EDITH COWAN UNIVERSITY

Australian Research in Power System Transformation

Topic 9-2 – Power System Cybersecurity

Interim Report: Securing Distributed Energy Resources (DER) Stability via Trusted Sovereign Monitor (TSM)

Commonwealth Scientific and Industrial Research Organisation

17 December 2025

Contents

1. Introduction

Australia's energy transition is entering a phase where distributed energy resources (DER) are not merely peripheral contributors but central actors in power system behaviour. The rapid deployment of Electric Vehicle Supply Equipment (EVSE) exemplifies this shift. Physical rollout continues at pace; however, the institutional, regulatory, and security frameworks needed to manage their integration lag behind. This creates an adoption-framework gap where vast fleets of technically heterogeneous, internet-connected devices enter the system with security postures designed for a substantially different era of power system operation [1]. In this environment, insecure or compromised DERs, including EV chargers, can act as "trojan horses," initiating destabilising behaviours from inside the trusted perimeter of the grid.

This risk was foreseen in CSIRO's *Australia's Research Roadmap for Power System Transformation* (2021), where Topic 9 (DERs and Stability) [2,3] identifies the need for advanced modelling of fast DER responses, improved understanding of aggregate behaviours under disturbance, and mechanisms to ensure system operators can maintain security under very high DER penetrations. Subsequent analyses under Topic 9 demonstrate that inverter-based resources can respond in milliseconds to disturbance events, often unpredictably, and that inadequate device compliance or untrusted firmware can amplify stability risks. EV charging loads, with their high power-ratings and synchronised operational profiles, were explicitly identified as both an emerging opportunity and a major threat to system stability if left ungoverned.

Stage 5 of this research program builds on these foundations by addressing a gap that the original roadmap did not fully anticipate in 2021: the cybersecurity–stability convergence [3]. As DER fleets grow and software-defined functionality becomes ubiquitous, the threat landscape now includes malicious or erroneous actions initiated through compromised OEM platforms, cloud services, or device firmware [4]. Ensuring system security under such conditions requires not only improved models but also new architectural safeguards embedded directly within DER devices.

Our research to analyse threats to EV-Charging infrastructure and design and develop a Trusted Sovereign Monitor (TSM) responds to this need. It introduces a verifiable, tamper-resistant oversight component embedded within EVSE hardware that operates independently of OEM or Charge Point Operator (CPO) backends. Functioning as a high-integrity "safety bus," the TSM continuously evaluates charger behaviour against grid-safety and security policies and can intervene when unsafe, non-compliant, or destabilising actions are detected. Even if primary firmware or external cloud services are compromised, the TSM enforces sovereign-level constraints that provide assurance and vetting capabilities to regulators to uphold overall system security in the context of large-scale DER penetration of the electricity grid.

This work aligns directly with Topic 9 Stage 5 objectives by:

- providing mechanisms to ensure secure and compliant DER behaviour under disturbance;
- enabling future modelling of controlled versus uncontrolled charger responses;
- safeguarding aggregate load behaviour to prevent large, fast load swings initiated by adversaries;
- supporting the broader G-PST vision of maintaining system operability and resilience in the context of state-level cyber-attacks.

2. Research completed

The Interim Report: Securing Distributed Energy Resources (DER) Stability via Trusted Sovereign Monitor (TSM) project is relatively small, exploring the threats, architecture choices and develops a prototype to demonstrate the feasibility of a TSM approach that governs DER cyber security. The research is undertaken by Edith Cown University.

Research completed under Topic 9 (DERs and Stability) [5,6] in earlier stages established a detailed understanding of how distributed energy resources behave during power system disturbances. Laboratory benchmarking and field data analyses showed significant variability and widespread non-compliance in inverter responses, with more than half of devices disconnecting or curtailing unexpectedly during voltage or frequency events. These inconsistent behaviours, coupled with limited operational visibility of DER fleets, highlighted that large numbers of devices can respond in synchrony and trigger load or generation changes larger than the system's largest credible contingency. Stage 4 modelling efforts, including development

of composite load DER models, further demonstrated that such coordinated DER responses can materially challenge power system security, even in the absence of malicious intent.

