Policy Proposal to Mitigate Cybersecurity Risks in Distributed Energy Resources and PV systems

***Authors**: Ryan Davidson, DNV; Jan Osenberg; Uri Sadot, SolarDefend*

This proposal sets out a framework for securing distributed energy resources (DERs), with a particular focus on photovoltaic (PV) systems, in line with the EU's broader objectives under NIS 2 and the Energy Union. Its purpose is to provide regulators and stakeholders with forward-looking guidance on how to safeguard the growing fleet of DERs against cyber-physical threats. By defining obligations for manufacturers, operators, aggregators and other service providers, and by clearly identifying those with remote access to large capacities of grid connected resources as critical infrastructure operators, the framework aims to ensure that the expansion of renewable energy in Europe strengthens, rather than weakens, the resilience of the electricity system.

The proposal addresses two risk categories:

1. Risks from **low technical cybersecurity baselines**, which can result in unauthorized access to large numbers of DERs
2. Risks of DER systems being misused by **politically motivated foreign actors**, with implications for energy sovereignty.

It accounts for the fact that device manufacturers and service providers can equally control critical amounts of capacity and threaten grid stability.

Contents

Overview of the proposal

- Section A defines the scope. In scope are companies with access to an aggregated capacity surpassing ECII thresholds. They are classified as critical entities and must comply with requirements in the proposal.
- Section B creates a market-based security layer, called "Trusted Entities" between the controlling entity and the device. It ensures that all commands with potentially disruptive impact on the electricity grids are checked and approved. It'll ensure updates contain no backdoors, based on a procedure set out in section E.
- Section C creates the governance for the Trusted Entities.
- Section D defines organisational requirements, covering supply chain due diligence, personnel security and data hosting. The definition complements NIS2 and the NCCS.
- Section E defines technical requirements which complement the CRA. Among others, it mandates secure sections inside devices which contain critical functionalities. They're called "Trusted Execution Environments" and can only be altered with oversight of a Trusted Entity. The proposal also requires a secure reboot functionality of the devices.

The annex contains best practices, where the core ideas are already implemented:

- From India and South Australia which are both implementing a security layer between the commands and the devices.
- From the automotive industry which has implemented Trusted Execution Environments.

Definitions

1. *"**Fail-safe operation**"* means the ability of a system, device, or process to default to a predefined state that ensures the safe and secure functioning of the system and prevents harm to human safety, network stability, or critical infrastructure, in the event of a fault, loss of communication, security compromise, or other abnormal operating condition.
2. *"**Secure remote reboot**"* means the remote restarting of a device using encrypted and authenticated communications, with access control and integrity checks to prevent unauthorised or unsafe activation.
3. *"**Predefined safe mode**"* means a restricted operational state that a device enters after reboot or failure, limiting grid interaction until secure reconnection is verified by an authorised operator.
4. *"**Critical sub-supplier**"* means any third party whose products or services, if compromised, could significantly affect the cybersecurity, functionality, or safety of a distributed energy resource system.
5. *"**Trusted Execution Environment (TEE)**"* means a secure and isolated execution environment within a device that contains all functionalities necessary to ensure its safe and continuous operation, which cannot be altered without explicit approval by the Trusted Entity.
6. *"**Aggregate command**"* means a command that, while individually harmless, when executed simultaneously across multiple devices, could endanger the stability of the electricity system.

Principle A – Responsible Parties

1. The following shall be classified as Critical Entities if they control or have remote access to power levels that meet or exceed the ECII (electricity cybersecurity impact index) thresholds defined in the Network Code for Cybersecurity and related methodologies:
    1. Manufacturers of inverters and DER devices, including firmware and software providers with remote access or update capabilities;
    2. Installers, Asset Owners, EPC contractors, Operation & Maintenance Service Providers of DER sites, and service providers responsible for commissioning, maintaining, or remotely accessing DER systems;
    3. Aggregators, Virtual Power Plant (VPP) operators, and flexibility service providers capable of controlling aggregated DER fleets;
    4. Operators of electric vehicle recharging infrastructure and electric heating, where such infrastructure contributes to aggregated load or generation capacity;
    5. Managed Security Service Providers (MSSPs) and critical ICT service providers supplying cybersecurity functions to any of the above;
    6. Third-party software and cloud service providers offering monitoring, analytics, or command-and-control functionality for DER systems.
2. Critical Entities shall comply with the requirements of the EU Directive 2022/2555 (NIS2).
3. All Critical Entities who are unable to fulfil the obligations of that role, are required to either permanently disable their remote access, or obtain access only through a relevant third party who meets the criteria of a critical entity.
4. Entities that, by financial or contractual control, significantly influence cybersecurity-related risk decisions of critical Entities shall be classified as *Important Entities with Extended Liability*. This includes, in particular, entities that:
    1. define technical or operational requirements for DER deployment;
    2. set insurance or financing conditions linked to cybersecurity; or
    3. determine capital or operational expenditure with direct cybersecurity impact.
5. Important Entities with Extended Liability shall:
    1. cooperate with Critical Entities in fulfilling obligations under this Regulation;
    2. be subject to notification, supervision, and enforcement in accordance with Directive (EU) 2022/2555 (NIS2).
6. National Competent Authorities shall have the authority to audit, sanction, or suspend operational licenses of non-compliant entities.

