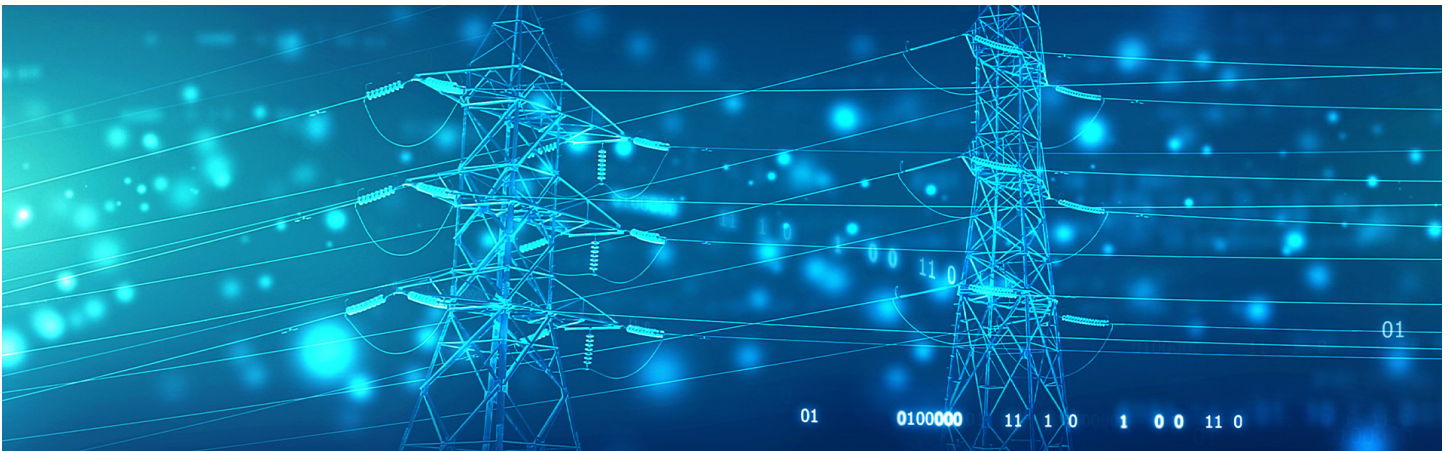


WHITE PAPER

Navigating Cybersecurity Risks in Distributed Energy Resources

By Sowmya Ragothaman, Kristina Beck, Jack Bliss and Peyton Sanders

The modern electric grid depends on digital infrastructure, distributed energy and advanced metering to manage increasingly dynamic operations. These technologies expand flexibility but widen the cyberattack surface. Protecting critical systems requires rigorous authentication, encryption, monitoring and updated regulatory frameworks to secure both transmission-level assets and distribution networks.



Modern Grid Architecture and Regulation

The traditional unidirectional power-flow model no longer reflects the complexity of the modern grid. Today's network is dynamic and interactive, requiring coordination of bidirectional energy flows supported by new layers of digital infrastructure to maintain stability and security. Distributed resources — including rooftop photovoltaic systems, battery energy storage and campus-scale microgrids — now integrate with distribution feeders through advanced inverters. To manage this complexity, utilities are deploying advanced distribution management systems (ADMS) and distributed energy resource management systems (DERMS) to provide real-time orchestration of voltage support, frequency response and market dispatch. Figure 1 illustrates how these elements fit together in a modern grid ecosystem, linking generation, distribution, operations and customer systems.

High-speed fiber, 5G and private LTE backhaul now connect distributed assets to cloud-based analytics and independent system operator/regional transmission organization (ISO/RTO) platforms. These connections enable aggregators to bid pooled DERs into the market as virtual power plants. While this layered, data-rich architecture enhances grid flexibility and resilience, it also expands the cyberattack surface. Every additional sensing node, communications pathway and application programming interface (API) endpoint introduces potential vulnerabilities. To protect this critical infrastructure, systems must be authenticated, encrypted and subjected to continuous monitoring.

