Australia's National
Science Agency

AR-PST Stage 5

Securing DER Stability via Trusted Sovereign Monitor (TSM)

EDITH COWAN UNIVERSITY

[Insert ISBN or ISSN and cataloguing-in-publication (CiP) information if required]

[Insert Research/Enterprise Unit specific information if required]

Citation

Smith BA, Jones KJ and White SM (2025) The CSIRO report template. CSIRO, Australia. [Insert correct details]

Copyright

Important disclaimer

Acknowledgement of Country

CSIRO acknowledges [the Traditional Owner/s name(s) as (delete if not required)] the Traditional Owners of the lands, seas and waters of the are that we live and work on across Australia and pays its respects to Elders past and present. CSIRO recognises that Aboriginal and Torres Strait Islander peoples have made, and will continue to make, extraordinary contributions to Australian life including in cultural, economic, and scientific domains.

Contents

Acknowledgments 10

Executive summary 11

1. Introduction 13

1.1 Significance of the Research 13

1.2 EV and EVSE infrastructure in Australia 14

1.3 DER Stability in Previous AR-PST Stages 14

1.4 EVSE as Critical Cyber-Physical Infrastructure 15

1.5 Gaps in Existing EVSE Trust Models 16

1.6 Research Problem 16

1.7 Stage 5 Focus Topic 9-2 17

1.8 Research Contribution and National Relevance 18

2 Methodology 20

2.1 Scientific Exploratory Methodology 21

2.2 Software and Platforms used 23

2.3 Reproducibility and Data Transparency 23

2.4 Project Structure 24

2.4.1 Phase 1- EVSE Threat Modelling 24

2.4.2 TSM Reference Architecture Design 29

2.4.3 Phase 2: Cyber–Physical Co-Simulation Platform Development 31

2.4.4 Phase 3: TSM Implementation and Experimentation 33

2.4.5 Phase 4. Policy Recommendations and Dissemination 40

2.5 Summary 40

3 Results 41

3.1 EVSE Vulnerabilities Analysis 41

3.1.1 Vulnerabilities Findings 41

3.1.2 Vulnerability Type Concentration (CWE Analysis) 42

3.2 EVSE Attack Surface Analysis 43

Firmware Governance and Trust Weaknesses: 45

3.3 Attack Graphs Analysis 45
Firmware Compromise Attack 45
3.4 Risk Analysis 47
3.4.1 EVSE Threat Distribution Across STRIDE Categories 47
3.4.2 Structural Dynamics of High-Risk Threats 48
3.5 TSM Reference Architecture 50
3.5.1 Architectural Design Realisation 50
3.5.2 TSM Integration with CO-Simulation Platform 51
3.5.3 Architectural Enforcement Properties 51
3.6 EVSE Co-simulation Baseline Model Results 52
3.6.1 Performance Evaluation 54
3.6.2 EV Charging Dynamics 55
3.6.3 Communication Interactions 56
3.6.4 EVSE Fleet with Grid Integration 57
3.6.5 Simulation Configuration 58
3.6.6 Grid Overload Analysis 59
3.6.7 Charging Station Concurrency 61
3.6.8 Battery Thermal Management 62
3.6.9 Communication Network Analysis 63
3.6.10 System Scalability Heatmap 65
3.6.11 Performance Metrics and Observations 66
3.6.12 Summary 66
3.7 TSM Implementation and Experimentation Results 66
3.7.1 Deployment Architecture 66
3.7.2 TSM Integration Within the Runtime 69
3.7.3 Protocol Layer Integration 71
3.7.4 Grid and Power System Model 72
3.7.5 Runtime Execution Flow 73
3.7.6 Scenario Manager and Threat Injector 74
3.7.7 End-to-End Demonstration Design 75
3.7.8 Evaluation and Results 78
3.8 TSM Validation Results 83
3.8.1 Fleet-level Impact and Risk Escalation 89

3.9 TSM Future Implementation 94
3.9.1 Practical Limitation and Challenges 95
3.9.2 TSM Supported Technologies 95
3.10 Summary 97

4 Insights 98

4.1 Security Threats to EVSE Infrastructure 98
Firmware Integrity as a Systemic Risk 98
Architectural Flatness 98
Backend Trust and Command Validation Weaknesses 99
Supply Chain Challenges in the EVSE ecosystem 99
4.2 Aggregation Effect: From Device Risk to Grid Risk 99
4.3 Sovereign Assurance Requirements 100

5 Future work 101

5.1 AR-PST Topic 9 (DER and Stability) 101
5.2 Future Research Work Opportunities 102

References 112

Table of Figures

Figure 1 : *EV Sales and Charging Infrastructure Growth Trends in Australia* 14

Figure 2 : *EVSE supply-chain trust concentration and absence of security architecture* 17