While this body of work advanced Australia's capability to represent, model and manage DER disturbances, it implicitly assumed that devices behaved incorrectly due to design limitations, non-compliance, or poorly tuned control parameters. What it did not address is the possibility of an *active agent* deliberately manipulating DER devices to induce instability. In other words, previous stages characterised the symptoms of unpredictable DER behaviour but did not consider cybersecurity as a driver, nor did they contemplate scenarios in which inverter-like behaviours, such as rapid disconnection, unexpected ramping, or synchronised load steps, could be orchestrated intentionally to disrupt the power system.

The Trusted Sovereign Monitor (TSM) work extends the Topic 9 program into this unaddressed and increasingly critical domain (Topic 9-2). It responds directly to the visibility and compliance gaps identified in Stage 4 by proposing a mechanism that provides verify able, device-level oversight of DER operation, independent of OEM or aggregator control. Whereas prior work improved models of how DER behave, the TSM initiative tackles the deeper question of how DER *should be governed* when their behaviour cannot be assumed trustworthy. By introducing a secure, tamper-resistant monitoring and enforcement layer within the device, the TSM enables system operators and regulators to ensure that DER actions remain within safe operational envelopes, even in the presence of compromised firmware, untrusted supply chains, or adversarial control signals.

In this way, the TSM is the natural and necessary progression of the Topic 9 stability work: it transforms insights about non-compliance and unpredictability into a concrete architectural response that addresses both inadvertent and malicious destabilising behaviours. It fills the missing cybersecurity dimension in the DER stability research program and provides the foundations for protecting the future system as high-penetration DER becomes increasingly software-defined, externally controllable, and therefore vulnerable to coordinated cyber-physical attack.

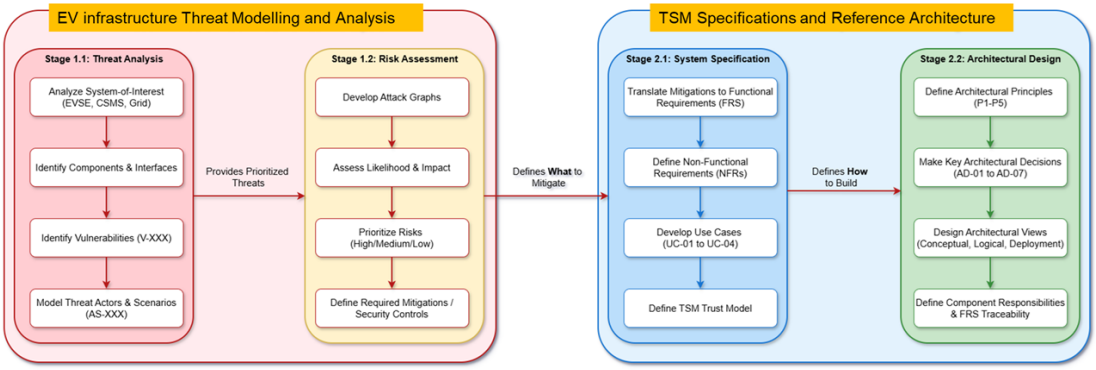

Figure 1: EVSE Evidence-based threat modelling towards TSM Specifications and architecture development.

Across Phase 1 and 2 of the project, three major workstreams have been completed: (1) a comprehensive threat analysis of EVSE as a DER asset; (2) the development of the Trusted Sovereign Monitor (TSM) system specification and reference architecture; and (3) the development of a high-fidelity cyber-physical co-simulation platform to validate TSM capabilities under realistic grid and adversarial conditions. Together, these outputs represent a structured progression from problem discovery to architectural design (see Figure 1) to empirical evaluation capability. They establish the technical basis required to transition into full TSM implementation and provide the critical linkage to DER stability, notably addressing issues of non-compliance, fleet-level invisibility, and the emerging need to reason about active cyber adversaries rather than passive device malfunction.

