Article

Not peer-reviewed version

Why the PV Industry Needs a Dedicated Cybersecurity Standard to Achieve CRA Compliance: A Technical and Regulatory Gap Analysis

V. Salas *

Posted Date: 20 March 2026

doi: 10.20944/preprints202603.1601.v1

Keywords: cyber resilience act (CRA); PV inverter cybersecurity; distributed energy resources (DER); Secure-by-design; Secure update mechanisms; SBOM transparency; grid-connected inverters; IoT/OT security; energy systems cybersecurity; conformity assessment; IEC standards; regulatory gap analysis

 doi:10.20944/preprints202603.1601.v1

Article

Why the PV Industry Needs a Dedicated Cybersecurity Standard to Achieve CRA Compliance: A Technical and Regulatory Gap Analysis

V. Salas

Department of Computer Science – IES Vista Alegre, Cybersecurity & PV Systems, Madrid, Spain; vsm425@educa.madrid.org

Abstract

The European Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all products with digital elements across the European Union. As a directly applicable EU regulation, the CRA is already legally binding in all Member States, with its obligations entering into force progressively: the designation of conformity assessment bodies from June 2026, manufacturer reporting obligations from September 2026, and full product-level cybersecurity requirements from December 2027. Because CRA conformity is assessed at the product level, photovoltaic (PV) inverters—now among the most widely deployed and exposed distributed energy resources (DER)—require clear, technology-specific guidance to meet these obligations. However, the PV industry currently lacks a sector-specific technical standard capable of translating the CRA's horizontal requirements into concrete, verifiable controls for inverter manufacturers. This regulatory gap creates uncertainty for compliance, hinders harmonized conformity assessment, and exposes critical DER assets to avoidable cybersecurity risks. This paper provides the first systematic analysis of the misalignment between CRA obligations and existing PV-related standards, demonstrating that frameworks such as IEC 62443, ETSI EN 303 645, IEEE 1547, and UL 2941 are either too generic, incomplete, or not tailored to inverter architectures, lifecycle processes, and communication interfaces. We argue that a dedicated product-level standard is essential to operationalize CRA requirements for secure development, secure update, vulnerability handling, SBOM transparency, interface protection, and conformity assessment. Building on the structure and principles of an internal working-level concept informally referred to as IEC 6XXXX-1 "Cybersecurity of Utility-Interconnected PV Inverters," we illustrate how a future sectoral standard with this scope and characteristics could provide the necessary foundation for CRA alignment—even though no such standard has been formally proposed within IEC. By mapping CRA essential requirements to inverter-specific technical controls and lifecycle processes, this work shows how a product-level sectoral standard can provide manufacturers with a clear path to compliance while enabling regulators, test laboratories, and grid operators to enforce consistent security baselines. The paper concludes that without such a standard, CRA compliance for PV inverters will remain fragmented, unverifiable, and insufficient to protect Europe's rapidly expanding solar infrastructure. While system-level cybersecurity frameworks are also needed, the CRA makes clear that compliance must begin with the component—making a dedicated inverter standard an urgent and strategic priority. Disclaimer — "IEC 6XXXX-1" referenced throughout this paper is a working-level conceptual framework, not an approved or formally proposed IEC project. It is used solely to illustrate the type of requirements that a future sector-specific standard would need to incorporate in order to align with CRA obligations.

Keywords: cyber resilience act (CRA); PV inverter cybersecurity; distributed energy resources (DER); Secure-by-design; Secure update mechanisms; SBOM transparency; grid-connected inverters; IoT/OT

 doi:10.20944/preprints202603.1601.v1

security; energy systems cybersecurity; conformity assessment; IEC standards; regulatory gap analysis

1. Introduction

The rapid expansion of photovoltaic (PV) generation across Europe has transformed PV inverters into critical digital components of the modern energy system [1]. Once simple power-conversion devices, inverters have evolved into highly connected cyber-physical systems equipped with remote monitoring, cloud integration, bidirectional communication, and grid-support functions [2,3]. This increased digitalization has amplified their cybersecurity exposure, making them potential entry points for attacks that could compromise grid stability, consumer privacy, and the resilience of distributed energy resources (DER) [1,4].

In response to the growing cybersecurity risks associated with connected products, the European Union has adopted the Cyber Resilience Act (CRA), a horizontal regulation establishing mandatory cybersecurity requirements for all products with digital elements [5,6]. As a directly applicable EU regulation, the CRA is already legally binding across all Member States, with its obligations entering into force progressively: the designation of conformity assessment bodies from June 2026, manufacturer reporting obligations from September 2026, and full product-level cybersecurity requirements from December 2027. PV inverters fall squarely within the CRA's scope: they contain embedded software, expose multiple communication interfaces, receive remote updates, and interact with cloud-based services [2,1]. Consequently, manufacturers must demonstrate secure development practices, vulnerability management, secure update mechanisms, SBOM transparency, and comprehensive technical documentation throughout the product lifecycle [5,7,8,9].

However, despite the CRA's broad applicability, the PV industry lacks a dedicated technical standard capable of translating the CRA's horizontal obligations into actionable, inverter-specific requirements. Existing frameworks—such as IEC 62443 [10], ETSI EN 303 645 [11], IEEE 1547 [12], and UL 2941 [13]—provide valuable guidance but remain either too generic, too narrow, or insufficiently aligned with inverter architectures, operational contexts, and communication protocols. This absence of a sector-specific standard creates a regulatory and technical gap: manufacturers have no clear path to demonstrate CRA conformity, test laboratories lack harmonized criteria for assessment [14], and regulators cannot enforce consistent security baselines across the European PV ecosystem [4]. Moreover, because CRA conformity is assessed at the product level, a system-level cybersecurity framework—while necessary—cannot substitute for a product-level standard. Compliance must begin with the component, and PV inverters represent the most widely deployed and exposed DER device.

This paper argues that a dedicated cybersecurity standard for PV inverters is essential to operationalize CRA compliance and ensure the security and resilience of Europe's rapidly expanding solar infrastructure [1,4]. Building on the structure of an internal working-level concept informally referred to as IEC 6XXXX-1 "Cybersecurity of Utility-Interconnected PV Inverters" [15], we analyze how a future sectoral standard could bridge the gap between CRA requirements and the unique characteristics of inverter systems. By mapping CRA essential requirements to inverter-specific controls, lifecycle processes, and documentation obligations, we demonstrate how such a standard would provide manufacturers with a clear, verifiable, and harmonized route to compliance—even though no such standard has yet been formally proposed within IEC.