Grid modernization depends on a diverse suite of digital systems and devices. Core elements include ADMS, phasor measurement units (PMUs), AMI, Internet of Things (IoT) technologies, and DERs. Together, these components form the foundation of a more

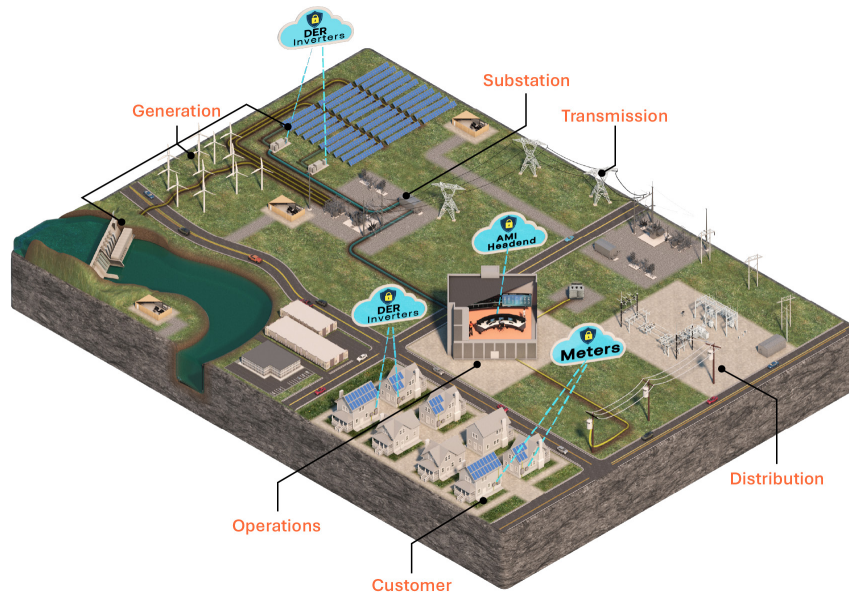


Figure 1. Illustration of the modern grid ecosystem.

intelligent, data-driven grid but also introduce new points of cybersecurity exposure.

North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) standards apply primarily to the bulk electric system (BES), which includes transmission elements operated at 100 kV and above, generation facilities with aggregate nameplate ratings greater than 75 MVA connected at BES voltage, and certain lower-voltage assets such as black start generation paths and high-voltage transmission facilities. These assets are subject to strict, mandatory cybersecurity controls designed to protect grid reliability and resilience.

Once power is stepped down at the sub-transmission or distribution level, most feeders, AMI systems, reclosers, and customer-sited DERs fall outside the BES definition and therefore beyond CIP requirements. Their protection is typically determined by state regulations or individual utility practices. While certain sub-100-kV equipment, such as black start units or under-voltage load-shedding schemes, may still qualify as BES, a significant regulatory gap persists. As a result, cyber defenses on the distribution side of the grid remain comparatively limited across most jurisdictions

Current Regulatory Standards

Current cybersecurity standards provide important guidance for grid security but fall short of addressing the full complexity of modern, highly distributed systems.

Regulatory updates that place cybersecurity at the center of modernization efforts are essential to building a secure, responsive and resilient grid.

FERC Order 901

Establishes requirements for data sharing, model validation and operational oversight of inverter-based resources (IBRs) within the Bulk-Power System (BPS). However, it exempts distributed resources, leaving a security gap outside direct utility oversight. Legacy systems that lack communication capabilities further contribute to blind spots in grid cybersecurity.

Cybersecurity Risks and Mitigation Strategies

As utilities integrate smart devices, automated control systems and cloud-based analytics into grid operations, these technologies introduce new vulnerabilities across software, communication protocols and third-party platforms. Compromises in any of these areas can disrupt power delivery, enable unauthorized access to operational networks or manipulate critical infrastructure. The grid's growing reliance on third-party vendors and opaque global supply chains further heightens these risks. Smart inverters, often manufactured overseas, illustrate the challenge most clearly, but similar concerns extend to smart meters, cellular and RF communications modules, battery management systems, EV chargers, and cloud gateways. All of these technologies represent potential vectors for firmware-level compromise or supply chain attack, underscoring the need for rigorous security oversight.

At the distribution level, AMI and distributed energy resources (DERs) represent significant cybersecurity concerns. Their widespread deployment creates a large attack surface, and successful compromises have the potential to disrupt operations, compromise customer data and affect grid stability.

AMI Cybersecurity Risks

AMI consists of smart meters, communication networks and data management platforms that enable real-time monitoring and control of electricity usage. The first wave of deployment in the late 2000s and early 2010s introduced roughly 62 million AMI 1.0 meters, designed primarily for “meter-to-cash” functions such as automated interval reads and remote connect/disconnect. In contrast, the next generation of AMI 2.0 devices, with approximately 2.5 million currently being installed, provides expanded capabilities, including high-resolution voltage sensing, edge computing, and native DER awareness.