The TR1 (*Threat Analysis of EVSE as a DER Cyber-Physical Asset*) report provides a rigorous, risk-driven threat analysis of Electric Vehicle Supply Equipment (EVSE) as a high-wattage, internet-connected DER node. Although the public version is redacted and only available on request, the underlying analysis spans more than 100 pages of technical detail, including system decomposition, attack-surface identification, protocol scrutiny, firmware supply-chain exposure, and failure-propagation pathways. The work catalogues vulnerabilities across hardware, firmware, communication protocols (OCPP, ISO 15118, IEC 61850), backend integration, and aggregator coordination. A set of formal attack graphs and a structured risk matrix identify the highest-impact scenarios, including remote firmware compromise, large-scale botnet-driven load manipulation, policy-bypass resulting in unsafe charging envelopes, spoofed attestation, and coordinated timing attacks. These threats directly map to DER stability concerns: mass synchronised load changes, malicious V2G injections, and the loss of operator control during peak periods. Critically, TR1 establishes that existing compliance mechanisms lack verifiable enforcement at the device level and provide no defence against an active adversary intentionally manipulating DER behaviour. These findings motivate the need for a sovereign, embedded trust anchor capable of enforcing grid safety behaviour in a non-bypassable manner.

Building on the threat landscape, TR2 (*TSM System Specification and Reference Architecture*) translates identified risks into a formalised system specification and complete TSM Reference Architecture. The report defines functional requirements, non-functional constraints, and four core use cases: sovereign-validated firmware updates, enforcement of grid-safety policies, remote attestation, and fail-safe shutdown.

The architecture introduces a dual-domain security model separating the Low Integrity Domain (LID) from the High Integrity Domain (HID). The HID hosts the Trusted Sovereign Monitor itself, anchored by a hardware root-of-trust enforcing secure boot, authenticated firmware provenance, and runtime integrity verification. A Policy Enforcement Engine (PEE) interposes between operational logic and physical actuators, ensuring device behaviour cannot exceed authorised grid safety envelopes. This directly addresses non-compliance behaviours previously observed in DER fleets and mitigates the lack of sovereign visibility into the devices' state. The architecture includes comprehensive network, data-flow, and deployment views, along with hooks for co-simulation validation, including firmware-distribution channels, attestation pathways, anomaly-logging, and grid-impact evaluation. Collectively, TR2 formalises the technical foundation required to implement a non-bypassable, verifiable trust layer for DER devices, which is an essential prerequisite for stabilising high-penetration DER environments in the presence of adversarial behaviours.