Principle B – Trusted Entities as a Backup Security Layer

1. Scope.
   This requirement applies to distributed energy resources (DER) and associated control systems whose operation, individually or in aggregation, may affect the stability or security of the Union's electricity system. It complements the obligations set out in Directive (EU) 2022/2555 (NIS2), the Network Code on Cybersecurity, and Regulation (EU) 2023/1230 (Cyber Resilience Act).

2. Designation of Trusted Entities.

   a) Each Member State shall ensure the accreditation of one or more *Trusted Entities* (TEs) by the competent authority designated under Article 57 of Directive (EU) 2019/944.

   b) A Trusted Entity shall act as the exclusive intermediary for grid-relevant commands, telemetry, and firmware or software update workflows for DER connected to its portfolio of sites.

   c) At the time of grid connection, each customer shall nominate a Trusted Entity for its installation. Users may switch Trusted Entities at any time; the previously nominated TE shall transfer all relevant credentials and bindings within 30 days.

   d) Trusted Entities shall implement mandatory standard interfaces enabling users to switch providers. All device credentials, cryptographic keys, and configuration data shall be transferable within 30 days. Trusted Entities shall not impose exit fees or any restrictions on the transfer of such regulated data or keys.

   e) Where a Trusted Entity is affiliated with an Original Equipment Manufacturer, Virtual Power Plant operator, or Distribution System Operator, it shall ensure operational and accounting separation of its activities as a Trusted Entity. Such entities shall apply non-discriminatory access conditions and publish wholesale terms for their services.

3. Access management:

   a) Remote access must be managed by a Trusted Entity via controls determined through a risk assessment.

   b) Local access shall include role based access and critical tasks shall only be made available to trained service personnel.

4. A Trusted Entity shall:

   a) register devices and bind them securely to the installation identifier, assigning digital certificates;

   b) monitor commands addressed to devices and block, stagger or rate-limit those which, while individually harmless, may in aggregate endanger system stability;

   c) enforce staged deployment of updates with rollback capability. Over-the-air updates shall be performed before or after system reaches 30% of its peak production, to minimize grid disturbance in case of error.

d) ensure that over-the-air updates are authenticated, cryptographically verified, and, where affecting the Trusted Execution Environment or other regulated functions, explicitly approved by the Competent Authority;

e) maintain continuous audit trails of telemetry, commands, and updates;

5. Security and integrity requirements. Trusted Entities shall comply with the following:

a) Any private party may apply to become a Trusted Entity, subject to governance safeguards ensuring neutrality, including conflict-of-interest rules and fair access terms. They shall be established in the Union, not directly or indirectly controlled by entities established outside the Union, and remain under the full ownership and effective control of Union stakeholders. Minority shareholdings by entities established outside the Union shall not constitute control, provided such shareholdings do not confer decisive influence.

b) certification under the latest revision of ISO/IEC 27001 or equivalent, with annual independent penetration testing;

c) strong device identity binding, mutual authentication, and encrypted communications;

Principle C – Oversight and Liability of Trusted Entities

1. Central policy and safe harbour.
   The Commission shall, by implementing acts, define machine-readable aggregate-risk thresholds, stagger rules, interoperability testing requirements, and emergency measures. Trusted Entities shall enforce such rules without deviation and shall not bear liability for systemic consequences when acting in compliance.