2. Background and Motivation

The cybersecurity posture of photovoltaic (PV) inverters has become a critical concern as Europe accelerates its transition toward a highly distributed, inverter-dominated power system. Modern PV inverters are no longer isolated power-conversion devices; they are complex cyber-physical systems equipped with embedded software, multiple communication interfaces, remote monitoring

 doi:10.20944/preprints202603.1601.v1

capabilities, and cloud-connected services. Their integration into grid-support functions—such as voltage regulation, frequency response, and curtailment—makes them essential components of grid stability and resilience. As a result, vulnerabilities in inverter firmware, communication protocols, or cloud platforms can have systemic consequences, enabling attackers to disrupt generation, manipulate telemetry, or coordinate large-scale distributed attacks.

Despite this increasing criticality, the PV industry has historically lacked a unified cybersecurity framework. Existing standards address only fragments of the problem: IEC 62109 focuses on electrical safety, IEEE 1547 addresses interoperability but not security, and IEC 62443 provides a generic industrial cybersecurity framework that is not tailored to inverter architectures or operational contexts. Meanwhile, real-world incidents—including remote compromise of DER gateways, exploitation of weak authentication mechanisms, and manipulation of inverter telemetry—demonstrate that the threat landscape is evolving faster than the industry's ability to respond.

The adoption of the European Cyber Resilience Act (CRA) marks a turning point. For the first time, manufacturers of PV inverters are legally required to implement secure development practices, provide secure update mechanisms, manage vulnerabilities throughout the product lifecycle, and supply transparency artifacts such as Software Bills of Materials (SBOMs). However, the CRA is intentionally horizontal: it defines essential requirements but does not specify how manufacturers in a given sector should meet them. Without a sector-specific technical standard, manufacturers face ambiguity in interpreting CRA obligations, test laboratories lack harmonized criteria for conformity assessment, and regulators cannot enforce consistent security baselines across the PV ecosystem.

This misalignment between regulatory expectations and available technical guidance creates a structural gap. Manufacturers need a clear, actionable, and inverter-specific standard that translates the CRA's high-level requirements into concrete controls, lifecycle processes, and documentation obligations. The absence of such a standard risks inconsistent implementations, fragmented security practices, and uneven levels of protection across Europe's rapidly expanding solar infrastructure.

The motivation for this work is therefore twofold: (1) to demonstrate that existing standards are insufficient to operationalize CRA compliance for PV inverters, and (2) to show that a dedicated standard—such as the proposed IEC 6XXXX-1—can provide the necessary technical foundation for secure, compliant, and resilient inverter design.

3. The Cyber Resilience Act and Its Implications for PV Inverters

The Cyber Resilience Act (CRA) represents the European Union's most comprehensive regulatory effort to date to strengthen the cybersecurity of products with digital elements. Unlike sector-specific directives or voluntary standards, the CRA establishes a horizontal, legally binding framework that applies to any hardware or software product placed on the EU market, regardless of its industry domain. Its objective is to ensure that digital products are designed, developed, and maintained with an adequate level of cybersecurity throughout their entire lifecycle. For manufacturers of photovoltaic (PV) inverters—devices that combine embedded software, network connectivity, and critical grid-support functions—the CRA introduces a set of obligations that fundamentally reshape product design, development processes, and post-market responsibilities.

3.1. Scope and Essential Requirements of the CRA

The CRA defines PV inverters as "products with digital elements," a category that includes any device whose functionality relies on software or network connectivity. As such, inverter manufacturers must comply with the CRA's essential cybersecurity requirements, which fall into three broad categories:

- **Secure product design and development**, including threat modeling, secure coding, and protection against known vulnerabilities.
- **Technical security measures**, such as secure boot, secure update mechanisms, authentication and access control, protection of communication interfaces, and integrity safeguards.

 doi:10.20944/preprints202603.1601.v1

- **Lifecycle and transparency obligations**, including vulnerability handling, coordinated disclosure, SBOM provision, and documentation of security properties.

These requirements apply not only to the inverter hardware and firmware but also to associated cloud services, mobile applications, configuration tools, and communication gateways. The CRA therefore extends its reach across the entire ecosystem surrounding a PV inverter.

3.2. Lifecycle Obligations and Post-Market Responsibilities

One of the most transformative aspects of the CRA is its emphasis on **post-market cybersecurity**. Manufacturers must continuously monitor vulnerabilities, provide timely security updates, and notify authorities of actively exploited vulnerabilities or incidents. This represents a significant shift for the PV industry, where long product lifetimes (15–25 years), fragmented firmware management, and inconsistent update practices have historically hindered coordinated security maintenance.

For PV inverters, these obligations imply:

- Maintaining secure update channels for the entire operational lifetime.
- Ensuring that firmware images are signed, verified, and protected against rollback.
- Providing vulnerability remediation within reasonable timeframes.
- Documenting all security-relevant changes and communicating them to operators.

Given the prevalence of remote monitoring portals and cloud-based fleet management systems, manufacturers must also ensure that these services comply with CRA requirements, including authentication, access control, data protection, and resilience.

3.3. Why PV Inverters Are Unambiguously Within the CRA's Scope

PV inverters exhibit all characteristics that the CRA explicitly targets:

- **Embedded software** controlling power conversion, grid support, and telemetry.
- **Multiple communication interfaces**, including Ethernet, RS485, Wi-Fi, LTE, and fieldbus protocols.
- **Remote connectivity** to cloud platforms for monitoring, diagnostics, and updates.
- **Bidirectional communication** with aggregators, DSOs, and grid operators.
- **Criticality to energy infrastructure**, making them potential targets for cyberattacks.

These features make PV inverters not only eligible but **high-priority** candidates for CRA enforcement. Their compromise could lead to coordinated disconnection, grid instability, manipulation of telemetry, or exploitation of cloud-connected services.

3.4. Challenges for Manufacturers Under a Horizontal Regulation

While the CRA provides a clear set of obligations, it does not specify how manufacturers in a given sector should meet them. This creates several challenges for inverter manufacturers:

- **Ambiguity in interpreting requirements** such as secure update, interface protection, or vulnerability handling.
- **Lack of harmonized standards** that provide presumption of conformity for inverter-specific architectures.
- **Difficulty in demonstrating compliance** to notified bodies without sector-specific criteria.
- **Inconsistency across manufacturers**, leading to uneven security baselines.
- **Uncertainty for test laboratories**, which lack inverter-specific evaluation procedures.

The CRA's horizontal nature is intentional, but it leaves a vacuum for sectors—like PV inverters—where the attack surface, operational context, and lifecycle characteristics differ significantly from consumer IoT or generic industrial devices.

3.5. Implications for the PV Industry

The implications of the CRA for the PV industry are profound:

 doi:10.20944/preprints202603.1601.v1

- Manufacturers must adopt secure development practices that many have not previously implemented.
- Legacy firmware and update mechanisms must be redesigned to meet CRA requirements.
- Cloud services associated with inverters must undergo security hardening and documentation.
- Operators will increasingly demand CRA-compliant products to meet their own NIS2 obligations.
- The absence of a sector-specific standard risks delaying compliance and increasing costs.