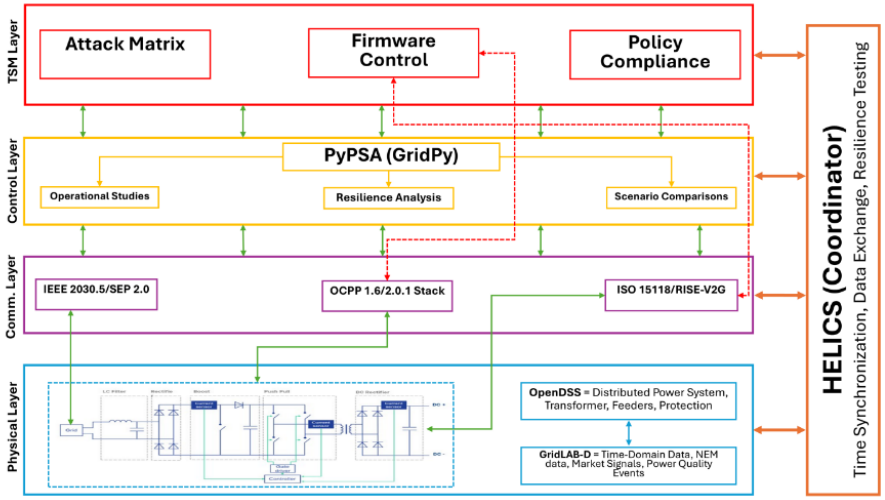

Figure 2: Layered Architecture of the Co-Simulation Platform

The PR1 report (*Co-Simulation Platform for Cyber-Physical Validation of TSM*) delivers a sophisticated, extensible cyber-physical co-simulation platform integrating OpenDSS, GridLAB-D, PyPSA, and HELICS into a unified environment capable of modelling EVSE behaviour (see Figure 2), distribution-network impacts, protocol-level interactions, and cyber-attack scenarios. The platform supports realistic modelling of DC fast-charging, fleet-scale interactions, firmware update mechanisms, battery dynamics, and communication protocols (ISO 15118-20, OCPP 1.6J, IEC 61850), with extensibility to IEEE 2030.5, OpenADR, OSCP and others. TSM-specific integration points allow testing of secure boot flows, attestation logic, PEE decision-interception, anomaly detection, and policy enforcement under adversarial stress. The platform evaluates device-level and fleet-level impacts using IEEE 13, 34, and 123-bus networks, enabling assessment of DER-induced voltage deviation, frequency perturbation, signalling delays, integrity failures, false-data injection, and coordinated malicious load attacks. This provides the experimental environment required to quantify the stabilising effect of TSM mechanisms, validate attack-response capabilities, and compare compliant versus adversarial operating conditions. It also forms the basis for future digital twin capability, supporting ongoing validation of EVSE behaviour at scale.

3. Outstanding activities

With the foundational stages of the project completed, the remaining work now focuses on the detailed design and implementation of the Trusted Sovereign Monitor (TSM) prototype and its progressive integration into the co-simulation environment. The architecture, requirements, and validation platform produced to date have established a solid technical base. The co-simulation environment has been deliberately structured with stubbed TSM components, allowing the project team to replace these placeholders incrementally with fully functional modules as development proceeds. This creates a controlled

pathway to transition from abstract architectural concepts to operational, testable software and hardware logic that can be evaluated under realistic scenarios.

Development follows an agile, iterative process in which each TSM capability is implemented and validated through short cycles anchored around specific use cases. The first of these is the firmware trust and secure update use case, which underpins all subsequent TSM functionality. Establishing a verifiable chain of trust for firmware provenance, ensuring that only authenticated code runs on the device, and detecting any attempt to bypass or tamper with this process provides the essential foundation for runtime integrity, policy enforcement, attestation, and anomaly detection. Once this cornerstone capability is operational, it is integrated into the co-simulation platform, replacing the corresponding stubbed behaviour and enabling immediate evaluation of its correctness and performance. Subsequent use cases, including runtime behavioural monitoring, grid-safety policy enforcement, and remote attestation, are approached in the same iterative manner. With each cycle, the fidelity of the simulated system increases, allowing the platform to transition progressively from a conceptual environment to a robust testbed capable of exploring adversarial behaviour, coordinated DER responses, and policy enforcement under realistic system loads.

The co-simulation platform developed earlier in the project is well-suited to this mode of iterative integration. It already provides detailed models of EV charging behaviour, distribution-network impacts, protocol interactions, and cyber attack pathways. As TSM logic replaces the placeholder components, the platform allows for controlled testing of its behaviour under a broad range of operational and adversarial scenarios. This includes evaluating how the TSM intervenes when the charger receives malicious commands, enforcing non-bypassable safety envelopes, validating attestation flows, and assessing the overall stabilising effect of the TSM on grid behaviour. In doing so, the platform becomes not only a technical validation tool but the primary means through which the prototype's efficacy, limitations, and implementation challenges are systematically explored.

Alongside the technical development, the project is also cultivating its dissemination and engagement pathways. Through the CSIRO and AEMO program forums, the team continues to build awareness of the risks identified in earlier stages and the practical value of the TSM as a device-level mechanism for ensuring DER compliance with system security requirements. These formal program channels are being complemented by broader engagement with national and state-level stakeholders who have responsibilities across cybersecurity, critical infrastructure protection, and supply-chain assurance. Connections into the Australian Signals Directorate, Defence, Home Affairs, and state government agencies are being developed to position the TSM within a wider national conversation on securing distributed energy systems. These bodies recognise the systemic risks posed by insecure DER fleets, and the project's findings offer a tangible pathway for addressing these challenges through embedded, sovereign trust mechanisms.