2. Supervisory access.
   Trusted Entities shall, upon request, provide National Competent Authorities, ENISA and ACER with real-time, read-only API access to:

   a. command and policy-engine decisions, including allow/deny reason codes;

   b. firmware/update ledgers (hashes, signatures, deployment stages);

   c. service-level metrics, including uptime and latency;

   d. incident tickets and status.

3. Accreditation renewal and re-evaluation.
   Accreditation shall be renewed annually and re-evaluated after mergers, acquisitions or material investment changes. Renewal shall require independent certification to the latest ISO/IEC 27001, SOC 2 Type II, or equivalent.

4. Stress testing.
   Trusted Entities shall participate annually in curtailment, rollback and failover drills organised by the Competent Authority and submit results to the Commission, ENISA and ACER.

5. Risk-based supervision.
   National Competent Authorities shall classify Trusted Entities into supervisory tiers according to ECII exposure; higher tiers shall be subject to increased reporting cadences, on-site inspections and heightened capital and insurance requirements. Non-confidential supervisory scorecards shall be published.

6. Incident reporting.
   Trusted Entities shall submit an early-warning notification within 24 hours of any significant incident and a final report within NIS2 deadlines, including fields specific to aggregate-command events, update rollbacks and policy-engine exceptions.

7. Supervisory decision rights.
   National Competent Authorities may issue binding instructions to Trusted Entities in emergency circumstances. Trusted Entities shall execute such instructions immediately and maintain complete audit records.

8. Enforcement.
   Competent Authorities shall condition grid connection and continued operation of

DER relying on Trusted Entities on compliance with sections D and E, and may order denial or disconnection in case of material non-compliance.

9. Union coordination.
   An EU-level coordination mechanism involving ENISA, ACER and National Competent Authorities shall be established to harmonise supervisory practices, approve aggregate-risk parameters and publish annual reports on the functioning of Trusted Entities.

Principle D – Organisational Obligations to Prevent Cyber Incidents

1. Supply chain security.
    1. Critical entities in the DER industry shall, through risk assessment, identify their critical sub-suppliers, as is common practice across in the non-distributed energy industry. This applies particularly to DER site firewalls, secure gateways, SCADA systems, industrial controllers and PV inverters and for their critical sub-components such as embedded modems, CPUs and other remote-access modules such as Wi-Fi or Bluetooth chipset.
    2. Critical Entities shall ensure the security of procured services, applications, and hardware via contractual arrangements with their sub-suppliers.
    3. Critical Entities shall maintain an approved supplier list of critical components or follow products listed by ENISA in an EU database.
2. Personnel security and insider threats: Personnel with direct or indirect access to DER software or firmware that exceeds ECII criteria must be subject to appropriate vetting, including background checks, consistent with operators of critical infrastructure.
3. Data hosting and access.
    1. Control applications and grid-relevant data shall be hosted only in secure data centres located in the EU or a country recognized under the Adequacy Decision based on Article 45 of Regulation (EU) 2016/679.
    2. Critical Entities shall manage operational commands and remote access portals within the EU or trusted partners. Maintenance of core hardware components (e.g., inverters, meters, RTUs) via software or firmware updates are to be considered as a form of operational command.
    3. Control applications of DER that exceed ECII criteria shall be stored and operated in secure cloud or backend environments, consistent with EUCS (EU Cloud Security Certification Scheme).
4. Process integration.
    1. Critical Entities shall cooperate with Competent Authorities and the Trusted Entity operator established in section D.
    2. They shall ensure that devices they place on the market or operate meet the technical requirements set out in section E.
    3. Member States shall encourage Critical Entities to benchmark their systems and internal operations to those of other high-criticality industries such as the banking industry, defence, health or aerospace