This wide-area, system-of-systems architecture significantly expands the cyberattack surface. Each smart meter operates on Linux-based firmware, making it susceptible to exploits such as remote code execution, denial-of-service and data tampering. Meter traffic traverses a mesh network before terminating at the AMI headend — a core SCADA component that, in some utilities, is bridged directly or through a demilitarized zone (DMZ) to the corporate IT network at the control center. A breach at any point along this path can lead to localized outages, inaccurate billing or the loss of manual-read fallback. When meters are equipped with remote disconnect relays, the stakes increase further, as a coordinated cyberattack could trigger wide-area disruptions, escalate into transmission-level instability and jeopardize overall grid reliability. In severe cases, cascading impacts could necessitate load shedding, extending instability well beyond the immediately affected region. Figure 2 highlights two potential AMI attack scenarios, showing how vulnerabilities, attack vectors, and methods

of exploitation could translate into widespread operational and financial impacts.

Utilities have already encountered integrity breaches within AMI that disrupted billing systems, producing financial losses in the millions and, in some cases, tens of millions of dollars. By contrast, the second attack scenario remains theoretical but has been validated as technically feasible. In 2023, researchers at Oregon State University demonstrated a proof of concept showing how coordinated manipulation of AMI systems could escalate into broader grid instability.

AMI Reference Architecture, Mitigation Strategies and Best Practices

Strengthening AMI requires more than compliance with baseline standards. Utilities can adopt reference architectures and implement layered mitigation strategies that address both technical vulnerabilities and operational risks. Figure 3 illustrates a representative AMI security architecture, highlighting key zones and defenses across the network.

The following best practices, split into two categories, highlight key measures such as **secure key management**, **network segmentation**, **access controls and continuous monitoring**, forming the foundation of a defensible and resilient AMI environment:

Key Management

- Smart meters function as the primary field devices within AMI. Most modern deployments are built on the device language

Attack Scenario	Vulnerability	Attack Vector	Exploitation	Impact
1. Wide area loss of AMI functions	1. Misconfigured network segmentation 2. Misconfigured user access/password management	1. Third-party (vendor) access to all individual meters 2. Access to the AMI headend	1. Abusing protocols 2. Exploiting firmware or OS flaws 3. Breaking weak key management and cryptographic defenses	1. Loss of billing 2. Lost utility revenue 3. Cause wide area loss of power at the distribution level (neighborhood, military base, etc.)
2. Attack relay function at the smart meter	3. Meters or related network devices not regularly updated, leaving known security flaws unaddressed	3. Living off the land Advanced Persistent Threat (APT)	4. Using radio frequency jamming or signal floods 5. Supply chain implants 6. leveraging insider or contractor misuse	1. Lost utility revenue 2. Cause wide area loss of power at the distribution level (neighborhood, military base, etc.)

Figure 2. Potential AMI attack scenarios, highlighting vulnerabilities, attack vectors, methods of exploitation and resulting impacts.