These challenges underscore the need for a dedicated technical standard that translates CRA obligations into actionable, inverter-specific requirements—precisely the gap that IEC 6XXXX-1 aims to fill.

4. Regulatory and Technical Gap Analysis

The introduction of the Cyber Resilience Act (CRA) marks a decisive shift in how cybersecurity is regulated across the European Union. However, the CRA's horizontal nature—designed to apply uniformly to all products with digital elements—creates a structural misalignment with the technical realities of photovoltaic (PV) inverters. This section analyzes the regulatory and technical gaps that arise when attempting to apply the CRA to inverter manufacturers in the absence of a dedicated sector-specific standard.

4.1. Absence of Sector-Specific Normative Guidance

The CRA relies on the concept of *presumption of conformity*, whereby manufacturers can demonstrate compliance by adhering to harmonized standards. Yet, no harmonized standard currently exists for PV inverter cybersecurity. The standards landscape is fragmented:

- IEC 62443 provides a generic industrial cybersecurity framework but does not address inverter-specific architectures, communication interfaces, or lifecycle constraints.
- ETSI EN 303 645 targets consumer IoT devices and lacks provisions for grid-support functions, DER communication protocols, or long-term operational requirements.
- IEEE 1547 focuses on interoperability and grid integration, not cybersecurity.
- UL 2941 addresses DER cybersecurity but is not aligned with CRA lifecycle obligations or European conformity assessment processes.

This fragmentation leaves manufacturers without a clear, authoritative reference for implementing CRA-aligned controls.

4.2. Misalignment Between CRA Obligations and Current Industry Practices

The CRA introduces obligations that many inverter manufacturers are not yet prepared to meet. These include:

- **Secure development lifecycle (SDLC)** requirements that exceed current industry norms.
- **Mandatory vulnerability handling and coordinated disclosure**, which are inconsistently implemented across manufacturers.
- **Secure update mechanisms**, including anti-rollback protections and cryptographic verification, which are not universally deployed.
- **SBOM transparency**, which is rarely provided in the PV sector.
- **Comprehensive security documentation**, which is often incomplete or proprietary.

The gap between CRA expectations and existing practices creates uncertainty and increases compliance costs, particularly for manufacturers with legacy product lines.

4.3. Lack of Harmonized Conformity Assessment Procedures

Without a sector-specific standard, conformity assessment bodies face significant challenges:

 doi:10.20944/preprints202603.1601.v1

- There is no agreed-upon test methodology for evaluating secure boot, secure update, or interface protection in PV inverters.
- Laboratories lack inverter-specific threat models and attack scenarios.
- CRA requires evidence of lifecycle processes, but there is no standardized way to audit inverter development pipelines, supply-chain controls, or vulnerability management workflows.
- Cloud-connected services associated with inverters fall within CRA scope, yet no guidance exists on how to evaluate their security in conjunction with the physical device.

This absence of harmonized procedures risks inconsistent assessments and divergent interpretations across EU member states.

4.4. Technical Complexity of PV Inverter Architectures

PV inverters present unique technical characteristics that complicate CRA compliance:

- **Multiple communication interfaces** (Ethernet, RS485, CAN, Wi-Fi, LTE) with varying security properties.
- **Dependence on cloud platforms** for monitoring, diagnostics, and fleet management.
- **Long operational lifetimes** (15–25 years), which challenge the CRA's requirements for long-term update support.
- **Integration with DER protocols** such as SunSpec Modbus, IEEE 2030.5, and IEC 61850, many of which lack robust security profiles.
- **Critical grid-support functions**, which require deterministic behavior and resilience under attack conditions.

These characteristics demand tailored technical controls that generic standards cannot provide.

4.5. Impact on Manufacturers, Operators, and Regulators

The absence of a sector-specific standard has cascading effects:

- **Manufacturers** face uncertainty in interpreting CRA requirements and risk over- or under-implementing controls.
- **Operators** cannot reliably assess whether an inverter is CRA-compliant, complicating procurement and NIS2 obligations.
- **Regulators** lack a harmonized baseline for enforcement, leading to inconsistent expectations across jurisdictions.
- **Test laboratories** cannot perform reproducible, inverter-specific evaluations.
- **The industry as a whole** risks fragmented security practices and uneven protection levels across Europe.

These gaps collectively demonstrate that the CRA, while comprehensive, cannot be effectively operationalized for PV inverters without a dedicated technical standard.

5. Limitations of Existing Standards for CRA Compliance

Although the cybersecurity landscape for industrial and IoT systems is rich with standards, guidelines, and best practices, none of the existing frameworks provides a complete or adequate foundation for demonstrating compliance with the Cyber Resilience Act (CRA) in the context of photovoltaic (PV) inverters. This section examines the most relevant standards and highlights their structural limitations when applied to CRA obligations.

5.1. IEC 62443: Comprehensive but Too Generic

The IEC 62443 series is widely regarded as the most mature framework for industrial cybersecurity. However, its applicability to CRA compliance for PV inverters is limited by several factors:

 doi:10.20944/preprints202603.1601.v1

- **Scope mismatch**: IEC 62443 is designed for industrial automation and control systems (IACS), not for distributed energy resources (DER) with long lifecycles, cloud dependencies, and consumer-facing interfaces.
- **Lack of product-specific requirements**: IEC 62443-4-1 and 4-2 define secure development and component requirements, but they do not address inverter-specific interfaces, telemetry workflows, or grid-support functions.
- **No CRA-aligned documentation obligations**: The standard does not require SBOMs, vulnerability disclosure processes, or the detailed security documentation mandated by the CRA.
- **Not harmonized for CRA**: Even if technically relevant, IEC 62443 does not provide presumption of conformity under the CRA.

As a result, IEC 62443 can serve as a useful reference but cannot be used as a standalone compliance pathway.

5.2. ETSI EN 303 645: Strong Baseline, Wrong Domain

ETSI EN 303 645 is the leading cybersecurity baseline for consumer IoT devices. While it introduces valuable principles—such as no default passwords, secure update mechanisms, and vulnerability disclosure—its limitations for PV inverters are significant:

- **Consumer IoT focus**: The standard does not address industrial communication protocols, DER control functions, or grid-support requirements.
- **Insufficient lifecycle depth**: CRA requires extensive lifecycle obligations (monitoring, patching, documentation) that exceed the scope of EN 303 645.
- **No conformity assessment framework**: The standard lacks the structured evidence and testing methodology required for CRA compliance.
- **Not aligned with inverter architectures**: It does not cover secure boot, firmware integrity, or multi-interface boundary protection at the depth required for PV inverters.

Thus, while conceptually aligned with CRA principles, EN 303 645 is not technically sufficient.

5.3. IEEE 1547: Interoperability Without Cybersecurity

IEEE 1547 defines interoperability and grid-support requirements for DER, including PV inverters. However:

- **Cybersecurity is explicitly out of scope**: The standard focuses on electrical and communication interoperability, not security.
- **No secure update, secure boot, or vulnerability management requirements**.
- **No lifecycle or documentation obligations**.
- **No provisions for cloud-connected services**, which are central to modern inverter architectures.