Principle E – Technical Obligations for DER Cybersecurity

1. The following core components shall be classified as critical products under CRA Annex IV when applied to DER sites above ECII thresholds: firewalls, secure gateways, SCADA systems, industrial controllers, PV inverters, switching gear, transformers, BESS systems and other components that serve critical functions in the operations of DER and DER sites (exact list to be determined).
2. Device registration and identification
    a) All DER devices larger than a size yet to be determined (e.g., prosumer DER installations above 4.2kW, if the DER is remotely controlled and exists in large concentrations on the grid) must be registered with a Trusted Entity before grid connection.
    b) Critical entities shall carry a full asset inventory of their DER, consistent with NIS2 requirements, to the component level.
3. Communication protocols
    a) All digital communication, including over-the-air updates shall pass through the Trusted Entity.
    b) Communications to a DER or DER site shall only be made with end-to-end encryption and upon mutual authentication.
4. Telemetry and reporting
    a) Devices shall transmit logs of power output.
    b) Devices shall transmit logs of internal network traffic, where applicable, and primarily for forensic and post-mortem capabilities after a breach.
    c) Devices shall transmit telemetry at intervals defined by the Commission in collaboration with relevant stakeholders, including power output, voltage, frequency, availability, fault codes, firmware version upon the creation of a repository at the union-level.
    d) Data schemas and cadences shall be harmonised across the Union.
5. Trusted Execution Environment (TEE)
    a) Each device shall include a TEE ensuring safe and continuous operation, for example via secure enclaves, secure boot, or secure storage.
    b) The TEE shall always guarantee basic functioning, regardless of other software components.
    c) Updates must be auditable and may not alter or disable the TEE without Trusted Entity approval.
    d) The Commission shall, by means of an Implementing Act, define the functions included in the TEE, covering at minimum, cryptographic functions, power output control, frequency measurement, voltage measurement, and emergency response.

e) Critical entities shall provide auditable documentation of security-relevant or operationally significant software changes that do not affect the TEE.

6. Over-the-air updates: Updates must be cryptographically signed and verified.
7. Logging and incident response
    a) Devices and operators shall log performance-altering commands, updates, and telemetry.
    b) Logs for the previous 6 months must be securely stored, immutable and be made available to competent authorities upon request.
    c) Logs shall be in a standard format and capable of forwarding and aggregation in standard cyber security monitoring tools.
    d) Commands that can negatively influence grid stability will be postponed when the DER senses preconditions of weakened voltage or frequency signal, when possible (if a PV inverter receives a command to shut-down when voltage levels are above range, the reboot order will be deferred)
8. Secure Remote Reboot
    a) Devices shall support secure remote reboot and hard reset functions via authenticated and encrypted channels. Trusted Entities shall ensure blackout robust communications and operation of devices to facilitate remote restart after network restoration.
    b) Devices shall implement role-based access control to ensure that only authorised operators may initiate reboot commands.
    c) Devices shall include a secure, cryptographically protected boot partition that verifies firmware integrity at start-up and, in case of failure or loss of communication to the Trusted Entity, automatically triggers rollback or enters a predefined safe mode. This mode shall prevent reconnection to the electricity grid until verified by an authorised operator and shall be protected against unauthorised modification.
    d) The fail safe mode shall only be configurable by authorized personnel and align with local system operators and Trusted Entity operating procedures.
    e) Devices shall log and audit all remote reboot or reconfiguration commands, and such logs shall be securely stored and made available to competent authorities upon request.

Annexe

Best practice: India's national Remote Monitoring System (RMS) for solar inverters

India's Ministry of New & Renewable Energy (MNRE) has issued draft guidelines that require every grid-connected PV inverter (starting with the PM Surya Ghar rooftop program) to connect directly to a central, India-hosted platform - the National RMS - instead of OEM clouds. MNRE (or a designated agency) operates the platform.

OEMs, EPCs/installers and other suppliers under PM Surya Ghar must onboard devices and integrate their inverter communication devices / dongles / data loggers with the National RMS according to the MNRE spec. Industry testing/onboarding begins Sept 1, 2025 (RMS side) with staged rollout.

How the security & comms architecture works

- Strong identity & mutual auth: Each RMS device is registered by IMEI; the national platform issues a client certificate bound to that IMEI. Devices authenticate with TLS/SSL client certificates (or username/password as fallback).
- Transaction-level protection: Every message carries a time-bounded one-time password (OTP); messages without valid OTP are dropped.
- Encrypted transport: Payloads are AES-256 encrypted and carried over TLS/SSL; the platform runs a private TLS/SSL VPN to resist interception/MiTM.
- Trusted routing: Communication uses M2M SIMs under Indian telecom rules to enforce known network paths and device identities.
- Protocols: Field buses: Modbus-RTU (inverters, DAQ) and DLMS/Modbus (meters). Uplink: MQTT (IEC20922) over cellular 4G/5G (fallback 2G).

