A Unified Security Baseline for Photovoltaic Inverters Integrating IEC, UL, IEEE, SunSpec and EU CRA Requirements

Vicente Salas *

Posted Date: 12 March 2026

doi: 10.20944/preprints202603.0988.v1

Keywords: cyber-physical security; photovoltaic inverters; DER cybersecurity; IoT/OT device security; Unified Security Baseline; IEC 62443 / IEC 62351; IEEE 1547 / IEEE 2030.5; SunSpec Modbus; Cyber Resilience Act (CRA); secure-by-design

 doi:10.20944/preprints202603.0988.v1

Article

A Unified Security Baseline for Photovoltaic Inverters Integrating IEC, UL, IEEE, SunSpec and EU CRA Requirements

Vicente Salas

Computer Science, IES Vista Alegre Madrid, Spain ; vsm425@educa.madrid.org

Abstract

The increasing digitalization of photovoltaic (PV) inverters and their integration into distributed energy resource (DER) ecosystems expose these devices to a rapidly expanding cyber-physical attack surface. Existing security requirements are fragmented across heterogeneous technical standards—including IEC 62443, IEC 62351, UL 2900-1, UL 1741 SB, IEEE 1547, IEEE 2030.5, and SunSpec profiles—and only partially aligned with emerging regulatory obligations such as the EU Cyber Resilience Act (CRA) and NIS2 Directive. This fragmentation complicates assurance, hinders interoperability, and leaves critical security controls inconsistently implemented across vendors and deployments. This paper introduces a Unified Security Baseline (USB) that harmonizes essential technical and lifecycle security controls for PV inverters, including secure boot, firmware signing, anti-rollback protection, strong authentication, TLS-secured communication, SBOM governance, secure over-the-air updates, and coordinated vulnerability disclosure. The USB provides a device-centric, standards-agnostic framework designed to strengthen the security posture of inverter-dominated DER environments while supporting regulatory compliance. By consolidating cross-standard requirements into a coherent baseline, this work establishes a foundation for future conformity assessment, certification efforts, and secure-by-design engineering practices in critical IoT/OT infrastructures.

Keywords: cyber-physical security; photovoltaic inverters; DER cybersecurity; IoT/OT device security; Unified Security Baseline; IEC 62443 / IEC 62351; IEEE 1547 / IEEE 2030.5; SunSpec Modbus; Cyber Resilience Act (CRA); secure-by-design

1. Introduction

The rapid digitalization of photovoltaic (PV) inverters and their integration into distributed energy resource (DER) ecosystems have transformed these devices from isolated power-electronic components into fully networked cyber-physical systems. Recent surveys highlight that modern PV and DER infrastructures increasingly rely on IP-based management interfaces, cloud-connected monitoring platforms, and standardized communication protocols, significantly expanding their cyber-physical attack surface [1–5]. As a result, the cybersecurity posture of inverter-dominated DER environments has become a critical factor for grid stability, operational resilience, and the protection of energy-related data.

Despite their growing importance, the security requirements governing PV inverter design, communication, and lifecycle processes remain fragmented across heterogeneous technical standards and regulatory frameworks. Industrial and power-system security standards such as **IEC 62443-4-1/-4-2** and the **IEC 62351** series provide mature building blocks for secure-by-design engineering and communication protection [6–7]. In parallel, DER-specific standards—including **IEEE 1547.3-2023**, **UL 2900-1**, **UL 1741 SB**, and SunSpec Modbus profiles—define interoperability and protocol semantics for inverter-based resources [8–11]. However, these documents differ widely in scope, terminology, and security coverage. Essential controls such as secure boot, firmware

 doi:10.20944/preprints202603.0988.v1

integrity protection, certificate lifecycle management, SBOM governance, and coordinated vulnerability disclosure are inconsistently specified or entirely absent across DER-focused standards.