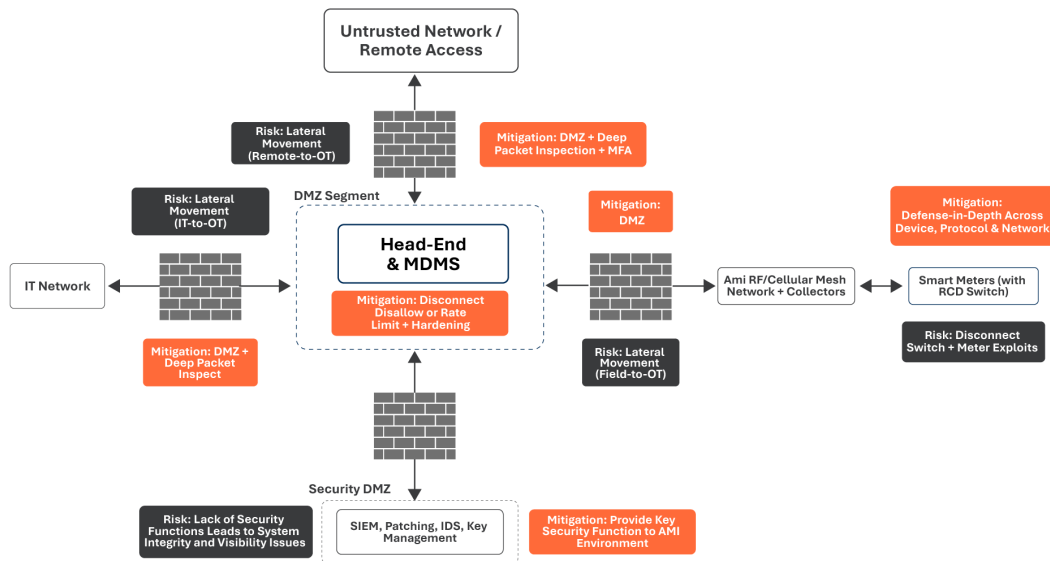


Figure 3: AMI security architecture

message specification/Companion Specification for Energy Metering standard (IEC 62056), which defines both the device model and application-layer communication protocols for energy meters. DLMS also establishes three security profiles, known as security suites, that provide tiered levels of authentication, encryption and key management to safeguard data exchange.

Defendable Network Architecture

• Network Segmentation and Zoning

- Divide infrastructure into microsegments or zones based on region, criticality or function. Techniques such as virtual local area networks (VLAN), software-defined networking (SDN) or logical segmentation help prevent a breach in one zone from propagating to others.
- Networks should not communicate directly with the headend server without traversing a firewall.

• Deploy a DMZ

- Place all external-facing services — such as remote management interfaces, vendor portals or systems requiring public access — in a dedicated DMZ.
- This buffer layer reduces exposure to core systems by filtering and controlling traffic between the internet and internal networks.

• Firewalls and IDS/IPS

- Position firewalls and intrusion detection/prevention systems (IDS/IPS) at key boundaries, including between network zones and between the DMZ and internal systems.
- Enforce strict rules for allowed ports and protocols while monitoring for anomalous traffic.

• Strong Access Controls

- Enforce role-based access control (RBAC) and multi-factor authentication (MFA) for critical systems and operations to limit sensitive functionalities to authorized users only.

◦ MFA for the Headend System

- Modern headend platforms typically support LDAP, RADIUS, SAML or OAuth integration, enabling connection with identity providers such as Okta, Azure AD or Ping.
- When a user logs into the headend console, the user is prompted for a username and password, and a second factor (e.g., authenticator app, short message service (SMS) code or hardware token).

◦ MFA for Critical Operations (Remote Disconnect)

- Assign permissions by role. For example, a “Standard Operator” can view meter data, while an “Operations Supervisor” can initiate disconnects.
- Restrict disconnect functionality to the smallest possible set of users or groups.
- Rate-limit disconnect commands to minimize the number that can be executed within a defined period.
- Consider removing automated disconnect functionality altogether and reverting to field-based practices, such as “pull and tag,” where operational risk warrants.

• Risk-Based Vulnerability Management

- Keep all network devices, firmware and systems updated against known vulnerabilities, prioritizing the most critical or externally exposed assets.

Security Tier	DLMS Security Suite	"Good → Better → Best" Level	Notes
Suite 0	Shared-secret, optional encryption	Good (baseline legacy)	Insecure by modern standards; no key rotation and no encryption by default
Suite 1	AES-GCM, GMAC, symmetric keys	Better (modern and secure)	Symmetric authenticated encryption, key wrap and HLS5 supported
Suite 2	ECDSA, ECDH, X.509	Best (asymmetric and scalable)	Enables true public key infrastructure (PKI), forward secrecy and digital signing

Figure 4: DLMS/COSEM security suites showing progression from legacy shared-secret methods (Suite 0) to modern symmetric encryption (Suite 1) and fully scalable asymmetric cryptography with PKI support (Suite 2).

- **Comprehensive Monitoring and Logging**
 - Implement continuous monitoring and detailed logging across all network segments.
 - Prioritize logging of high-risk actions, such as remote disconnect commands, and focus additional oversight on critical systems like the AMI headend.

IBR Cybersecurity Risks

Inverter-based resources (IBRs), including solar photovoltaics and battery energy storage systems, present distinct cybersecurity challenges due to their dependence on networked monitoring and control. Their rapid deployment across residential, commercial and industrial settings creates a highly distributed footprint. Combined with remote connectivity requirements, this expansion introduces new attack surfaces and amplifies system vulnerabilities.