IEEE 1547 is essential for grid integration but irrelevant for CRA compliance.

5.4. UL 2941: DER-Focused but Incomplete

UL 2941 is one of the few standards specifically addressing cybersecurity for distributed energy resources. However:

- **It is not aligned with CRA lifecycle requirements**, such as vulnerability disclosure, SBOM, or long-term update obligations.
- **It lacks detailed conformity assessment procedures** compatible with EU regulatory frameworks.
- **It focuses on technical controls but not on documentation**, which is a core CRA requirement.
- **It is not harmonized in Europe**, meaning it cannot provide presumption of conformity.

UL 2941 is valuable but insufficient as a CRA compliance mechanism.

 doi:10.20944/preprints202603.1601.v1

5.5. NISTIR 8259 and Related U.S. Frameworks: Useful but Non-Binding

NISTIR 8259 provides a strong IoT cybersecurity baseline, but:

- **It is voluntary**, except for U.S. federal procurement.
- **It does not address inverter-specific architectures or DER protocols**.
- **It lacks CRA-aligned conformity assessment and documentation requirements**.
- **It does not cover secure boot, anti-rollback, or firmware integrity at the depth required for critical energy systems**.

NIST frameworks can inspire best practices but cannot substitute for a CRA-aligned standard.

5.6. Summary of Limitations

Across all existing standards, several structural gaps remain:

- No standard covers the full CRA lifecycle obligations (monitoring, disclosure, updates, documentation).
- No standard provides inverter-specific technical controls for interfaces, telemetry, cloud dependencies, and grid-support functions.
- No standard includes CRA-aligned conformity assessment procedures.
- No standard is harmonized for CRA presumption of conformity.
- No standard integrates security, privacy, and resilience in a unified framework, as required for modern PV inverters.

These limitations collectively demonstrate that the current standards landscape is insufficient for CRA compliance and that a dedicated sectoral standard—such as IEC 6XXXX-1—is necessary to bridge the gap.

Table 1. Comparison of Existing Cybersecurity Standards Against CRA Requirements for PV Inverters.

Scope	Industrial automation & control systems	Consumer IoT	DER interoperability	DER cybersecurity	All products with digital elements	None fully aligned with inverter architectures
Product specificity	Generic components	Consumer devices	Electrical/communication behavior	DER devices	Requires product-specific controls	No inverter-specific standard exists
Secure development (SDLC)	✓ Partial (4-1)	✓ Basic	✗	✓ Partial	✓ Mandatory	None covers full lifecycle for inverters
Supply-chain security	✓ Partial	✗	✗	✓ Partial	✓ Mandatory	No standard defines inverter

 doi:10.20944/preprints202603.1601.v1

						supply-chain controls
Secure boot / firmware integrity	✓ High-level	✓ Basic	✗	✓ Partial	✓ Mandatory	No inverter-specific requirements
Secure update / anti-rollback	✓ High-level	✓ Basic	✗	✓ Partial	✓ Mandatory	No standard defines update requirements for long-lived DER
Authentication & access control	✓ Strong	✓ Basic	✗	✓ Partial	✓ Mandatory	No multi-interface inverter guidance
Interface protection (Ethernet, RS485, CAN, Wi-Fi, LTE)	✓ Generic	✓ IoT-focused	✗	✓ Partial	✓ Mandatory	No standard covers all inverter interfaces
DER protocol security (Modbus, 2030.5, 61850)	✗	✗	✗	✓ Partial	✓ Required implicitly	No standard defines protocol-specific controls
Cloud service security	✓ Generic	✓ Basic	✗	✓ Partial	✓ Mandatory	No inverter-cloud integration guidance
Telemetry integrity & confidentiality	✓ Generic	✓ Basic	✗	✓ Partial	✓ Mandatory	No inverter-specific telemetry requirements
Logging & monitoring	✓ Strong	✓ Basic	✗	✓ Partial	✓ Mandatory	No inverter-spec

 doi:10.20944/preprints202603.1601.v1

						ific logging guidance
Vulnerability handling / disclosure	✓ High-level	✓ Basic	✗	✓ Partial	✓ Mandatory	None aligned with CRA timelines
SBOM transparency	✗	✗	✗	✗	✓ Mandatory	No standard includes SBOM requirements
Documentation requirements	✓ Partial	✓ Minimal	✗	✓ Partial	✓ Extensive	No standard meets CRA documentation depth
Conformity assessment	✓ Mature	✗	✗	✓ Partial	✓ Required	No inverter-specific assessment methodology
Harmonization potential under CRA	Low	Low	None	Low	—	None can provide presumption of conformity
Overall suitability for PV inverter CRA compliance	**Medium–Low**	**Low**	**None**	**Medium–Low**	**High bar**	**A dedicated standard is required**

6. The Case for a Dedicated PV Inverter Cybersecurity Standard

The regulatory and technical gaps identified in the previous sections reveal a fundamental misalignment between the Cyber Resilience Act (CRA) and the current standards landscape for photovoltaic (PV) inverters. While the CRA establishes essential cybersecurity requirements for all products with digital elements, it does not prescribe how these requirements should be implemented in specific sectors. For PV inverters—complex cyber-physical systems with long operational lifetimes, diverse communication interfaces, and critical grid-support functions—this absence of sector-specific

 doi:10.20944/preprints202603.1601.v1

guidance creates a structural barrier to compliance. A dedicated cybersecurity standard tailored to PV inverters is therefore not merely beneficial but essential for operationalizing the CRA.

6.1. Unique Characteristics of PV Inverters Require Tailored Controls

PV inverters differ significantly from typical IoT or industrial devices in ways that directly affect cybersecurity requirements:

- **Long lifetimes (15–25 years)** demand update mechanisms and vulnerability management processes far beyond those of consumer electronics.
- **Multiple communication interfaces** (Ethernet, RS485, CAN, Wi-Fi, LTE) introduce heterogeneous attack surfaces that require interface-specific protections.
- **Dependence on cloud services** for monitoring, diagnostics, and fleet management means that cybersecurity must extend beyond the device to include remote platforms.
- **Grid-support functions** (e.g., voltage regulation, frequency response, curtailment) require deterministic behavior and resilience under attack conditions.
- **Integration with DER protocols** such as SunSpec Modbus, IEEE 2030.5, and IEC 61850 introduces protocol-specific vulnerabilities not addressed in generic standards.

These characteristics make it impossible for horizontal or generic standards to provide adequate guidance for CRA compliance.