Telemetry, commands & topics (what flows, and how)

- Topic model: Devices publish/subscribe only to authorized MQTT topics (info, OTP, heartbeat, data, on-demand, config). Authorization is tied to issued credentials.
- Data cadence: Periodic push (e.g., inverter data every 5 min), event-driven alarms, on-demand read for retrieval and on-demand write/config-over-the-air for controlled parameter changes.
- Onboarding & lifecycle: Vendors register IMEIs; a secured API returns the client cert, credentials, Device-Management-Server URL, and topic map. Certificate renewal is handled per the spec (download via authenticated file service).

What risk this mitigates (and why it matters)

- Removes unilateral OEM control: Because all commands and updates traverse the national RMS with mutual auth + OTP + topic authorization, OEMs/VPPs cannot issue hidden "kill-switch" or mass-shutdown commands from their own clouds. Actions are auditable and attributable under Indian jurisdiction.
- Data/sovereignty by design: Operational data and command-and-control remain on India-based service run by (or for) MNRE, reducing exposure to extra-jurisdictional control.

Compliance & wider regulatory hooks

- Testing timeline & conformity: MNRE's notice sets integration/testing windows and stakeholder comment periods; OEMs must pass interface and security checks to go live.
- Product conformity (separate track): Inverters remain subject to India's BIS/QCO regime (e.g., IS16169, IS 16221, QCO 2025) for quality/safety - complementary to the RMS comms/cyber stack.

Continues on next page

Continuation

What's not explicitly in the draft
The draft RMS spec governs communications, identity, routing, and command mediation. It does not mandate source-code escrow or pre-publication audit of firmware updates; those risks are instead mitigated by command gatekeeping, identity, and auditability on the RMS. (This is an inference from the draft's scope.)

Primary sources

- MNRE Draft Guidelines: RMS Communication & Security Architecture (PDF). (Security model, IMEI-bound certs, OTP, MQTT topics, data/command flows.)
- MNRE Notice page (consultation window, access to draft). Ministry of New and Renewable Energy
- Mercom India (testing from Sept 1, 2025; M2M SIM, AES-256/TLS, IMEI/cert/OTP flow).
- NDTV Profit / Economic Times (national servers in India; managed by/for MNRE).

Best practice: South Australia's "Relevant Agent" model as a security layer for DER control

What it is (legal basis & scope)
South Australia's *Smarter Homes* regulatory changes (in force since **28 Sept 2020**) require every **new or upgraded** grid-connected solar (and certain batteries/DER) installation to nominate a **Relevant Agent**. The Relevant Agent is an accredited third party (which can be **SA Power Networks (SAPN)** or approved companies) that holds the *exclusive right and obligation* to **remotely disconnect/reconnect** the system on instruction from the **state government, SAPN (the DSO), or AEMO** during security events.

Dynamic export control (from 1 July 2023)
A second layer—the **Dynamic Export Requirements**—mandates that new exporting systems be **capable of remote, real-time export-limit updates** and be **compatible with SAPN's Flexible Exports** service. Export limits are raised or lowered automatically to match local network capacity, reducing curtailment while preserving system security.

How the Relevant Agent layer works (process & roles)

- **Nomination at connection:** The customer/installer nominates a **Relevant Agent** during the SAPN connection (SEG) application. SAPN itself can act as agent, or the customer can appoint an **approved private agent** from the government list.
- **Authorised command path:** Inverters (or site gateways) are integrated so that **remote disconnect/reconnect** and **export-limit commands** are accepted **only** from the nominated agent—*not* directly from the OEM cloud. Agents act **on instruction** from SAPN/AEMO/government in emergencies or for network management.
- **Technology coverage:** SAPN publishes **supported technology lists** and commissioning guides (e.g., Fronius, SolarEdge, Alpha ESS). Where needed, certified **site devices** (e.g., Wattwatchers) provide the switching/control interface under the agent's control.
- **Terms & responsibilities:** SAPN's **Relevant Agent Appointment Terms** set customer and agent obligations, including fault handling and ensuring the site remains controllable for emergency actions.

Continuation on the next page

Continuation from previous page

Cybersecurity posture (governance + technical)

- **Governance separation:** By design, **OEMs/VPPs cannot unilaterally shut down** fleets; only **accredited agents**—operating under SA Government/SAPN/AEMO direction—can issue grid-impacting commands. This breaks potential single-vendor "killswitch" risk.

- **Minimum security controls:** SAPN consulted on **Dynamic Exports Cyber Security Requirements** for technology providers to harden identity, authentication and communications for flexible exports integrations. (Consultation closed Oct 2023; requirements underpin agent-to-device control channels.)