In solar power systems, panels generate direct current (DC) that is converted to alternating current (AC) by photovoltaic (PV) inverters before being fed into the grid. In residential and commercial installations, these inverters often connect to the internet through serial communication dongles using Wi-Fi, general packet radio service (GPRS), 4G or wired connections. Data is transmitted to cloud services via protocols such as MQTT, enabling remote monitoring, visualization and management of millions of distributed devices. Some inverter models bypass dongles entirely, connecting directly to the cloud. Owners typically interact with these platforms through mobile or web applications, often using HTTP during setup and configuration.

By contrast, utility-scale inverters are usually integrated into local supervisory control and data acquisition (SCADA) or energy management systems. They operate over secure, private networks

using industrial protocols such as Modbus, DNP3 or IEC 61850, with data managed on-site. While this architecture reduces exposure to internet-based threats, it is not immune. Risks persist from misconfigured firewall rules, insufficient network segmentation, insecure remote access pathways and unpatched protocol vulnerabilities. Emerging practices such as the adoption of cloud-based analytics and digital twin technologies further complicate the landscape. If not properly segmented from operational networks, these tools can reintroduce external attack vectors into systems otherwise designed for isolation.

There are three primary categories of solar power system installations:

- **Residential:** Typically consist of 6 to 20 rooftop panels, producing between 5 and 15 kilowatts (kW) of electricity, which is generally sufficient to power a single home.
- **Commercial:** Larger systems that generate approximately 100 kW or more, designed to meet the energy demands of businesses ranging from small retail operations to large industrial facilities.
- **Utility-scale:** Comprise hundreds to thousands of ground-mounted panels in expansive solar farms, producing at least 1 megawatt (MW) of power. These systems are commonly owned and operated by electric utility companies.

A significant share of residential and commercial string inverters are equipped with wireless connectivity to cloud platforms, many of which are operated by Chinese companies. Six of the world's top 10 solar power system vendors, including inverter manufacturers, are headquartered in China. As a result, more than half of all inverters are both owned and manufactured in China, while another 30% are produced in Chinese facilities on behalf of U.S. or other

international companies. This concentrated supply chain raises serious cybersecurity concerns. Risks include remote firmware updates routed through foreign-controlled infrastructure, as well as persistent internet connectivity that enlarges the attack surface and the possibility of hardware-level compromises such as embedded rogue communication devices. Equally concerning is the potential for deliberate actions by the manufacturer, or for the exploitation of vulnerabilities, that push malicious firmware at scale and jeopardize the security and reliability of deployed systems.

Although utility-scale inverters are not typically connected to public cloud services, they remain exposed to similar risks. Utilities often enforce strict network segmentation and prohibit direct internet-based remote access to inverter equipment. Even so, investigations have revealed instances of inverters and batteries, particularly those manufactured in China, containing undocumented communication hardware, such as embedded cellular radios. These components create covert communication channels that can bypass firewalls and monitoring systems. In parallel, utilities continue to depend on vendor-supplied firmware and update packages. If compromised in

the supply chain, these updates could deliver malicious code into critical infrastructure. The SolarWinds breach demonstrated how trusted update mechanisms can be exploited to insert backdoors at scale. A comparable compromise within the inverter supply chain could have severe implications for grid stability and national energy security.

Commercial and residential inverters represent a critical intersection of high likelihood and high impact. These systems often operate with weaker security controls, creating a broad and vulnerable attack surface. The risk is amplified by the growing aggregate generation capacity of distributed solar resources, which now supply a substantial share of daytime demand in many regions. This makes them both more attractive targets and more capable of leading to large-scale disruption. Potential threats include unauthorized configuration changes, remote shutdowns and tampering with safety mechanisms, any of which could result in localized or neighborhood-scale outages. More severe risks arise if attackers disable anti-islanding protections or override export limits, as the resulting grid imbalances could escalate into transmission-