Regulatory developments add further complexity. The **EU Cyber Resilience Act (CRA)** and the **NIS2 Directive** introduce binding obligations for connected products, including secure development practices, vulnerability handling, secure update mechanisms, and supply-chain transparency [12–13]. Complementary guidance from ENISA and NTIA emphasizes SBOM governance, firmware integrity, and lifecycle security for energy-sector devices [14–15]. Yet these regulations do not provide device-level technical baselines, leaving manufacturers and operators to reconcile overlapping and sometimes diverging requirements across standards and jurisdictions.

This fragmented landscape complicates assurance, hinders interoperability, and creates uncertainty for vendors seeking compliance with both technical and regulatory expectations. It also exposes inverter-dominated DER environments to cyber-physical risks, as attackers can exploit protocol inconsistencies, weak firmware protections, or insufficient lifecycle governance to compromise devices and disrupt grid operations. Prior analyses and testbed studies have demonstrated that compromised inverters can manipulate grid parameters, propagate through supply-chain vulnerabilities, or serve as pivot points into OT networks [16–19].

To address these challenges, this paper introduces a **Unified Security Baseline (USB)** that consolidates essential technical and lifecycle security controls for PV inverters. The USB harmonizes requirements across IEC, UL, IEEE, SunSpec, and EU regulatory frameworks, providing a device-centric, standards-agnostic foundation for secure-by-design engineering, conformity assessment, and long-term lifecycle management in critical IoT/OT infrastructures. By aligning cross-standard expectations and addressing persistent security gaps, the USB aims to strengthen the cyber-physical resilience of inverter-dominated DER environments and support future certification and regulatory compliance efforts [20].

2. Background and Motivation

The security posture of photovoltaic (PV) inverters has become a critical concern as these devices evolve into fully networked cyber-physical components within distributed energy resource (DER) ecosystems. Modern inverters expose IP-based management interfaces, cloud-connected monitoring platforms, and standardized communication protocols, placing them at the intersection of IoT and operational technology (OT). This convergence expands their attack surface and introduces new risks for grid stability, data privacy, and system-level resilience.

A diverse set of technical standards governs different aspects of inverter functionality and security. Industrial and power-system cybersecurity standards such as IEC 62443-4-1/-4-2 and IEC 62351 provide mature requirements for secure development, component hardening, and communication protection. In parallel, DER-specific standards—including IEEE 1547, IEEE 2030.5, UL 2900-1, UL 1741 SB, and SunSpec Modbus profiles—define interoperability, protocol semantics, and in some cases optional security mechanisms. However, these documents differ significantly in scope and depth. Essential device-level controls such as secure boot, firmware signing, anti-rollback protection, certificate lifecycle management, logging, and SBOM governance are inconsistently specified or entirely absent across DER-focused standards.

Regulatory developments add further complexity. The EU Cyber Resilience Act (CRA), NIS2 Directive, and related supply-chain security initiatives introduce binding obligations for connected products, including secure-by-design development, vulnerability disclosure, secure update mechanisms, and transparency through SBOMs. Yet these regulations do not provide detailed technical baselines for PV inverters, leaving manufacturers responsible for reconciling regulatory expectations with heterogeneous and sometimes conflicting technical standards.

This fragmented landscape creates practical challenges for manufacturers, integrators, and utilities. Inconsistent security requirements hinder interoperability, complicate conformity assessment, and increase the likelihood of weak or uneven security implementations across inverter fleets. At the same time, research on DER cybersecurity has demonstrated that compromised

 doi:10.20944/preprints202603.0988.v1

inverters can be leveraged to manipulate grid parameters, disrupt protection functions, or exfiltrate sensitive operational data, underscoring the need for robust, harmonized security controls.

These factors motivate the development of a Unified Security Baseline (USB) that consolidates essential technical and lifecycle security requirements into a coherent, device-centric framework. By harmonizing cross-standard expectations and aligning them with emerging regulatory obligations, the USB aims to provide a practical foundation for secure-by-design engineering, interoperability, and long-term lifecycle governance in inverter-dominated DER environments.