6.2. Horizontal Regulations Cannot Address Sector-Specific Needs

The CRA is intentionally technology-neutral and sector-agnostic. While this ensures broad applicability, it also means that:

- The CRA does **not** define how to secure inverter firmware, telemetry workflows, or DER communication protocols.
- The CRA does **not** specify how to evaluate secure boot, anti-rollback, or firmware integrity in inverter architectures.
- The CRA does **not** address the operational constraints of grid-connected DER, such as deterministic control or safety-critical fallback modes.
- The CRA does **not** provide conformity assessment procedures tailored to inverter testing environments.

Without a sector-specific standard, manufacturers must interpret CRA requirements independently, leading to inconsistent implementations and unverifiable compliance claims.

6.3. A Dedicated Standard Enables Presumption of Conformity

Under the CRA, manufacturers can demonstrate compliance through **harmonized standards**. A dedicated PV inverter cybersecurity standard—once harmonized—would:

- Provide **presumption of conformity**, reducing regulatory uncertainty.
- Establish **uniform technical requirements** across all manufacturers.
- Enable **consistent conformity assessment** by test laboratories.
- Reduce compliance costs by eliminating the need for custom interpretations.
- Support regulators in enforcing **consistent security baselines** across the EU.

This is particularly important for PV inverters, where the absence of harmonized standards currently prevents manufacturers from accessing a clear compliance pathway.

6.4. Benefits for Manufacturers, Operators, and Regulators

A dedicated standard would create value across the entire PV ecosystem:

For manufacturers

- Clear, actionable requirements aligned with CRA obligations.

 doi:10.20944/preprints202603.1601.v1

- Reduced ambiguity in secure development, update mechanisms, and vulnerability handling.
- A structured framework for documentation, SBOM, and lifecycle processes.

For operators and integrators

- Confidence that purchased inverters meet a consistent security baseline.
- Simplified procurement aligned with NIS2 obligations.
- Improved interoperability and reduced integration risk.

For regulators and conformity assessment bodies

- A harmonized basis for evaluating CRA compliance.
- Reduced fragmentation and inconsistent interpretations.
- A clear reference for enforcement and market surveillance.

6.5. Alignment With International Trends

The need for sector-specific cybersecurity standards is increasingly recognized worldwide:

- The United States has UL 2941 for DER cybersecurity.
- Japan's CPSF and smart-grid guidelines include device-specific requirements.
- Brazil's ONS/ANEEL frameworks impose cybersecurity obligations on DER operators.

Europe, however, lacks an equivalent standard for PV inverters. A dedicated standard would position the EU as a global leader in DER cybersecurity and support international harmonization efforts.

6.6. Summary

The case for a dedicated PV inverter cybersecurity standard is clear:

- Existing standards are insufficient for CRA compliance.
- PV inverters have unique technical and operational characteristics that require tailored controls.
- A sector-specific standard would provide presumption of conformity, reduce compliance costs, and harmonize security practices.
- IEC 6XXXX-1 offers a viable foundation for such a standard.

A dedicated standard is therefore essential to bridge the gap between CRA obligations and the practical realities of inverter design, deployment, and lifecycle management.

7. IEC 6XXXX-1 as a Candidate Sectoral Standard

Figure 1 provides a high-level overview of the PV inverter cybersecurity ecosystem and the CRA control points that a sectoral standard must address.

 doi:10.20944/preprints202603.1601.v1

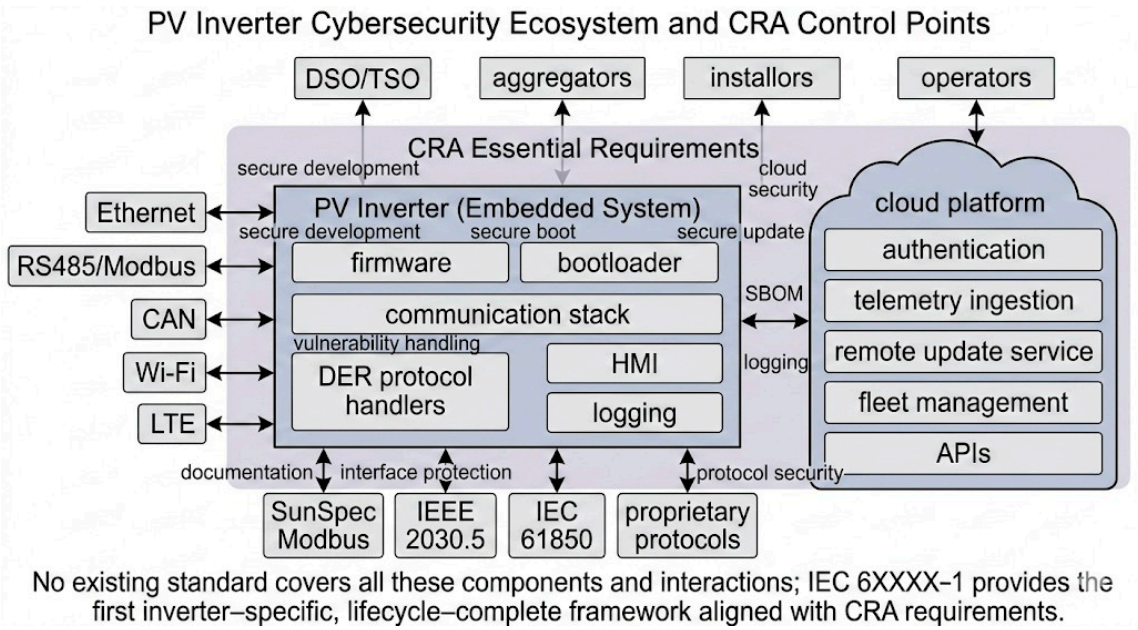

Figure 1. PV Inverter Cybersecurity Ecosystem and CRA Control Points.

Although no formal proposal currently exists within IEC for a cybersecurity standard dedicated to PV inverters, a preliminary working-level concept—informally referred to as IEC 6XXXX-1 "Cybersecurity of Utility-Interconnected PV Inverters"—could offer a useful model for exploring how such a standard might be structured. The following subsections do not describe an existing standard, but rather the set of technical requirements that a future sector-specific standard should consider in order to meet the obligations of the CRA.

The analysis presented thus far demonstrates that existing cybersecurity standards are insufficient to operationalize CRA compliance for photovoltaic (PV) inverters. In this context, the IEC 6XXXX-1 concept does not represent an approved project, but rather a plausible framework illustrating how a dedicated standard could bridge the gap between CRA obligations and the technical realities of inverter design, deployment, and lifecycle management.

7.1. Structure and Scope Aligned With CRA Requirements

In its conceptual form, IEC 6XXXX-1 is envisioned as covering the full cybersecurity lifecycle of PV inverters, from development to decommissioning. Its proposed structure mirrors the CRA's essential requirements, providing a clear mapping between regulatory obligations and technical controls. Key sections *could* include:

- Section 7 — Security lifecycle requirements, covering secure development, supply chain security, commissioning, operation, vulnerability handling, and end-of-life processes.
- Section 8 — General cybersecurity requirements, defining technical controls such as access control, authentication, secure communication, secure boot, secure update, firmware integrity, logging, and boundary protection.
- Section 9 — Documentation requirements, including SBOM, configuration guidance, update policies, and evidence for conformity assessment.
- Section 10 — Conformity assessment framework, outlining the evidence manufacturers must provide and the role of test laboratories.