Attack Scenario	Vulnerability	Attack Vector	Exploitation	Impact
Removal of export limits on a wide area of string inverters	<ol style="list-style-type: none"> Misconfigured network segmented Misconfigured user access or password management Meters or related network devices not regularly updated, leaving known security flaws unaddressed Malicious firmware update Cloud-based vulnerability used to connect to residential or commercial based inverters 	<ol style="list-style-type: none"> Third-party (vendor) access to all individual meters Living off the land Advanced Persistent Threat (APT) 	<ol style="list-style-type: none"> Override or significantly raise the export limit Coordinate changes across multiple inverters to create a sudden power surge Tamper with logs to hide activities 	<ol style="list-style-type: none"> Local or widespread grid instability Extended outages occur when the grid operator detects unsafe conditions (such as voltage spikes), prompting automatic or manual load shedding to protect the grid and potentially causing blackouts beyond the immediate site

Figure 5. Cyberattack scenario illustrating how vulnerabilities in string inverters can be exploited.

level instability, undermining overall grid reliability. Figure 5 illustrates how vulnerabilities in string inverters can be exploited to trigger these types of outcomes.

IBR Reference Architecture, Mitigation Strategies and Best Practices

Mitigation Strategies and Best Practices

While residential and commercial solar users do not have the same security infrastructure as utilities, they often face the greatest exposure and can still take meaningful steps to reduce their risk.

Figure 6 shows a reference architecture for inverter-based resources (IBRs), illustrating key risk points and mitigations across residential, commercial, and utility-scale deployments.

Residential and commercial users can reduce exposure by adopting practices such as:

- Purchase inverters from trusted or U.S.-based manufacturers:** Select vendors with U.S. headquarters, domestic manufacturing or demonstrably secure and transparent supply chains. This reduces the risk of