3. Cross-Standard Fragmentation

The security requirements applicable to photovoltaic (PV) inverters are distributed across a heterogeneous collection of technical standards, industry specifications, and regulatory frameworks. While each document addresses specific aspects of device security, none provides a complete or coherent baseline. This fragmentation results in inconsistent protection across vendors, protocols, and deployment environments.

Industrial cybersecurity standards such as IEC 62443-4-1/-4-2 define mature requirements for secure development, component hardening, and authentication mechanisms. Power-system communication standards like IEC 62351 specify encryption, key management, and message integrity for selected protocols. However, these standards are not tailored to DER-specific communication workflows or inverter lifecycle constraints.

In contrast, DER-focused standards—including IEEE 1547, IEEE 2030.5, UL 2900-1, UL 1741 SB, and SunSpec Modbus profiles—primarily target interoperability, functional behavior, and protocol semantics. Their security coverage is uneven: some controls (e.g., TLS in IEEE 2030.5) are mandatory, while others (e.g., authentication, certificate lifecycle management, secure boot, firmware integrity) are optional, loosely defined, or entirely absent. SunSpec Modbus profiles, widely deployed in field installations, often rely on unencrypted and unauthenticated communication channels unless vendors implement proprietary extensions.

Regulatory frameworks introduce additional complexity. The EU Cyber Resilience Act (CRA) and NIS2 Directive mandate secure-by-design development, vulnerability disclosure, SBOM governance, and secure update mechanisms for connected products. Yet these regulations do not prescribe specific technical controls or protocol-level requirements, leaving manufacturers responsible for mapping regulatory obligations onto inconsistent technical standards.

This misalignment across standards and regulations creates four recurring fragmentation patterns:

Technical fragmentation: essential controls such as secure boot, firmware signing, anti-rollback protection, and logging are inconsistently specified across standards.

Communication fragmentation: encryption, authentication, and certificate management differ significantly between IEEE 2030.5, SunSpec Modbus, and legacy Modbus TCP.

Lifecycle fragmentation: secure development, SBOM governance, vulnerability disclosure, and patch management are addressed unevenly or omitted entirely.

Regulatory fragmentation: CRA and NIS2 obligations exceed the security coverage of existing DER standards, creating compliance gaps.

These inconsistencies hinder interoperability, complicate conformity assessment, and increase the likelihood of weak or uneven security implementations across inverter fleets. This motivates the need for a unified, device-centric security baseline that harmonizes cross-standard expectations and aligns them with emerging regulatory requirements.

4. Unified Security Baseline (USB)

The Unified Security Baseline (USB) consolidates essential technical and lifecycle security controls for photovoltaic (PV) inverters operating as networked IoT/OT devices. Its purpose is to harmonize fragmented requirements across IEC, UL, IEEE, SunSpec, and emerging regulatory

 doi:10.20944/preprints202603.0988.v1

frameworks, providing a coherent foundation for secure-by-design engineering, interoperability, and long-term lifecycle governance. The USB is intentionally standards-agnostic: it does not replace existing specifications but aligns their core expectations into a single, device-centric model.

4.1. Principles

The USB is built on four foundational principles:

• Completitud

The baseline must cover all critical security domains—technical, communication, and lifecycle—ensuring that no essential control (e.g., secure boot, firmware integrity, SBOM governance) is left unspecified.

• Interoperabilidad

Security controls must remain consistent across heterogeneous DER communication protocols, including SunSpec Modbus, IEEE 2030.5, and legacy Modbus TCP, avoiding inconsistent protection levels across interfaces.

• Alineamiento regulatorio

The USB integrates mandatory obligations from the EU Cyber Resilience Act (CRA), NIS2, and related supply-chain security initiatives, ensuring that device-level controls support regulatory compliance.

• Orientación al ciclo de vida

Security must extend beyond device commissioning to include secure development, vulnerability disclosure, patch management, and end-of-life processes.

4.2. USB Technical Controls

The USB defines a concise set of mandatory technical controls that address the most critical weaknesses observed across existing standards:

• Secure boot

Ensures that only authenticated, untampered firmware can execute on the device.

• Firmware signing

All firmware images must be cryptographically signed using vendor-controlled keys.

