resillion

Cyber-physical security of distributed energy resources in the UK grid

The UK's transition to a decentralised energy system has accelerated the deployment of Distributed Energy Resources (DERs), introducing new cyber security risks to the national grid. This report examines technical vulnerabilities in DERs, evaluates regulatory gaps and proposes a multi-layered defence strategy. It also outlines Resillion's capabilities in securing DER ecosystems and offers actionable recommendations to strengthen the resilience of UK energy infrastructure.

The cyber security imperative in a decentralised grid

The United Kingdom's energy system is undergoing a fundamental transformation, driven by Net Zero targets and the rapid deployment of DERs. These include solar photovoltaic (PV) systems, battery energy storage systems, electric vehicle (EV) chargers and vehicle-to-grid (V2G) technologies. While these technologies enhance grid flexibility and decarbonisation, they also significantly expand the cyber-physical attack surface.

Each DER device, when connected to the grid, becomes a potential entry point for adversaries. The urgency to deploy these technologies at scale has often outpaced the implementation of robust cyber security controls. This report explores the technical vulnerabilities, regulatory gaps and mitigation strategies necessary to secure the UK's distributed energy infrastructure.

Technical vulnerabilities in DER devices

Remote code execution and firmware exploits

Security assessments have revealed critical flaws in DER firmware, including remote code execution (RCE) vulnerabilities. Legacy web interfaces on inverters have allowed unauthenticated file uploads, enabling attackers to execute arbitrary code[1]. These vulnerabilities stem from outdated development practices, such as a lack of input sanitisation and insecure file handling.

Cryptographic weaknesses

Many DER devices employ weak or wrongly implemented cryptographic protocols. Common issues include:

- use of hard-coded AES (Advanced Encryption Standard) keys
- acceptance of invalid SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificates
- lack of mutual authentication in MQTT (Message Queuing Telemetry Transport) and REST (REpresentational State Transfer) APIs

These flaws expose DERs to man-in-the-middle (MitM) attacks, data interception and command injection[2, 3].

API and credential management failures

Exposed APIs without authentication, hard-coded credentials and insecure password reset mechanisms are prevalent. These issues allow attackers to enumerate users, hijack accounts and remotely manipulate device behaviour[4]. In some cases, attackers can reconfigure EV chargers or inverters to cause physical damage or grid instability.

Supply chain and hardware risks

Undocumented communication modules and rogue firmware components have been identified in some DER[5]. These may be indicative of supply chain compromise or inadequate hardware validation processes.

Regulatory landscape: G98/G99/G100 and the cyber security gap

Overview of G98, G99 and G100

Engineering Recommendations G98, G99 and G100 define the technical requirements for connecting generation equipment to the UK distribution network[6]. While they address electrical safety, frequency response and protection settings, their cyber security provisions are high-level and non-prescriptive about the specific evidence required to satisfy these requirements. While this may be intentional, to account for a rapidly evolving cyber threat space, it has several downsides.

Self-declaration and compliance ambiguity

Manufacturers self-declare compliance via the Energy Networks Association (ENA) Type Test Register. However, there is no mandatory requirement for the specific evidence to be provided or for independent cyber security testing in sample forms[7]. This creates a systemic risk, as devices may be deployed with unverified security claims.

Inadequate enforcement of cyber standards

Although the recommendations reference established standards such as ETSI EN 303 645[8] and (the proposed) PAS 1879[9], they do not mandate conformance testing to any specific scheme[10] to achieve compliance. The lack of enforcement mechanisms means that even well-intentioned manufacturers may deprioritise security due to cost or time-to-market pressures.

resillion

The risks: DER malware and grid-scale threats

A coordinated attack on DERs could mimic a distributed denial-of-service (DDoS) event, overwhelming grid infrastructure with synchronised load or generation events. Firmware-level manipulation could bypass protection settings, creating a new class of grid malware.

Commercial and operational pressures

Market incentives vs. security investment

In a cost-sensitive market, manufacturers often prioritise feature delivery over security hardening. Energy retailers, incentivised to offer DERs as part of tariff packages, may not scrutinise device security rigorously.

Consumer awareness and procurement gaps

End-users typically lack the technical expertise to evaluate DER cyber security. Procurement decisions are driven by price and performance, not security posture.