If developed, such a structure could offer a comprehensive framework for implementing the CRA in PV inverters.

7.2. Inverter-Specific Technical Controls

 doi:10.20944/preprints202603.1601.v1

The conceptual IEC 6XXXX-1 framework also anticipates technical requirements tailored to the unique characteristics of PV inverters, including:

- Multi-interface protection for Ethernet, RS485, CAN, Wi-Fi, LTE, and fieldbus protocols.
- Secure telemetry workflows, including integrity protection and confidentiality of operational data.
- Cloud-connected architectures, addressing authentication, access control, and data governance for remote monitoring platforms.
- Grid-support functions, ensuring that cybersecurity controls do not compromise deterministic behavior or safety-critical operations.
- Combined systems, such as inverter + gateway/dongle configurations, which introduce additional attack surfaces.

These inverter-specific provisions illustrate how a future standard could fill critical gaps left by IEC 62443, ETSI EN 303 645, and UL 2941.

7.3. Lifecycle Coverage Beyond Existing Standards

CRA compliance requires manufacturers to implement cybersecurity across the entire product lifecycle. **The IEC 6XXXX-1 concept envisions addressing this comprehensively**, including:

- Secure development (SDLC): threat modeling, secure coding, code review, and security testing.
- Supply chain security: component verification, firmware provenance, and manufacturing integrity.
- Commissioning and onboarding: secure enrollment, credential provisioning, and interface hardening.
- Operation and maintenance: secure remote access, logging, monitoring, and configuration management.
- Vulnerability handling: coordinated disclosure, patch management, and remediation timelines.
- End of life: secure decommissioning and data sanitization.

No existing standard provides this level of lifecycle completeness for PV inverters, which highlights the potential value of such a framework.

7.4. Documentation and Transparency Requirements

The CRA places strong emphasis on transparency, including SBOMs, security documentation, and update policies. **A future IEC 6XXXX-1 standard could directly address these needs**, including:

- SBOM and component transparency (Section 9.2)
- Security configuration documentation (Section 9.4)
- Update and patching policy (Section 9.3)
- Evidence for conformity assessment (Section 9.5)

These provisions illustrate how a sectoral standard could support CRA documentation and post-market monitoring obligations.

7.5. Conformity Assessment Framework

One of the most significant contributions that **a future IEC 6XXXX-1 standard podría ofrecer** is a structured conformity assessment framework, providing:

- Clear evidence requirements for manufacturers.
- Defined roles for test laboratories.
- Applicability across inverter categories (residential, C&I, utility-scale).
- A basis for harmonization under the CRA.

Such a framework would fill a critical gap, as conformity assessment bodies currently lack tools to evaluate CRA compliance for PV inverters.

 doi:10.20944/preprints202603.1601.v1

7.6. Compatibility With Existing Standards and Grid Codes

The conceptual IEC 6XXXX-1 framework is designed to complement—not replace—existing standards, including:

- IEC 62443: foundational principles for secure development and component security.
- ETSI EN 303 645: baseline IoT security practices.
- IEEE 1547: interoperability and grid-support functions.
- UL 2941: DER-specific insights.

A future Annex B could map these standards explicitly, ensuring interoperability and avoiding duplication.

7.7. A Viable Path Toward CRA Harmonization

Given its structure, scope, and alignment with CRA requirements, **a formally developed IEC 6XXXX-1 standard podría convertirse en un candidato sólido para armonización bajo el CRA**. Its adoption could:

- Provide manufacturers with presumption of conformity.
- Enable consistent testing and certification.
- Reduce compliance costs and ambiguity.
- Strengthen the cybersecurity posture of Europe's PV infrastructure.
- Support NIS2 obligations for operators and grid entities.

7.8. Summary

Although still only a conceptual framework, IEC 6XXXX-1 illustrates how a comprehensive, inverter-specific, lifecycle-complete standard could address the gaps preventing CRA compliance in the PV sector. If formally developed and adopted, such a standard would provide the clarity, consistency, and technical depth required to secure Europe's rapidly expanding solar ecosystem.

8. Mapping CRA Requirements to IEC 6XXXX-1 Controls

This section illustrates how a possible future sector-specific IEC standard could operationalize CRA obligations for PV inverters.

A central challenge for manufacturers seeking to comply with the Cyber Resilience Act (CRA) is the absence of a sector-specific standard that translates the CRA's horizontal obligations into concrete, verifiable requirements for photovoltaic (PV) inverters. The proposed IEC 6XXXX-1 addresses this gap by providing a structured set of lifecycle processes, technical controls, and documentation requirements that align closely with the CRA's essential cybersecurity requirements. This section presents a systematic mapping between CRA obligations and the corresponding provisions in IEC 6XXXX-1, demonstrating how the proposed standard can serve as a practical implementation framework for CRA compliance.

8.1. Secure Development and Lifecycle Processes

The CRA mandates that manufacturers implement secure development practices, conduct risk assessments, and maintain cybersecurity throughout the product lifecycle. IEC 6XXXX-1 could provide direct support for these obligations:

- CRA Requirement: Secure development lifecycle (SDLC) → IEC 6XXXX-1 Section 7.1 — Secure development Includes threat modeling, secure coding, code review, and security testing.
- CRA Requirement: Supply-chain security → Section 7.2 — Supply chain and manufacturing security Covers component verification, firmware provenance, and manufacturing integrity.
- CRA Requirement: Secure commissioning and onboarding → Section 7.3 — Commissioning and onboarding Defines secure enrollment, credential provisioning, and interface hardening.

 doi:10.20944/preprints202603.1601.v1

- CRA Requirement: Post-market monitoring and vulnerability handling → Section 7.5 — Vulnerability handling and disclosure Aligns with CRA obligations for coordinated vulnerability disclosure and remediation timelines.
- CRA Requirement: End-of-life security → Section 7.6 — Decommissioning and end-of-life Addresses secure data erasure and device retirement.