• Anti-rollback protection

Prevents downgrades to vulnerable firmware versions.

• TLS 1.3

Mandatory for all IP-based communication channels, eliminating plaintext or legacy TLS versions.

• Mutual authentication

Devices and management systems must authenticate each other using certificates or equivalent strong credentials.

• Certificate lifecycle management

Covers provisioning, renewal, revocation, and secure storage of cryptographic keys.

• Secure OTA updates

Updates must be authenticated, encrypted, integrity-protected, and logged.

• Logging and auditability

Security-relevant events must be recorded locally and/or remotely with tamper-resistant mechanisms.

• SBOM generation and maintenance

A complete software bill of materials must be produced, updated, and made available for vulnerability tracking.

• Coordinated Vulnerability Disclosure (CVD)

Manufacturers must maintain processes for reporting, triaging, and remediating vulnerabilities.

 doi:10.20944/preprints202603.0988.v1

4.3. USB Lifecycle Controls

Technical controls require supporting lifecycle processes to remain effective over time. The USB defines the following lifecycle requirements:

• Secure Development Lifecycle (SDL)

Manufacturers must adopt structured secure-by-design practices, including threat modeling, code review, and security testing.

• SBOM governance

SBOMs must be maintained throughout the product lifecycle, including updates and third-party component changes.

• Vulnerability disclosure processes

Clear channels for reporting vulnerabilities, aligned with CRA and industry best practices.

• Patch and update management

Timely delivery of security patches, with mechanisms for safe deployment and rollback prevention.

• End-of-life (EOL) security

Manufacturers must define EOL timelines, provide final security updates, and communicate risks to operators.

4.4. USB Communication Security Model

The USB harmonizes communication-security expectations across DER protocols, addressing inconsistencies that currently expose inverter fleets to cyber-physical risks.

• SunSpec secure profile

SunSpec Modbus deployments must adopt authenticated and encrypted channels, replacing legacy plaintext Modbus TCP.

• IEEE 2030.5 PKI requirements

IEEE 2030.5 integrations must rely on robust public-key infrastructures, certificate-based authentication, and strict key-lifecycle management.

• Modbus hardening

Legacy RS-485/Modbus deployments must incorporate gateway-level protections, including TLS tunneling, access control, and command filtering.

• No plaintext paths

5. Threat Model (conceptual)

The Unified Security Baseline (USB) is designed to mitigate realistic cyber-physical threats affecting photovoltaic (PV) inverters operating as networked IoT/OT devices. The threat model focuses on adversarial capabilities, attack surfaces, and potential impacts on inverter-dominated DER environments. It does not assume nation-state sophistication but considers attackers with moderate technical expertise and access to common exploitation tools.

5.1. Adversary Capabilities

The USB assumes adversaries may possess one or more of the following capabilities:

• Remote network access

Attackers may reach inverter interfaces through cloud platforms, vendor APIs, or exposed IP-based services.

• Local network access

Adversaries may compromise field networks (e.g., LAN, Wi-Fi, RS-485 gateways) through weak segmentation or insecure deployments.

• Firmware and configuration manipulation

Attackers may attempt to install modified firmware, downgrade versions, or alter configuration parameters.

 doi:10.20944/preprints202603.0988.v1

• Credential compromise

Weak authentication, shared credentials, or certificate mismanagement may allow unauthorized access.

• Protocol exploitation

Plaintext or unauthenticated protocols (e.g., Modbus TCP, legacy SunSpec deployments) may be abused to inject commands or read sensitive data.

5.2. Attack Surfaces

PV inverters expose multiple cyber-physical attack surfaces:

• Communication interfaces

Including IEEE 2030.5, SunSpec Modbus, proprietary APIs, and cloud-connected services.

• Firmware update mechanisms

OTA update channels, bootloaders, and firmware integrity checks.

• Cryptographic assets

Certificates, private keys, and trust anchors stored on the device.

• Local management ports

Serial interfaces, web dashboards, or vendor-specific tools.

• Supply-chain components

Third-party libraries, embedded modules, and vendor ecosystems.