Industry reluctance to acknowledge vulnerabilities

Security researchers have encountered resistance when disclosing vulnerabilities. Some vendors downplay risks or delay remediation, fearing reputational damage.

The threat landscape and real-world incidents

The threat environment facing the energy sector has intensified dramatically. In Q3 2024 alone, vulnerability-based attacks surged by 124%, with a marked increase in zero-day exploitation[11]. In early 2025, organisations reported an average of 1,925 cyber attacks per week, a 47% increase from 2024 levels[12]. Adversaries are now able to weaponise disclosed vulnerabilities within hours, bypassing traditional patch management cycles. This trend underscores the urgency for real-time threat intelligence, secure development practices and enforced vulnerability disclosure protocols, especially for DER devices that are increasingly embedded within the UK's critical infrastructure.

Case studies: Grid fragility

Recent incidents, such as the Heathrow power outage and the Spanish blackout, underscore the fragility of interconnected infrastructure[13]. While not cyber-related, they illustrate the potential for cascading failures, scenarios that compromised DERs could trigger.

Advanced persistent threats and nation-state actors

The energy sector is a high-value target for Advanced Persistent Threats (APTs), sophisticated and prolonged cyber attacks where an intruder gains access to a network and remains undetected for an extended period. Motivations range from espionage and sabotage to geopolitical leverage[14]. DERs, as edge devices with limited defences, are attractive targets for lateral movement into critical Operational Technology (OT) systems.

resillion

IT/OT convergence and attack surface expansion

The convergence of IT and OT networks increases the risk of cross-domain attacks. DERs often bridge these domains, making them ideal pivot points for attackers.

Technical recommendations for securing DERs

Securing DERs requires a multi-layered, technically rigorous approach that addresses the full lifecycle of device development, deployment and operation. As DERs increasingly serve as critical nodes in the UK's decentralised energy infrastructure, their cyber security posture must be elevated to match the threat landscape. The following recommendations outline essential technical controls and practices for DER manufacturers, integrators and operators.

Adopt secure development lifecycles (SDLs)

Manufacturers must embed security into every phase of the product development lifecycle. An SDL should include:

- threat modelling to identify attack vectors specific to DER architectures (e.g., inverter control logic, EV charger firmware)
- static and dynamic code analysis to detect vulnerabilities early
- secure coding practices aligned with OWASP and CERT guidelines
- security-focused design reviews, particularly for embedded systems and communication stacks

Automated tooling and continuous integration pipelines should support SDLs to ensure repeatability and traceability of security controls.

Mandate third-party cyber security testing

All DERs intended for grid connection should undergo independent cyber security testing by accredited laboratories. Testing should include:

- penetration testing of device firmware, APIs and cloud interfaces
- protocol fuzzing for Modbus, MQTT, OCPP and proprietary protocols
- validation of cryptographic implementations (e.g., TLS handshake integrity, key management)
- evaluation of physical interfaces (e.g., UART, JTAG) for debug port exposure

Test results should be documented in a standardised format and submitted as part of the DER's compliance package to the ENA or equivalent regulatory body.

resillion

Implement secure telemetry and anomaly detection

DERs must support secure telemetry to enable real-time monitoring and anomaly detection. This includes:

- encrypted data transmission using TLS 1.3 or equivalent
- device attestation and integrity verification at runtime
- behavioural baselining and anomaly detection using edge or cloud-based analytics
- integration with Security Information and Event Management (SIEM) systems for centralised visibility

Anomaly detection should be capable of identifying deviations in power output, communication frequency or command patterns that may indicate compromise.

Ensure secure OTA firmware updates

Over-the-air (OTA) update mechanisms must be designed with robust security controls, including:

- Firmware signing using asymmetric cryptography (e.g., RSA/ECDSA)
- Version control and rollback protection to prevent downgrade attacks
- Secure boot validation to ensure only trusted firmware is executed
- Update delivery via authenticated and encrypted channels

Update infrastructure should support staged rollouts and fail-safe mechanisms to prevent bricking of devices in the field.

Enforce standards-based conformance through approved certification schemes

All DERs should demonstrate conformance to cyber security standards, such as ETSI EN 303 645. These standards provide baseline requirements for:

- password management and credential protection
- secure communications and data protection
- software update mechanisms
- vulnerability disclosure and lifecycle support

Conformance should be validated through third-party audits and established certification schemes involving credible penetration testing methodologies. It should be maintained through continuous compliance monitoring.