We also explore the commercial potential of the TSM technology and the co-simulation platform with the CSIRO and ECU.

4. Progress against the Roadmap

This project directly advances the objectives set out in CSIRO's *Australia's Research Roadmap for Power System Transformation* [7], particularly its recognition that high-penetration DER environments require new forms of device-level observability, controllability, and assured behaviour to maintain system stability. Earlier Roadmap stages, including the Topic 9 research on DER disturbance response, demonstrated that uncontrolled, non-compliant, or synchronised DER actions can create system-wide security events that exceed traditional contingency planning. However, these studies assumed benign malfunction rather than malicious manipulation, and identified significant gaps in the ability of system operators to verify, trust, or enforce DER behaviour in real time. The TSM project responds directly to these limitations by developing a sovereign, embedded mechanism that provides verifiable firmware integrity, continuous behavioural oversight, and non-bypassable enforcement of grid-safety envelopes. In doing so, it provides the device-level foundation that the Roadmap identifies as essential for stable operation under deep DER penetration.

The architectural and co-simulation outcomes of the project also extend the Roadmap by equipping Australia with a concrete means of assessing and governing DER behaviour under adversarial conditions, a dimension not addressed in earlier stages. By demonstrating how compromised or manipulated DER fleets could destabilise the system, and by developing a prototype mechanism capable of constraining such behaviour, the TSM work broadens the Roadmap's stability framework into the cyber-physical domain. This enables future market design, standards reform, and operational practices to be grounded in a realistic understanding of DER security risks and the technical measures required to mitigate them. The project therefore not only builds directly on the Roadmap's findings but substantively advances it by integrating cybersecurity, sovereignty, and device assurance into the core toolkit for achieving a resilient, DER-rich power system.

5. Research relevance to Australia

Australia's energy transition depends on the rapid and sustained growth of distributed energy resources, including electric vehicles, rooftop solar, home batteries, and flexible loads. However, this transition introduces technical limits that, if unaddressed, will constrain the pace and scale of renewable integration. High-wattage DER fleets such as EV chargers can create unpredictable or synchronised load behaviours that destabilise distribution networks, undermine frequency control, and exceed the system's capacity to manage disturbances. These risks impose implicit ceilings on how quickly EV adoption can grow and how aggressively electrification policies can proceed, because system operators must assume a worst-case scenario in which DER behaviour is neither visible nor controllable. Without demonstrably trustworthy behaviour at the device level, large penetrations of DER require costly network reinforcements, conservative operating margins, and increased procurement of stabilising services simply to maintain system security.

The research undertaken in this project provides a pathway to relieve these limits by developing an embedded, sovereign mechanism that ensures DER devices behave predictably, safely, and in compliance with system-security requirements, even under cyber compromise. The Trusted Sovereign Monitor (TSM) establishes verifiable firmware integrity, non-bypassable enforcement of grid-safety envelopes, and continuous visibility into device health and behaviour. When deployed at scale, these capabilities would allow Australia to integrate significantly larger DER fleets without incurring the operational and capital costs currently required to compensate for uncertainty and risk. They also position Australia as a global leader in securing the cyber-physical foundations of renewable energy systems, addressing challenges that all advanced economies will face as electrification accelerates.