5.3. Potential Impacts

Compromised inverters can produce both cyber and physical consequences:

• Manipulation of grid-relevant parameters

Alteration of setpoints, protection thresholds, or ride-through behavior.

• Service disruption

Coordinated inverter shutdowns or oscillatory behavior affecting feeders.

• Privacy leakage

Extraction of fine-grained energy data revealing user behavior.

• Lateral movement

Pivoting from inverter networks into SCADA, DERMS, or utility IT systems.

• Supply-chain propagation

Firmware-level compromises affecting entire fleets.

5.4. Security Objectives

Based on these threats, the USB aims to ensure:

• Integrity

Prevent unauthorized firmware, configuration changes, or command injection.

• Confidentiality

Eliminate plaintext communication paths and protect sensitive operational data.

• Authentication and trust

Ensure strong identity verification for devices, users, and management systems.

• Resilience

Support secure updates, vulnerability remediation, and lifecycle governance.

• Interoperability

Provide consistent protection across heterogeneous DER protocols.

6. Discussion

The Unified Security Baseline (USB) proposed in this work addresses a long-standing gap in the cybersecurity landscape for photovoltaic (PV) inverters and distributed energy resource (DER) ecosystems. By consolidating fragmented requirements from IEC, UL, IEEE, SunSpec, and emerging

 doi:10.20944/preprints202603.0988.v1

regulatory frameworks, the USB provides a coherent foundation for secure-by-design engineering and lifecycle governance. This section discusses the broader implications of the USB, its benefits for stakeholders, and its limitations.

6.1. Practical Implications for Manufacturers

For inverter manufacturers, the USB offers a clear and actionable set of security expectations that reduce ambiguity across heterogeneous standards. Instead of navigating partially overlapping requirements, vendors can adopt the USB as a unified reference for:

- secure firmware development and integrity protection
- certificate and key lifecycle management
- secure update pipelines
- SBOM generation and maintenance
- vulnerability disclosure and patch management

This alignment simplifies product design, accelerates compliance efforts, and reduces the likelihood of inconsistent or incomplete security implementations across product lines.

6.2. Benefits for Utilities and System Operators

Utilities and DER aggregators increasingly manage large fleets of heterogeneous inverters with varying security capabilities. The USB provides a consistent baseline that can be used to:

- evaluate device security posture during procurement
- define minimum security requirements for interconnection
- reduce operational risk in mixed-protocol environments
- support secure integration with SCADA, DERMS, and cloud platforms

By harmonizing communication-security expectations across SunSpec, IEEE 2030.5, and legacy Modbus deployments, the USB also helps operators avoid weak links created by protocol inconsistencies.

6.3. Regulatory Alignment and Conformity Assessment

The USB is intentionally aligned with the security obligations introduced by the EU Cyber Resilience Act (CRA), NIS2 Directive, and related supply-chain security initiatives. While these regulations define mandatory processes—such as vulnerability handling, secure updates, and SBOM transparency—they do not prescribe device-level technical baselines. The USB fills this gap by translating regulatory expectations into concrete controls that manufacturers can implement and auditors can verify.

This positions the USB as a potential foundation for future conformity-assessment schemes or certification programs targeting DER and inverter security.

6.4. Limitations

The USB is a conceptual baseline and does not evaluate specific vendor implementations or provide protocol-level formal verification. Its scope is limited to device-centric security and does not address broader system-level considerations such as grid-wide anomaly detection, intrusion-tolerant control, or coordinated response mechanisms. Additionally, while the USB harmonizes cross-standard requirements, it does not replace the need for compliance with domain-specific standards or regional interconnection rules.

 doi:10.20944/preprints202603.0988.v1

6.5. Future Directions

Future work may extend the USB by:

- validating its applicability through testbed experiments
- developing automated tools for conformity assessment
- integrating the USB with grid-level monitoring and detection systems
- exploring certification pathways aligned with CRA and international standards

Such efforts would further strengthen the security posture of inverter-dominated DER environments and support the transition toward resilient, cyber-secure energy systems.