Resillion's technical capabilities

We deliver a comprehensive portfolio of cyber security services engineered to address the unique challenges of securing DERs and the broader energy ecosystem. Our capabilities span the full lifecycle

of DER deployment, from secure design and validation to operational resilience and incident response, ensuring that energy stakeholders can meet both regulatory requirements and evolving threat landscapes.

Security assessments of DER firmware, APIs and protocols

We conduct in-depth security assessments of DER components, including embedded firmware, mobile and web APIs, and communication protocols. These assessments involve:

- static and dynamic analysis of firmware binaries to detect buffer overflows, insecure memory handling and logic flaws
- reverse engineering of proprietary protocols and inspection of MQTT, Modbus, OCPP and IEC 61850 traffic
- API fuzzing and authentication bypass testing for cloud-connected DER management platforms
- validation of cryptographic implementations and key management schemes

Our assessments are aligned with standards such as OWASP IoT Top 10 and NIST SP 800-115, ensuring comprehensive coverage of attack surfaces.

Penetration testing of DER ecosystems and cloud platforms

Our penetration testing services simulate real-world adversarial scenarios across the DER attack surface. They include:

- exploitation of insecure OTA update mechanisms and bootloader vulnerabilities
- privilege escalation and lateral movement within DER fleet management systems
- cloud infrastructure testing (e.g., AWS, Azure) for misconfigurations, insecure APIs and IAM (Identity and Access Management) flaws
- red teaming* exercises targeting DER-integrated demand response platforms and aggregator networks

*Red teaming in cyber security is a proactive approach where a group of ethical hackers simulates real-world attacks to identify vulnerabilities and strengthen an organisation's defences.

Testing is conducted using both black-box and grey-box methodologies, with detailed reporting and remediation guidance.

IoT security assurance aligned with international standards

We provide conformance testing and certification support for DER devices under frameworks such as:

- ETSI EN 303 645 (IoT cyber security baseline)
- NIST IR 8259 (IoT Device Cyber Security Capability Core Baseline)

Our IoT assurance services include secure boot validation, firmware signing verification and assessment of device lifecycle management practices.

Cyber risk management and threat modelling

We support energy stakeholders to identify, qualify and mitigate cyber risks through:

- threat modelling using STRIDE and attack tree methodologies tailored to DER architectures
- risk scoring based on CVSS and MITRE ATT&CK for ICS
- development of risk registers and mitigation roadmaps aligned with ISO/IEC 27005 and NIS2 Directive requirements

This enables informed decision-making and prioritisation of security investments.

Incident response and digital forensics

In the event of a security breach, we provide rapid-response capabilities, including:

- triage and containment of compromised DER assets
- forensic acquisition and analysis of device logs, memory dumps, and network traffic
- root cause analysis and attribution support
- post-incident reporting and regulatory liaison (e.g., with Ofgem or the National Cyber Security Centre (NCSC))

We also assist in developing and testing incident response playbooks specific to DER environments.

Security engineering and architecture reviews

We work with DER manufacturers and integrators to embed security into system architecture and product design. Services include:

- secure architecture reviews of DER control systems, edge gateways and cloud backends
- design of secure OTA update pipelines and key provisioning workflows
- implementation of zero-trust principles in DER network segmentation and access control
- support for achieving ‘security by design’ certification under emerging UK and EU regulatory frameworks

By integrating these capabilities, Resillion empowers energy sector clients to proactively defend against cyber threats, achieve regulatory compliance and build trust in a rapidly evolving digital energy landscape[15].

resillion

Policy and industry recommendations

The evolving threat landscape surrounding DERs necessitates a comprehensive and technically robust policy framework. As DERs become increasingly integrated into the UK's critical energy infrastructure, the absence of enforceable cyber security standards poses a systemic risk to grid stability, national security and consumer safety. The following recommendations outline a multi-layered approach to policy and industry reform, grounded in technical rigour and operational feasibility.

Mandate independent cyber security certification for DERs

A foundational step in securing the DER ecosystem is the implementation of mandatory, third-party cyber security certification for all grid-connected DER devices. This certification should be based on conformance to internationally recognised standards such as ETSI EN 303 645 and NIST IR 8259.