6. Recommended research priorities

Future work should first focus on maturing the concrete project outputs developed in this program. A key priority is the progression of the Trusted Sovereign Monitor (TSM) prototype to higher technology readiness levels through iterative refinement, hardware integration, and field-facing evaluation. This includes direct engagement with EVSE OEMs, aggregators, operators, and government partners to conduct a pilot deployment that assesses real-world performance, operational constraints, and economic considerations associated with embedding sovereign trust anchors into DER fleets. Such a trial could be supported through ARP mechanisms or undertaken in partnership with ARENA, providing a rigorous evidence base for national adoption pathways. In parallel, the cyber-physical co-simulation platform developed in this project should be advanced into a full testing rig for DER security and safety validation. While initial efforts focus on EV chargers, the platform should be extended to incorporate batteries, smart inverters, and emerging flexible loads, creating a scalable environment for validating device behaviour under disturbance, compromise, and coordinated adversarial conditions. This work can be directly linked to national policy developments through collaboration with the Department of Home Affairs and IoT Alliance Australia, supporting the evolution of an Australian DER cybersecurity certification or labelling scheme grounded in realistic cyber-physical performance criteria.

Building on these project-specific activities, broader research under Topic 9 should address the systemic and operational challenges associated with managing very large fleets of heterogeneous DER devices under conditions of uncertainty, compromise, or attack. While the TSM provides a technical means of enforcing device-level trust and compliance, integrating such capabilities into grid operations, market structures, and critical-infrastructure governance frameworks requires sustained investigation. Priority areas include the development of standards and international best practice, beginning with the formation of a Standards Australia working group to lead the translation of TSM concepts into globally recognised device-security specifications, benefiting partners such as the US Department of Energy and European regulators. Topic 9 research should also explore how future national infrastructures, such as the emerging DER registry and national PKI ecosystem, can incorporate device-level attestation and trust signals to strengthen whole-of-system visibility. Finally, as Australia approaches very high levels of DER penetration, there is a need for research into incident management, coordinated response strategies, and graceful degradation of DER fleets during cyber-physical disruptions. Understanding how to contain compromised devices, operate securely in degraded states, and recover swiftly after coordinated disturbances will be essential to achieving the Roadmap's long-term vision of a stable, resilient, and secure high-renewables grid.

References

1. Kaur, A., Valizadeh, N., Nandan, D., Szydlo, T., R. K. Rajasekaran, J., Kumar, V., Barika, M., Liang, J., Ranjan, R., & Omer, R. (2025). Cybersecurity Challenges in the EV Charging Ecosystem. ACM Computing Surveys. https://doi.org/10.1145/3735662
2. Commonwealth Scientific and Industrial Research Organisation. (2024). Topic 9: DER and stability – Final report (GPST Roadmap Series). CSIRO. https://www.csiro.au/-/media/EF/Files/GPST-Roadmap/Topic-9-DER-and-Stability-Final-Report-with-alt-text-2.pdf
3. Commonwealth Scientific and Industrial Research Organisation. (2024). AR-PST guidance document for Stage 5 RFQ (AR-PST Program). CSIRO. https://www.csiro.au/-/media/Energy/AR-PST/AR-PST-Guidance-Document-for-Stage-5-RFQ-FINAL.pdf
4. Australian Energy Market Operator. (2023). EV technical standards for grid operation: Insights for the NEM. AEMO. https://www.aemo.com.au/-/media/files/initiatives/engineering-framework/2023/enx---ev-technical-standards-for-grid-operation---insights-for-the-nem.pdf
5. John Fletcher - Naomi Stringer - Georgios Konstantinou - Iain MacGill, CSIRO Australian Research for the GPST Task #9 – ENSURING SYSTEM SECURITY AND MODELLING FAST LOAD-DER RESPONSES WITH HIGH PENETRATIONS OF IBR – Report, 28/10/2021, https://www.csiro.au/-/media/EF/Files/GPST-Roadmap/Topic-9-DER-and-Stability-Final-Report-with-alt-text-2.pdf
6. Awais Ahmad, et.al, AUSTRALIAN RESEARCH FOR POWER SYSTEM TRANSITION Topic 9 – DER and Stability Stage 4 Final Report, 20/5/2025 https://www.csiro.au/-/media/EF/Files/GPST-Roadmap/Stage-4-Final/AR-PST-Stage-4-Topic-9-pdf.pdf
7. CSIRO, Australia's Research Roadmap for Power System Transformation **https://www.csiro.au/en/research/technology-space/energy/Electricity-transition/AR-PST/**, accessed 12/12/2025.