7. Conclusion

This work has presented a Unified Security Baseline (USB) for photovoltaic (PV) inverters operating as networked IoT/OT devices within distributed energy resource (DER) ecosystems. By synthesizing requirements from IEC, UL, IEEE, SunSpec, and emerging regulatory frameworks such as the EU Cyber Resilience Act (CRA) and NIS2 Directive, the USB addresses long-standing fragmentation across technical, communication, and lifecycle security domains. The resulting baseline provides a coherent, device-centric foundation for secure-by-design engineering, interoperability, and long-term lifecycle governance.

The USB highlights the need for consistent protection across heterogeneous DER communication protocols, robust firmware integrity mechanisms, strong authentication, secure update pipelines, and structured vulnerability-handling processes. By aligning these controls with regulatory expectations, the USB supports manufacturers, utilities, and system operators in strengthening the cyber-physical resilience of inverter-dominated grids.

While the USB does not replace domain-specific standards or provide formal verification of protocol implementations, it establishes a practical and extensible framework that can guide future conformity-assessment efforts and certification schemes. Future research may expand the USB through empirical validation, automated assessment tools, and integration with grid-level monitoring and detection systems. As DER penetration continues to grow, harmonized and lifecycle-oriented security baselines will be essential to ensuring the resilience and trustworthiness of modern energy infrastructures.

References

1. Ye, J., et al. “A review of cyber-physical security for photovoltaic systems.” *IEEE J. Emerging and Selected Topics in Power Electronics*, 2021.
2. Dzobo, O., Tivani, L., Mbatha, L. “A review on cybersecurity for distributed energy resources.” *Journal of Infrastructure, Policy and Development*, 2024.
3. Liu, M., Teng, F., Zhang, Z., et al. “Enhancing cyber-resiliency of DER-based smart grids: A survey.” *arXiv preprint*, 2023.
4. Tuyen, N.D., et al. “A comprehensive review of cybersecurity in inverter-based smart power systems.” *IEEE Access*, 2022.
5. Harrou, F. “Cybersecurity of photovoltaic systems: challenges, threats and solutions.” *Frontiers in Energy Research*, 2023.
6. IEC 62443-4-1 / 62443-4-2. “Secure product development lifecycle and technical security requirements for IACS components.” IEC, 2023.
7. IEC 62351 series. “Power system cybersecurity standards.” IEC, 2023.
8. IEEE 1547.3-2023. “Guide for cybersecurity of DER interconnected with electric power systems.” IEEE Standards Association, 2023.
9. SunSpec Alliance. “SunSpec Modbus models, secure profiles, and DER cybersecurity program notes.” SunSpec Technical Documentation, 2024–2025.
10. UL 2900-1. “Standard for Software Cybersecurity for Network-Connectable Products.” UL Solutions, 2024.

 doi:10.20944/preprints202603.0988.v1

11. UL 1741 SB. "Supplement B cybersecurity update notice." UL Solutions, 2024.
12. Cyber Resilience Act (EU). "Product cybersecurity requirements for digital elements." European Commission, 2025.
13. NIS2 Directive (EU). "Operational cybersecurity requirements for essential and important entities." European Union, 2023.
14. ENISA. "Energy sector cybersecurity and IoT supply-chain security guidance." ENISA Reports, 2023–2025.
15. NTIA. "SBOM in energy systems: implementation guidance." NTIA Report, 2024.
16. DOE CESER. "Secure firmware update mechanisms for grid-connected devices." U.S. DOE CESER Report, 2023.
17. Sandia National Laboratories. "Recommendations for trust and encryption in DER interoperability standards." SAND2019-1490, 2019.
18. Krotofil, M., et al. "Cyber-physical attack surfaces in inverter-based resources." *Computers & Security*, 2024.
19. Hahn, A., et al. "OT cybersecurity for distributed energy systems." *IEEE Transactions on Industrial Informatics*, 2023.
20. CIGRE. "Cybersecurity for DER integration in distribution networks." CIGRE Technical Brochure, 2024.