What's not explicitly in the draft
The draft RMS spec governs communications, identity, routing, and command mediation. It does not mandate source-code escrow or pre-publication audit of firmware updates; those risks are instead mitigated by command gatekeeping, identity, and auditability on the RMS. (This is an inference from the draft's scope.)

Primary sources
- MNRE Draft Guidelines: RMS Communication & Security Architecture (PDF). (Security model, IMEI-bound certs, OTP, MQTT topics, data/command flows.)
- MNRE Notice page (consultation window, access to draft). Ministry of New and Renewable Energy
- Mercom India (testing from Sept 1, 2025; M2M SIM, AES-256/TLS, IMEI/cert/OTP flow).
- NDTV Profit / Economic Times (national servers in India; managed by/for MNRE).

Best Practice: Trusted Execution Environments (TEEs) in the Automotive Sector

Modern vehicles integrate between 30–100 Electronic Control Units (ECUs), linked by in-vehicle networks. Safety-critical ECUs (braking, steering, airbags, battery management) coexist with non-critical systems (infotainment, navigation, connectivity). This convergence creates a high cybersecurity risk: attackers could exploit weak entry points (Bluetooth, Wi-Fi, infotainment) to access and manipulate critical functions. To mitigate this, the automotive sector has introduced **Trusted Execution Environments (TEEs)**, isolating essential functions in a secure enclave that cannot be altered without authorised approval.

Implementation in Vehicle Models
Several leading manufacturers already deploy TEEs in production vehicles:

- **Tesla**: integrates hardware-based enclaves to protect OTA (over-the-air) firmware updates, ensuring safety-critical ECUs (e.g. Autopilot control, battery management) cannot be overwritten by malicious software.

- **Volkswagen, Ford, BMW**: use **NXP's S32G processors** with ARM TrustZone TEEs in vehicle gateways, securing cryptographic keys, update verification, and communication integrity between ECUs.

- **Renesas & Continental/Bosch ECUs**: supply automotive-grade SoCs and control units that implement TEE-based partitioning. These isolate functional safety domains (braking, airbags, steering) from infotainment and third-party applications.

Continuation on the next page

Continuation from previous page

- **Qualcomm Snapdragon Automotive Platform**: deployed in models by General Motors and Mercedes, leverages TrustZone to separate telematics, infotainment, and safety-critical communications.

These integrations ensure that **critical driving functions remain protected**, even if non-critical software layers are compromised.

Applications of TEEs in Vehicles

- **Firmware integrity**: critical software (e.g. braking logic, steering assistance) runs inside TEEs and verifies signatures at boot.
- **Secure OTA updates**: TEEs guarantee rollback protection and staged deployment.
- **Key management**: storage of cryptographic identities used for vehicle-to-infrastructure (V2X) communications.
- **Fail-safe behaviour**: TEEs enforce predefined safe states when faults or abnormal commands occur.

Regulatory Drivers

The use of TEEs in automotive systems is driven by binding international regulation and standards:

- **UNECE WP.29 Cybersecurity Regulation (UN R155)** – mandatory since July 2022 for all new vehicle types sold in the EU, Japan, South Korea and many other markets. Requires automakers to implement a **Cybersecurity Management System (CSMS)** and protect against risks from OTA updates, supply chain vulnerabilities, and cross-domain compromise. While not naming TEEs explicitly, the regulation mandates effective partitioning of safety-critical functions from external threats, which TEEs deliver in practice.
- **ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering, 2021)** – establishes lifecycle obligations for secure design, risk management, and update integrity. The standard explicitly requires protection of safety-critical domains from compromise of non-critical systems, reinforcing the TEE approach.
- **ISO 26262 (Functional Safety, 2018 revision)** – addresses fail-safe and redundancy requirements for safety-critical ECUs. TEEs are increasingly used to fulfil these cybersecurity-relevant safety obligations.

Key Takeaway

The automotive sector provides a concrete, real-world example of how TEEs can secure distributed, safety-critical assets. **By isolating essential functionalities in hardware-based trusted environments**, automakers prevent malicious or faulty updates from destabilising vehicles. This approach is now embedded in vehicle design worldwide, supported by UNECE R155 and ISO/SAE 21434. For the energy sector, TEEs can serve a similar role in distributed energy resources (DER), guaranteeing that inverter safety functions (frequency, voltage, emergency response) remain uncompromised, even under cyberattack or flawed update rollouts.