Figure 3 *: Scientific Exploratory Methodology.* 21

Figure 4*: **Threat Modelling Approach*** 24

Figure 5*: EVSE Eco-System Architectural view* 25

Figure 6: Interplay of threat, vulnerability, and consequence in defining security risk 26

Figure 7: Two-pronged EVSE vulnerability exploration: literature survey and NVD mining converge in a centralized repository for evidence-based threat modelling 28

Figure 8*: TSM with Dual Domain Architecture* 34

Figure 9*: TSM Abstract Operational States* 38

Figure 10*: Integration of the TSM within the Co-Simulation Platform employing supervisory mediation and trust boundary separation* 40

Figure 11*: Key Interfaces and Components that Contribute to the EVSE Attack Surface* 41

Figure 12*: Vulnerabilities distribution with cyber impact types for EVSEs* 44

Figure 13: *EVSE Vulnerabilities by Architecture Domain* 44

Figure 14*: Firmware Compromise Attack Graph with multiple attack paths* 46

Figure 15*: **EVSE attack-chain model demonstrating cross-domain propagation from backend compromise to fleet-wide control and grid-level disruption.*** 47

Figure 16: *EVSE-Threat Distribution with STRIDE Model* 48

Figure 17*: Risk Count by Severity: overall distribution of identified risks by severity level.* .. 48

Figure 18 *: Top 10 Threats* 49

Figure 19*: Comparison of Inherent vs Residual Risks* 49

Figure 20*: EVSE Risk Drivers* 50

Figure 21*: Grid integration architecture for single EVSE showing HELICS federation, OpenDSS power flow interface, and bidirectional communication pathways.* 53

Figure 22*: Top panel shows total system power demand over time. Bottom panel displays grid utilization factor (percentage of feeder capacity) demonstrating stable operation below 80% threshold, with shaded regions indicating charging phases and reserve margins.* 54

Figure 23*: The charging dynamics of two EVs and their control trajectories in a single EVSE scenario* 55

Figure 24*: The total energy consumption of the system and individual EVs in a single EVSE scenario.* 56

Figure 25*: The communication protocols, statistics, and message exchange in the single EVSE scenario.* 57

Figure 26*: EVSE fleet grid integration architecture showing distributed deployment across IEEE 13-bus system, HELICS federation coordination, and aggregate load management.* 59

Figure 27*: Estimating power grid capacity, grid utilization, and grid overload detection in the EVSE fleet scenario.* 60

Figure 28*: Charging station concurrency estimation for charging loads, station capacity, EV distribution in the charging stations, and active sessions of EVs in the EVSE fleet scenario.* 62

Figure 29*: Battery thermal management for estimating individual EV battery temperature, the frequency of temperature limit, peak temperature of EVs during charging, and temperature distribution in the span of EV charging in the EVSE fleet scenario.* 63

Figure 30*: Communication protocol analysis for estimating rate of communication messages, utilization of protocols, latency of communication messages, and frequency of popular control interactions in the EVSE fleet charging scenario.* 64

Figure 31*: System scalability heatmap for power and SoC of EV charging in the EVSE fleet charging scenario.* 65

Figure 32*: The formulation of sequential steps for the firmware update verification in the TSM-enabled pipeline* 70

Figure 33*: The scenario categorization and execution framework within the co-simulation platform.* 74

Figure 34*: The comparative analysis of scenario running without TSM and with TSM enforcement.* 76

Figure 35*:The sequence of six steps demonstration flow for running simulation scenarios.* 77

Figure 36*: The results of Layer 1: key performance metrics, decision latencies for each scenario, and firmware update verification scenarios.* 79

Figure 37*: TSM policies enforcement and trust chain for decision latencies, cascade failure analysis of TSM policy enforcement, and decision metrics analysis for different attack scenarios.* 80

Figure 38*: Layer 2 results: EV fleet charging profiles and statistics of communication protocols interactions* 81

Figure 39*: Real-time charging profile of EV fleet: the SoC charging profile over sixty minutes, total power delivery to EV fleets, and temperature distribution for individual EV across the EVSE fleet.* 82

Figure 40*: Layer 3 results: TSM enforced frequency and voltage stability of power grid.* 83

Figure 41*: TC1: Injection of invalid firmware image. The TSM enforcement uses a crypto engine to reject all firmware images with invalid keys using ECDSA signatures verification and validating the certificate chain in the trust chain.* 85

Figure 42*: TC2: Malicious but validly signed firmware. The TSM security pipeline is enforcing a runtime behavioural model for the EVSE charger behaviour within 50 ms, while the unsafe duration is 0.05 sec.* 86

Figure 43*: TC3: Firmware rollback attack. TSM-enabled enforcement triggered HRoT monotonic counter to block the older version and maintained full security features with RPR=100%.* 87

