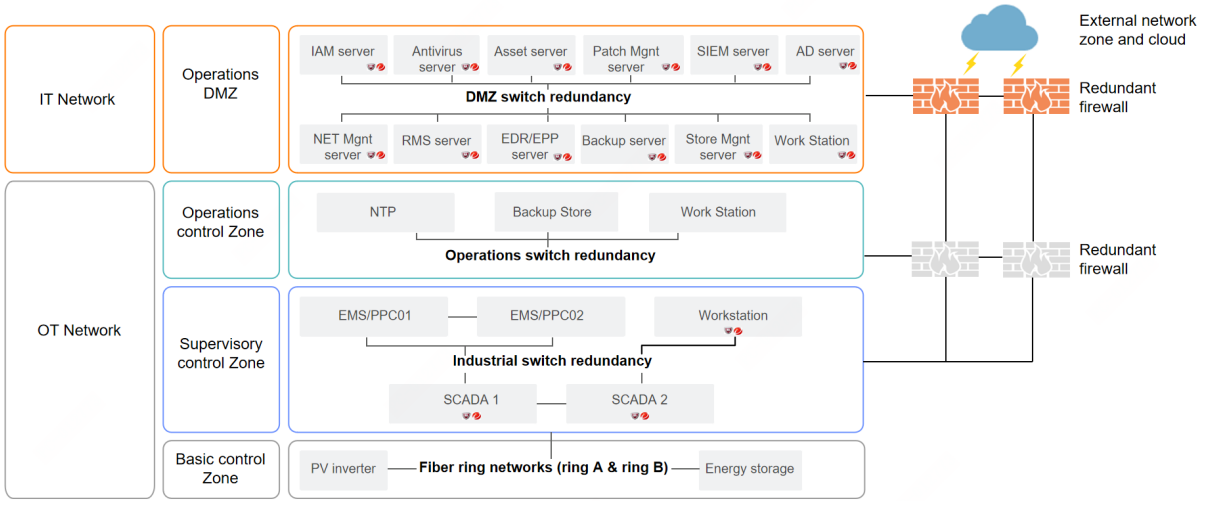

Fig. 5 Cybersecurity Architecture for Utility Systems

It is mainly divided into two domains:

- IT Network, which includes the external network and cloud (not within the scope of this document), as well as the industrial demilitarized zone (Operations DMZ).

• OT Network, which includes the operations and control zone (Operations management), the process control zone (Supervisory control, Basic control, Physical process).

The cybersecurity requirements for each layer are as follows:

Tab. 3 Security Measures and Requirements for Operations DMZ

Security Measures	Cybersecurity Requirements
Firewall	Deploy a layered network architecture that incorporates access control, DPI, IPS, logging, and high-availability design to achieve asset isolation and dynamic threat defense, thereby ensuring network security, reliability, and scalability.
Identity Authentication	Integrate MFA, encrypted transmission, and access control, with support for SSO and session management. Identity authenticity and data security are further ensured through log auditing and countermeasures against attacks such as session hijacking.
Antivirus	Real-time monitoring, scheduled scanning, and automatic virus database updates are implemented to detect and remove malicious software (e.g., ransomware), preventing data breaches and system damage while strengthening endpoint security protection.
Patch Updates	Automated distribution of security patches and regular vulnerability remediation ensure that devices and software remain up to date, reducing the risk of known vulnerabilities being exploited, and enhancing overall system security.
Data Backup	Automated local and cloud-based backups (including incremental backups) ensure data recoverability in the event of hardware failure, cyberattacks, or disasters, thereby safeguarding business continuity and data integrity.

Tab. 4 Security Measures and Requirements for Operations Management

Security Measures	Cybersecurity Requirements
Network Isolation	An industrial firewall is deployed between operations DMZ and operations management zone to prevent the spread of attacks.
Protocol Security	Enable DPI to monitor communications of commonly used protocols and prevent the injection of abnormal commands.
Device Authentication	Before network access, devices must undergo fingerprint-based authentication to prevent unauthorized device intrusion.
Patch Management	All operations management zone device patches must be tested to ensure they do not affect the stability of the control system.

Tab. 5 Security Measures and Requirements for Supervisory Control

Security Measures	Cybersecurity Requirements
Physical Isolation	Unidirectional data isolation devices are deployed between the operations management zone and supervisory control zone. Only devices from operations DMZ and operations management zone are permitted to access supervisory control zone devices, while supervisory control zone devices are prohibited from initiating network connections.
Firmware Security	Device firmware updates must undergo digital signature verification to prevent firmware tampering.
Port Management	All unnecessary ports must be disabled, and only those required for essential industrial protocols are enabled.

Tab. 6 Security Measures and Requirements for Basic Control

Security Measures	Cybersecurity Requirements
Network Minimization	Devices are only allowed to communicate with the supervisory control zone layer, and external access is strictly prohibited.

Physical Protection	Equipment rooms and wiring cabinets must be locked to prevent physical tampering.

Tab. 7 Security Measures and Requirements for Physical Process

Security Measures	Cybersecurity Requirements
Physical Security	The area around the equipment must have surveillance cameras and access control measures to prevent intentional damage.
Safe Operating Mode	In the event of an abnormal condition, devices must be able to automatically switch to a safe mode to prevent catastrophic failures.

4.3.4 Supply Chain Security

Any third-party digital component that includes code (including software-integrated components) must be evaluated for supply chain cybersecurity risks and incorporated into the organization's overall supply chain risk management framework. This is because external digital components — such as software, firmware, network connectivity, or digital processing capabilities — can directly or indirectly increase the attack surface of the supply chain. Moreover, inadequate security practices by third-party vendors may become a weak link in the organization's overall cybersecurity posture.