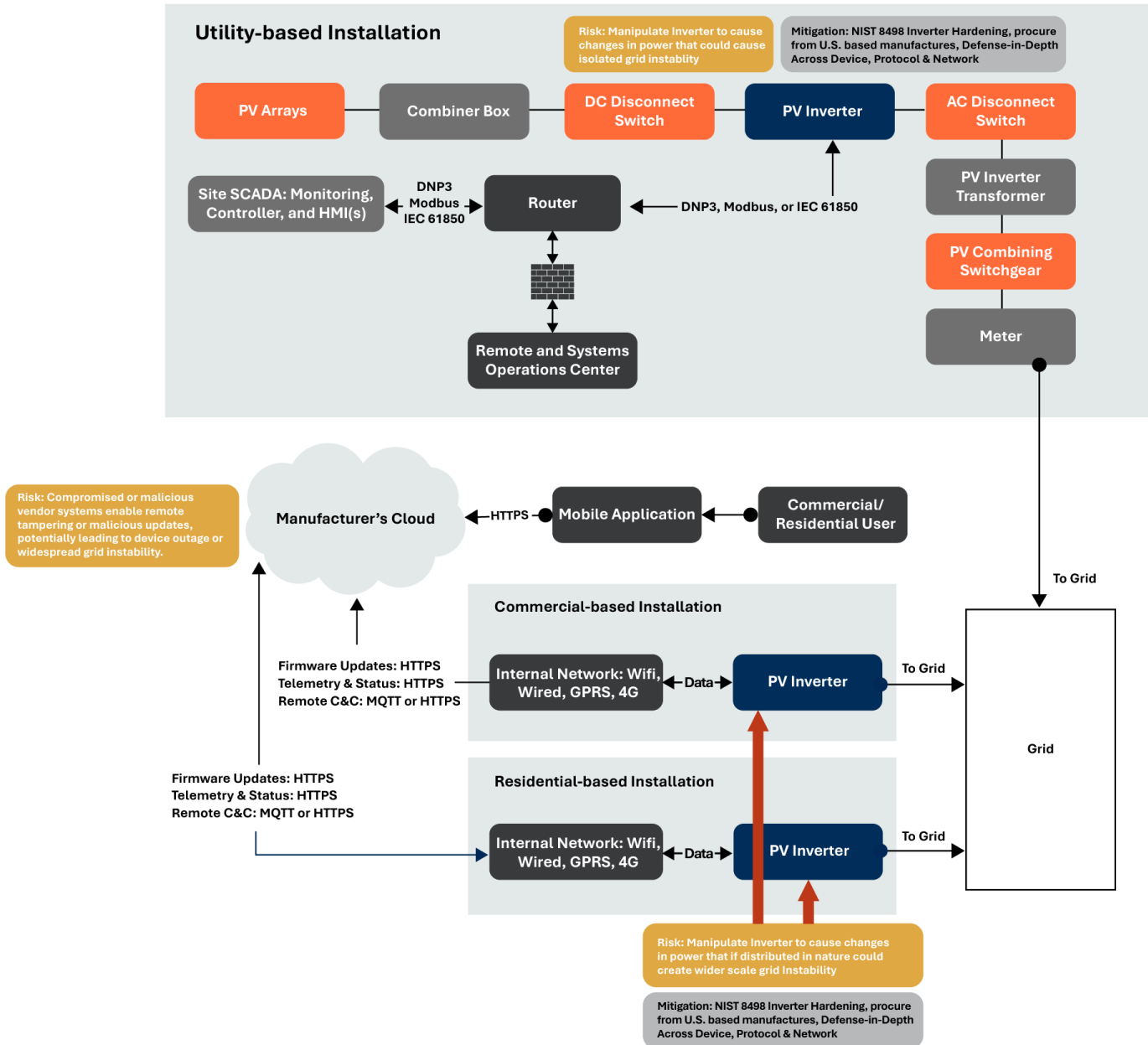


Figure 6: IBR reference architecture.

foreign influence, hidden hardware components or firmware manipulation.

- **Implement network segmentation:** Place inverters on isolated VLANs or guest networks to limit their exposure and lateral movement from compromised devices.
- **Restrict outbound connectivity:** Limit inverter internet access to known, necessary cloud endpoints using firewall or router rules.
- **Disable cloud connectivity if not required:** Turn off mobile app pairing or cloud syncing for systems that don't need remote access features.
- **Manually control firmware updates:** Disable automatic updates and apply firmware manually after verifying source authenticity and checksums.
- **Request software bill of materials (SBOM) and cybersecurity transparency:** Ask vendors for SBOMs and inquire about their participation in secure development frameworks (e.g., software development life cycle, third-party audits).

Utility-Scale Installations

While inverter-based resources continue to expand across energy systems, their growing digital footprint creates new risks that can be targeted through both supply chain vulnerabilities and weak device configurations. Owners and operators can significantly reduce exposure by adopting structured cybersecurity measures, including:

- **Buy from vetted, domestic or allied suppliers.** Prioritize vendors with U.S.-based or allied-nation supply chains. Favor manufacturers participating in NREL, Department of Energy (DOE), or UL cybersecurity initiatives such as UL 2941. Avoid suppliers linked to known vulnerabilities or rogue hardware components.
- **Implement NIST IR 8498 controls.**
 - **Change default credentials.** Replace all default usernames and passwords with strong, unique credentials.
 - **Role-based access control (RBAC):**
 - Level 1 (basic): A single user account provides unrestricted access to inverter features.
 - Level 2 (role account): Access is segmented by role (e.g., installer, maintainer or owner), with credentials shared among authorized individuals.
 - Level 3 (full RBAC): User accounts are assigned to defined roles with specific permissions, which allows for granular access control.
 - **Enable security logging.** Stream inverter syslogs to the utility security information and event management (SIEM) system, capturing key events such as successful logins,

failed logins and configuration changes. Incorporate logs into containment exercises.

- **Update software regularly.** Apply vendor patches promptly, as most inverter common vulnerabilities and exposures (CVE) are addressed upstream months before active exploitation.
- **Manage supply chain risk.** Vet vendors, especially low-cost importers, for secure development practices. Request SBOMs and require vulnerability-notification service-level agreements (SLAs).
- **Backup critical system information.** Maintain secure backups of inverter configurations and system data.
- **Disable unused features.** Turn off unnecessary services, such as embedded web servers or unused protocols, to minimize the attack surface.
- **Secure communication interfaces.** Harden Ethernet, Wi-Fi and cellular connections against unauthorized access.
- **Validate firmware predeployment.** Require cryptographic signing, manual hash verification and offline review of firmware packages prior to installation.
- **Conduct comprehensive supply chain risk assessments.** Reference *INL/RPT-24-80434 Revision 0*, a DOE-sponsored report from Idaho National Laboratory: “Battery Supply Chain Security: Procurement Guidance and Sample Contract Terms.” The report provides structured guidance for utilities and government agencies on integrating cybersecurity and supply chain risk management into procurement processes for battery energy storage systems (BESS) and inverter-based resources. Recommendations include vendor selection protocols, risk assessment frameworks and model contractual language to provide integrity, transparency and resilience in critical energy infrastructure.
- **Maintain strong network isolation.** Physically and logically segment inverter networks from IT environments. Incorporate monitoring and deep packet inspection to identify and contain anomalous traffic.