Certification must include:

- penetration testing of firmware and communication interfaces
- cryptographic protocol validation
- secure boot and firmware integrity checks
- evaluation of OTA update mechanisms
- authentication and access control assessments

Certification bodies should be accredited under a national scheme, potentially aligned with the UK Cyber Essentials Plus or an equivalent framework tailored for OT. This would ensure consistency, impartiality and technical depth in the evaluation process.

Establish a national DER vulnerability disclosure programme

To facilitate coordinated vulnerability management, the UK should establish a centralised DER Vulnerability Disclosure Programme (VDP). This programme would serve as a trusted intermediary between security researchers, manufacturers and grid operators. Key components should include:

- a secure submission portal for zero-day and known vulnerabilities
- defined timelines for vendor response and remediation
- public advisories for confirmed vulnerabilities with CVE assignments
- legal protections for good-faith researchers under a safe harbour policy

The VDP should be overseen by a national cyber security authority such as the NCSC, with integration into the UK's broader critical infrastructure threat intelligence ecosystem.

Incentivise secure procurement through government-backed schemes

To drive market adoption of secure-by-design DERs, the government should introduce procurement incentives for energy retailers, aggregators and consumers. These could include:

- tax credits or rebates for certified secure DER devices
- preferential treatment in capacity market auctions for aggregators using secure infrastructure
- inclusion of cyber security scoring in public procurement tenders for smart grid projects

Such incentives would shift the economic calculus for manufacturers and service providers, making cyber security a competitive differentiator rather than a cost centre.

Develop a DER cyber security maturity model

A DER-specific cyber security maturity model (CMM) would provide a structured framework for assessing and improving the security posture of DER manufacturers, operators and integrators. The model should define progressive levels of maturity across domains such as:

- governance and risk management
- secure software development lifecycle
- incident detection and response
- supply chain security
- compliance and audit readiness

The CMM could be modelled after existing frameworks such as the NIST Cyber Security Framework or the Cyber Security Capability Maturity Model but adapted to the unique constraints and architectures of DER systems.

Public-private collaboration on threat intelligence

Given the distributed and heterogeneous nature of DER deployments, effective threat detection and response require real-time information sharing across stakeholders. The UK government should facilitate the creation of a DER-focused Information Sharing and Analysis Centre, enabling:

- exchange of Indicators of Compromise and Tactics, Techniques and Procedures
- joint analysis of emerging threats and vulnerabilities
- collaborative incident response exercises
- development of shared detection rules and response playbooks

Participation should include DER manufacturers, DNOs, aggregators, cyber security vendors and government agencies. This collaborative model would enhance collective situational awareness and reduce the dwell time of adversaries within the energy ecosystem.

resillion

Building a resilient, secure energy future

The UK's energy transition hinges on the secure integration of DERs. Without robust cyber security, the benefits of decentralisation could be eclipsed by systemic vulnerabilities. A coordinated effort, spanning regulation, industry and research, is required to harden the distributed energy landscape.

At Resillion, we're ready to support this mission, offering the technical expertise, tools and partnerships necessary to secure the grid edge. By embedding security into every layer of the DER ecosystem, the UK can lead the world in building a resilient, cyber-secure energy future.

References

1. Researchers Uncover 46 Critical Flaws in Solar Power Systems - The Hacker News
2. Cyber security Challenges in the Renewable Energy Sector - EC-Council University
3. Cyber security Considerations for DERs - U.S. Department of Energy
4. A comprehensive survey on IoT - ScienceDirect
5. Reuters - Ghost Machine: Rogue Communication Devices in Inverters
6. 240801ttr-guidance-240325-clean.pdf Energy Networks Association
7. G99_Amd 8_A3.2.pdf Energy Networks Association
8. ETSI EN 303 645 - Cyber Security for Consumer IoT
9. PAS 1879 - Energy Smart Appliances: Cyber Security Requirements
10. Resillion - Secure Connected Device Assurance Scheme - Resillion
11. 192 Key Cybersecurity Statistics: Indusface
12. Q1 2025 Global Cyber Attack Report from Check Point Software
13. Heathrow and Spain Grid Outages - News Reports
14. Resecurity - Cyber Threats Against Energy Sector Surge
15. Resillion - Powerhouse Pentest-as-a-Service