SUNGROW applies a structured and carefully managed process for the onboarding and evaluation of digital suppliers. Supplier selection is conducted by the Procurement Center based on the technical requirements proposed by the requesting department and in accordance with project tendering rules. Supplier admission considerations and qualification reviews include but are not limited to: relevant qualification certificates issued by authorities, company size, security capabilities (such as supplier security certifications, quality certifications, history of major cybersecurity incidents, and emergency response capabilities), as well as technical competencies.

SUNGROW implements tiered supplier management, assigning differentiated security requirements to different supplier levels. A "Prevention-Monitoring-Response-

Recovery" model has been established as the foundation of its supply chain security management system, enabling risk control for third-party digital components including software-integrated components. This approach enhances the resilience of the product supply chain and ensures that associated risks remain controllable.

4.3.5 Best Security Practices

- Penetration testing

Penetration testing is an authorized simulated attack conducted on software systems to assess their security. It serves as a mechanism to verify that cybersecurity defense functions are operating as intended.

SUNGROW adopts the Plan–Do–Check–Act (PDCA) mechanism to continuously enhance its security testing capabilities. Regular penetration tests are conducted, categorized into internal and external testing. Internal penetration tests are performed with each new version release, while external penetration tests are conducted annually by third-party security audit organizations or security vendors to validate the effectiveness of product security controls.

- Bug Bounty Program

In today's highly interconnected network environment, cybersecurity has become an integral part of the product development lifecycle. Although enterprises take various measures to ensure the security of their systems, it must be acknowledged that no system is completely immune to vulnerabilities. Moreover, with the growing economic losses caused by cyberattacks worldwide, enterprises have realized that relying solely on internal security teams is insufficient to identify and fix all potential vulnerabilities.

Therefore, to further enhance product security, SUNGROW has launched a vulnerability bounty program for its mainstream products. A comprehensive mechanism has been established for vulnerability submission, verification, remediation, and feedback, along with a reward and incentive system. Global white-hat contributors are invited to help identify and report product security vulnerabilities. In addition, following industry best practices, SUNGROW discloses the handling status of vulnerabilities and continuously improves its product protection system, enhancing

overall defense capabilities to gain recognition and trust from both industry and users.

5 Future Outlook

Progress around cybersecurity in the sector is being made but, as we have highlighted, it is an iterative, systematic, long-term undertaking. It is one that SUNGROW prioritizes within our own operations and champions externally to foster industry wide adoption. To this end, we offer two recommendations.

5.1 Develop Unified End-to-End Cybersecurity Standards

Given the current fragmentation of standards, it is necessary to develop a unified set of end-to-end cybersecurity standards for power systems. To achieve this within the next three years, equipment manufacturers, service providers, and system operators should join forces to collaborate on the creation of clearly defined responsibilities in standards development. This unified framework should cover the entire "device–network–platform" chain.

The implementation of a single set of standards will help reduce cross-regional compliance costs and enhance the overall security and interoperability of renewable energy infrastructure. Ultimately, it will lay a solid security foundation for the large-scale deployment of renewable energy facilities.

5.2 Engage Customers

It is recommended that both manufacturers and users share responsibility for energy cybersecurity, each fulfilling their respective obligations. SUNGROW has long placed strong emphasis on this topic and is committed to continuously enhancing its practices.

Building on existing measures, SUNGROW is focusing on further strengthening user-side O&M security awareness, standardizing access and account management, and ensuring robust long-term management of the OT/IT boundary. These efforts are supported by close cooperation with customers and partners — through ongoing training, sharing of best practices, clearer communication, and the provision of

practical tooling support.

Another important step is to ensure that security roles and responsibilities are clearly defined. SUNGROW therefore recommends assigning tasks in the following way:

(1) **User Responsibilities**

- Avoid exposing devices directly to the Internet.
- Properly protect account credentials to prevent loss or theft.
- Upgrade and update devices in a timely manner.
- Do not disable security features.
- Isolate the OT network from the IT network.
- Install necessary security protection software.

(2) **Manufacturer Responsibilities**

- Comply with applicable laws and regulatory standards.
- Obtain security and compliance certifications.
- Provide secure and reliable products.
- Remediate product vulnerabilities in a timely manner.
- Provide supporting security protection solutions.
- Implement strict data protection measures.

In addition, we proactively collaborate with industry stakeholders - from associations and policymakers to operators - to promote best practice in cybersecurity and system reliability. SUNGROW will continue to take all opportunities, such as position paper and public consultation, to contribute to building secure, clean, efficient, and trusted energy infrastructure in Europe.

6 Conclusion

We are all travelling toward the same net-zero destination: a world where our energy is as secure as it is sustainable and reliable. To achieve this mission, the industry must build end-to-end security capabilities that meet regulatory requirements.

Compliance with industry standards is only the starting point for market access.

Competitive market success must go beyond that, responding to the ever-evolving digital landscape. **It requires continuous commitment and investment**. This extends to product security design, data protection, platform architecture, and supply chain management. **It demands collaboration**. This must be embraced for the creation of new standards, and to forge closer, transparent working relationships where security responsibilities are shared among manufacturers, service providers, and users. In this way, the industry can build an open, transparent, collaborative, and trustworthy security governance framework.

With our continuous commitment, investment, and collaboration, we can move Europe's industry forward, unlocking even more sustainable development and large-scale applications of renewable energy systems.

Sungrow Europe

Address: Balanstr. 59 | 81541 Munich | Germany
Telephone: +49 89 998 2414 02
Email: germany@sungrow-emea.com
Web: https://ger.sungrowpower.com/

Version: 1.03