8.2. Technical Security Measures

The CRA requires manufacturers to implement technical controls that ensure the confidentiality, integrity, and availability of digital components. IEC 6XXXX-1 provides inverter-specific implementations of these controls:

- CRA Requirement: Authentication and access control → Section 8.1 — Access control and identity management → Section 8.2 — Authentication mechanisms
- CRA Requirement: Credential protection → Section 8.3 — Credential management
- CRA Requirement: Secure communication → Section 8.4 — Secure communication Covers encryption, integrity protection, and protocol hardening.
- CRA Requirement: Protection against unauthorized firmware modification → Section 8.5 — Secure boot → Section 8.7 — Application and firmware security
- CRA Requirement: Secure update mechanisms → Section 8.6 — Secure update Includes signature verification, anti-rollback, and update provenance.
- CRA Requirement: System integrity and resilience → Section 8.8 — System integrity protection → Section 8.13 — Resilience and fail-safe behaviour
- CRA Requirement: Logging and monitoring → Section 8.10 — Logging and monitoring
- CRA Requirement: Protection of cryptographic material → Section 8.11 — Digital certificates and cryptographic material
- CRA Requirement: Interface hardening and boundary protection → Section 8.12 — Interface exposure and boundary protection

These mappings demonstrate that IEC 6XXXX-1 provides a comprehensive set of technical controls tailored to inverter architectures and operational contexts.

8.3. Documentation and Transparency Requirements

The CRA places strong emphasis on transparency, requiring manufacturers to provide documentation that enables users and regulators to understand the security properties of the product. IEC 6XXXX-1 directly supports these obligations:

- CRA Requirement: Security documentation for users and operators → Section 9.1 — Security documentation for operators
- CRA Requirement: Software Bill of Materials (SBOM) → Section 9.2 — SBOM and component transparency
- CRA Requirement: Update and patching policy → Section 9.3 — Update and patching policy
- CRA Requirement: Secure configuration guidance → Section 9.4 — Security configuration documentation
- CRA Requirement: Evidence for conformity assessment → Section 9.5 — Evidence for conformity assessment

These provisions ensure that manufacturers can meet the CRA's transparency and documentation obligations in a structured and verifiable manner.

8.4. Conformity Assessment and Verification

The CRA requires manufacturers to demonstrate compliance through internal controls or third-party assessment, depending on product classification. IEC 6XXXX-1 provides a dedicated conformity assessment framework:

 doi:10.20944/preprints202603.1601.v1

- CRA Requirement: Demonstration of conformity → Section 10.3 — Evidence required from manufacturers
- CRA Requirement: Role of notified bodies and test laboratories → Section 10.4 — Role of test laboratories
- CRA Requirement: Applicability across product categories → Section 10.5 — Applicability across inverter categories

This framework enables consistent, reproducible evaluation of CRA compliance for PV inverters.

8.5. Summary Mapping Table

To clarify how the proposed conceptual structure of IEC 6XXXX-1 aligns with the Cyber Resilience Act (CRA), Table 2 provides a consolidated mapping between the CRA's essential requirements and the corresponding sections of this possible future sector-specific IEC standard. The table highlights that the conceptual framework offers full coverage across lifecycle processes, technical controls, documentation, and conformity assessment, illustrating how a future IEC standard—if formally developed—could operationalize CRA obligations for PV inverters.

Table 2. Alignment Between CRA Requirements and the possible IEC 6XXXX-1 Conceptual Framework.

Secure development	7.1	Full
Supply-chain security	7.2	Full
Commissioning security	7.3	Full
Vulnerability handling	7.5	Full
End-of-life security	7.6	Full
Authentication & access control	8.1–8.2	Full
Credential management	8.3	Full
Secure communication	8.4	Full
Secure boot	8.5	Full
Secure update	8.6	Full
Firmware integrity	8.7–8.8	Full
Logging & monitoring	8.10	Full
Cryptographic material	8.11	Full
Interface protection	8.12	Full
Resilience	8.13	Full
SBOM	9.2	Full
Documentation	9.1–9.5	Full
Conformity assessment	10	Full

8.6. Conclusion

The mapping demonstrates that IEC 6XXXX-1 provides a comprehensive, inverter-specific framework that operationalizes the CRA's essential requirements. By covering lifecycle processes, technical controls, documentation, and conformity assessment, the proposed standard offers a clear and harmonized pathway for manufacturers to achieve CRA compliance.

9. Discussion: Implications for the PV Industry

 doi:10.20944/preprints202603.1601.v1

The introduction of the Cyber Resilience Act (CRA), combined with the absence of a sector-specific cybersecurity standard for photovoltaic (PV) inverters, creates a pivotal moment for the European solar industry. The findings of this paper reveal that the current standards landscape is insufficient to support CRA compliance and that the proposed IEC 6XXXX-1 offers a viable path forward. This section discusses the broader implications of these findings for manufacturers, operators, regulators, and the long-term resilience of Europe's distributed energy ecosystem.

9.1. Implications for Manufacturers

For inverter manufacturers, the CRA represents both a challenge and an opportunity.

Challenges

- **Increased compliance burden**: Manufacturers must implement secure development practices, vulnerability handling processes, and secure update mechanisms that many have not previously formalized.
- **Legacy product constraints**: Older inverter models may lack the hardware capabilities (e.g., secure elements, cryptographic accelerators) required to meet CRA technical controls.
- **Cloud service alignment**: CRA obligations extend to associated cloud platforms, requiring manufacturers to harden authentication, access control, and data governance mechanisms.
- **Documentation requirements**: SBOMs, update policies, and security configuration guides must be produced and maintained throughout the product lifecycle.

Opportunities

- **Competitive differentiation**: Manufacturers that adopt IEC 6XXXX-1 early can position themselves as leaders in secure and compliant inverter design.
- **Reduced long-term costs**: A harmonized standard reduces the need for custom compliance interpretations and repeated audits.
- **Improved product quality**: Secure development practices and structured lifecycle processes lead to more robust and reliable products.

In this sense, IEC 6XXXX-1 provides a roadmap that reduces uncertainty and accelerates compliance readiness.

9.2. Implications for Operators, Installers, and Integrators

Operators of PV plants—whether residential, commercial, or utility-scale—face increasing cybersecurity obligations under NIS2 and national grid codes. The lack of a sector-specific standard complicates procurement and risk assessment.

Key implications

- **Procurement uncertainty**: Without a harmonized standard, operators cannot easily determine whether an inverter meets CRA requirements.
- **Integration complexity**: Inconsistent security implementations across manufacturers increase integration risks and operational overhead.
- **Operational risk**: Weak security controls in inverters can expose operators to cyberattacks that disrupt generation, compromise telemetry, or affect grid stability.
- **Regulatory exposure**: Operators may be held responsible for deploying insecure equipment, especially under NIS2.

A dedicated standard such as IEC 6XXXX-1 would provide operators with a clear benchmark for evaluating inverter security and compliance.

9.3. Implications for Regulators and Conformity Assessment Bodies

Regulators and notified bodies face significant challenges in enforcing the CRA without sector-specific guidance.

Regulatory implications

 doi:10.20944/preprints202603.1601.v1

- **Lack of harmonized criteria**: Without a dedicated standard, regulators must interpret CRA requirements on a case-by-case basis, leading to inconsistent enforcement.
- **Market fragmentation**: Divergent national interpretations risk creating uneven security baselines across EU member states.
- **Increased oversight burden**: Regulators must evaluate complex technical claims without a standardized reference.