Additional Actions That Would Reduce Risk Across the DER Ecosystem

Under the current regulatory framework, cybersecurity for commercial and residential inverters remains the responsibility of the consumer-operator. Utilities, however, can play a critical role by educating customers and collaborating with local governments to establish policies that promote secure communication with distributed inverter resources. Enabling this connectivity would enhance visibility and control, significantly strengthening grid security. Establishing minimum cybersecurity expectations, supporting domestic or allied-nation manufacturing, and aligning distributed systems with recognized best practices can greatly

reduce the likelihood of these assets serving as distributed attack vectors. Key steps to advance inverter cybersecurity and strengthen grid resilience include:

- **Coordinate multistate oversight.** State public utility commissions should align on requiring cybersecurity expectations and controls for behind-the-meter (BTM) assets, including inverters, that could impact bulk power system reliability. This approach would shift security responsibility from consumer-operators to utilities, creating a more consistent and enforceable framework.
- **Establish an approved vendor list.** Agencies such as DOE, Department of Homeland Security, or a multistate body like the National Association of Regulatory Utility Commissioners should maintain a vetted list of inverter vendors based on cybersecurity posture, code transparency and hardware integrity. This would provide utilities with a trusted reference for procurement decisions.
- **Require UL 2941 certification.** Regulators and utilities should make cybersecurity certification a prerequisite for procurement once UL 2941 is finalized. This standard would establish a certifiable cybersecurity baseline for DER devices, so that inverters and similar technologies would be secure by design, field-ready and aligned with utility and regulatory expectations. Vendors would be required to demonstrate compliance with UL 2941 certification requirements before deployment.

Key vulnerabilities at the grid edge include cloud-connected inverters susceptible to remote tampering and smart meters exposed through insecure firmware, weak key management and insufficient network segmentation. For AMI systems, utilities should prioritize modern DLMS/COSEM security suites with robust encryption and authentication, while segmenting AMI networks from both trusted and untrusted domains. Role-based access controls and multi-factor authentication must be enforced, with high-risk functions such as remote disconnect restricted to a minimal set of authorized users. Regular patching, validated firmware updates and continuous monitoring across the AMI environment are essential to strengthen detection, accelerate response and sustain long-term resilience.

For inverter-based systems, effective risk reduction starts with procuring devices from U.S.-based or allied manufacturers with transparent and verifiable supply chains. Residential and commercial installations should isolate inverter networks, restrict outbound communications and disable unnecessary cloud connectivity. Firmware updates must be manually verified and applied only after source authentication. At the utility scale, additional measures are required, including role-based access controls, centralized logging, firmware validation aligned with NIST IR 8498 and formal supply chain risk assessments guided by frameworks such as INL RPT-24-80434. Taken together, these practices — across both AMI and inverter deployments — move cybersecurity from a reactive safeguard to a foundational component of modern grid reliability.

Technical controls alone are not sufficient. Under the current regulatory framework, cybersecurity for residential and commercial inverters remains largely the responsibility of consumer-operators. To close this gap, state public utility commissions should collaborate with utilities to establish multistate oversight that enforces minimum cybersecurity requirements for behind-the-meter devices capable of affecting grid reliability. A nationally supported list of approved vendors, maintained by DOE, DHS or a multistate body, could provide further assurance by guiding procurement based on code transparency and hardware integrity. Once UL 2941 is finalized, utilities and regulators should require certification as a condition of procurement, creating a verifiable cybersecurity baseline for inverter-based resources. Together, these measures, combined with technical remediation, build a stronger and more coordinated foundation for securing distributed energy infrastructure at scale.

About 1898 & Co.



1898 & Co. is a global business, technology, and security consultancy serving critical infrastructure industries. We partner with clients to plan, secure and optimize their business. As part of Burns & McDonnell and our

120 years of industry experience, we understand the complexity of your asset-intensive business model, the trends impacting your industry, and the need to ground big ideas in operational realities. Learn more at [1898andCo.com](https://www.1898andCo.com).