Assessment implications

- **No reproducible test methodology**: Laboratories lack inverter-specific procedures for evaluating secure boot, secure update, interface protection, or cloud dependencies.
- **Difficulty verifying lifecycle processes**: CRA requires evidence of secure development, vulnerability handling, and post-market monitoring, but no standard defines how to audit these processes for PV inverters.

IEC 6XXXX-1 would provide the harmonized foundation needed for consistent conformity assessment and regulatory oversight.

9.4. Implications for Grid Stability and Energy Resilience

PV inverters are increasingly central to grid stability, providing voltage regulation, frequency support, and reactive power control. Cybersecurity weaknesses in these devices can have systemic consequences.

Risks without a dedicated standard

- **Coordinated disconnection attacks** could destabilize local or regional grids.
- **Manipulation of telemetry** could mislead grid operators or aggregators.
- **Compromise of cloud platforms** could affect thousands of devices simultaneously.
- **Exploitation of insecure DER protocols** could propagate across heterogeneous fleets.

A sector-specific standard strengthens the resilience of distributed energy resources and supports Europe's broader energy transition goals.

9.5. Implications for International Harmonization

The PV industry operates globally, and cybersecurity requirements must align across regions to avoid fragmentation.

- The United States has UL 2941 but lacks CRA-equivalent lifecycle obligations.
- Japan's CPSF and smart-grid guidelines provide device-specific security requirements.
- Brazil's ONS/ANEEL frameworks regulate DER operation but not product cybersecurity.

IEC 6XXXX-1 could serve as a **global reference**, enabling international harmonization and reducing compliance complexity for multinational manufacturers.

9.6. Summary

The implications of the CRA for the PV industry are profound. Without a dedicated cybersecurity standard, manufacturers face uncertainty, operators face risk, regulators face inconsistency, and the energy system faces avoidable vulnerabilities. IEC 6XXXX-1 provides a structured, comprehensive, and technically grounded solution that can harmonize security practices, reduce compliance costs, and strengthen the resilience of Europe's solar infrastructure.

10. Conclusion

The Cyber Resilience Act (CRA) represents a transformative shift in how cybersecurity is regulated across the European Union. By imposing mandatory, lifecycle-wide obligations on all products with digital elements, the CRA establishes a new baseline for security, transparency, and accountability. For photovoltaic (PV) inverters—now central components of Europe's distributed energy infrastructure—these obligations are both necessary and overdue. Yet the analysis presented

 doi:10.20944/preprints202603.1601.v1

in this paper demonstrates that the current standards landscape is fundamentally inadequate to support CRA compliance in the PV sector.

Existing frameworks such as IEC 62443, ETSI EN 303 645, IEEE 1547, and UL 2941 provide valuable guidance but fail to address the unique architectural, operational, and lifecycle characteristics of PV inverters. None of these standards offers the inverter-specific technical controls, documentation requirements, or conformity assessment procedures needed to operationalize CRA obligations. As a result, manufacturers face ambiguity, regulators lack harmonized criteria, and operators cannot reliably assess the security posture of deployed equipment.

In this context, a preliminary working-level concept informally referred to as IEC 6XXXX-1 — *Cybersecurity of Utility-Interconnected PV Inverters* — could provide a useful illustration of what a future sectoral standard could encompass. This concept does not represent an existing or formally proposed IEC standard; rather, it outlines the technical depth, lifecycle coverage, and CRA-aligned structure that a dedicated PV inverter cybersecurity standard would need to include. By integrating secure development practices, inverter-specific technical controls, comprehensive documentation requirements, and a structured conformity assessment framework, such a standard could fill the critical gap identified in this study.

If formally developed, a future IEC 6XXXX-1-type standard could offer a complete and actionable pathway for CRA compliance, enabling manufacturers to demonstrate conformity, supporting regulators with harmonized assessment criteria, and providing operators with a reliable basis for evaluating the cybersecurity posture of deployed equipment. Its alignment with CRA essential requirements suggests that a sector-specific standard is not merely beneficial but essential for ensuring consistent, verifiable, and harmonized security across the European PV ecosystem.

The adoption of such a standard as a harmonized CRA standard would deliver significant benefits: reduced compliance costs for manufacturers, clearer procurement criteria for operators, consistent evaluation procedures for test laboratories, and stronger cybersecurity baselines for Europe's rapidly expanding solar infrastructure. Moreover, it would position the European Union as a global leader in DER cybersecurity and support international harmonization efforts.

In conclusion, the PV industry cannot meet CRA obligations without a dedicated cybersecurity standard. While IEC 6XXXX-1 remains only a conceptual framework, it demonstrates the structure and content that a future sectoral standard should incorporate. The formal development of such a standard should therefore be considered a strategic priority for manufacturers, regulators, and standards bodies committed to building a resilient, secure, and sustainable energy future.

References

1. European Union Agency for Cybersecurity (ENISA). *Cybersecurity for Distributed Energy Resources: Threat Landscape and Recommendations*. ENISA Publications, 2023.
2. SunSpec Alliance. *SunSpec Modbus Information Model*. SunSpec Technical Specifications, 2023.
3. IEC 61850 Series. *Communication Networks and Systems for Power Utility Automation*. International Electrotechnical Commission (IEC).
4. European Commission. *NIS2 Directive (Directive (EU) 2022/2555) on Measures for a High Common Level of Cybersecurity Across the Union*. Brussels, 2022.
5. European Commission. *Regulation (EU) 2024/… on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act)*. Brussels, 2024.
6. European Commission. *Guidance on the Implementation of the Cyber Resilience Act*. Brussels, 2024.
7. ENISA. *SBOM: Software Bill of Materials — Challenges and Recommendations*. ENISA Publications, 2022.
8. ISO/IEC 30111. *Vulnerability Handling Processes*. International Organization for Standardization (ISO), 2019.
9. ISO/IEC 29147. *Vulnerability Disclosure*. International Organization for Standardization (ISO), 2018.
10. IEC 62443 Series. *Industrial Communication Networks – IT Security for Networks and Systems*. International Electrotechnical Commission (IEC), Geneva.
11. ETSI EN 303 645. *Cyber Security for Consumer Internet of Things: Baseline Requirements*. European Telecommunications Standards Institute (ETSI), 2020.

 doi:10.20944/preprints202603.1601.v1

12. IEEE 1547-2018. *Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*. Institute of Electrical and Electronics Engineers (IEEE), 2018.
13. UL 2941. *Cybersecurity for Distributed Energy Resources*. UL Standards & Engagement, 2022.
14. CENELEC. *Harmonized Standards under the Cyber Resilience Act — Roadmap and Work Programme*. CENELEC Technical Board, 2024.
15. IEC 6XXXX-1. *Cybersecurity of Utility-Interconnected PV Inverters*. IEC TC 82 WG6 Internal Working Document, 2026.