Figure 44*: TC4: Trust anchor compromise. The TSM-enabled enforcement provides remote attestation capabilities to detect HRoT manipulation using attestation cycle and detection latency to isolate the promised EVSE chargers from the fleets and restore EVSE fleet.* 89

Figure 45*: A fleet-level coordinated load attack occurs under TC2 when a malicious firmware update is initiated simultaneously on 20 EVSE chargers. This causes the total load to surge to 3.0 MW, exceeding the distribution feeder's rated capacity by 150%. With TSM* 90

Figure 46*: The risk escalation model follows a cascade from Devices → Sites → Fleets → Grids. In the absence of TSM, a single compromised EVSE can propagate the attack through all levels, reaching the grid within approximately 4 minutes. With TSM-enforcement.* 92

Figure 47*: The summarized TSM-enabled security metrics are: True Positive Rejection Rate (TPR) = 1.00, False Accept Rate (FAR) = 0.00, False Reject Rate (FRR) = 0.00, and Fail-Safe Reliability (FSR) = 1.00. All firmware update-related threat classes are mitigated.* 93

Figure 48*: The aggregate performance of the TSM firmware update security pipeline for the 60-minute simulation window. The mean latency is 7.6 ms indicate the operational feasibility and latency acceptance of TSM enforcement policies for the firmware update.* 94

Table of Tables

Table 1*: Software stack and platforms used* 23

Table 2*: EVSE Core Architectural Components and their Security Relevance* 25

Table 3*: EVSE-Attack Surface categories* 28

Table 4: Safety and Security parameters modelled in Co-simulation Platform 32

Table 5: TSM internal operational states 38

Table 6: Critical Vulnerabilities in the EV to EVSE Domain 43

Table 7: Critical Vulnerabilities in the EVSE Local Device Domain 43

Table 8*: Critical Vulnerabilities in the EVSE to Grid / DERMS Domain* 43

Table 9: Core Architectural Components and Functional Alignment 50

Table 10*: TSM Functional Requirements* 51

Table 11*: TSM integration with co-simulation platform* 51

Table 12*: TSM Architectural Enforcement Properties* 52

Table 13*: The group categorization and summarization of REST API endpoints.* 68

Table 14*: TSM PEE policies and classification of security levels.* 69

Table 15*: TSM interceptions and protocol inventories in the protocol layer.* 71

Table 16*: Grid Safety Envelope parameter bounds*. 73

Table 17*: Scenario categorization, sub scenarios, and types of sub scenarios* 75

Table 18*: The summarization of attack scenarios and their impact on TSM enforced trust chain* 80

Table 19: Challenges and Enabling Technologies for TSM Deployment..... 97

Acknowledgments

This project was funded by the Commonwealth Scientific and Industrial Research Organisation (CSIRO) under the Australian Research in Power Systems Transition (AR-PST), Topic 9-2 – Power System Cybersecurity program.

The authors gratefully acknowledge the collaboration and technical contributions of the research teams at Edith Cowan University (ECU) and CSIRO. The project benefited from cross-institutional expertise in power systems, cybersecurity, and cyber-physical modelling.

ECU Research Team

Name	Role
Prof. Helge Janicke	Principal Investigator (Cyber Expert) School of Science ECU
Dr. Ahmad Mohsin	Chief Investigator (Cyber and Systems) School of Science ECU
Dr. Asma Azhar	Chief Investigator (Power Systems) School of Engineering ECU
Dr. Iqbal Sarker	Chief Investigator (Cyber) School of Science ECU
Dr. Ahmed Ibrahim	Chief Investigator (Cyber) School of Science ECU
Muhammad Ikram	Research Associate (Power Systems) School of Engineering ECU
Dr. Ali Hur	Research Associate (Cyber) School of Science ECU

CSIRO Collaborators

Name	Role

Executive summary

This report presents the findings of the AR-PST Stage 5 project Securing DER Stability via Trusted Sovereign Monitor (TSM), funded by AEMO, CSIRO, and ECU. The project addresses the growing need to secure Australia's energy infrastructure as the power system becomes increasingly dependent on renewable and distributed energy resources (DER). Its central concern is the cybersecurity and sovereign control implications of this transition. The particular focus is on electric vehicle charging infrastructure (EVCI), as these are high-power assets with multiple digital connections and the potential to cause physical disruption and affect the stability of Australia's electricity grid.

A key issue examined in this work is Australia's reliance on third parties and foreign nations in the operation of its evolving power system. Most consumer-owned energy resources, including EV chargers, are not made in Australia. They are supplied, and in some cases partly operated or controlled, by original equipment manufacturers (OEMs) located overseas, predominantly in China and the EU. In a power grid projected to exceed 80 per cent DER penetration by 2030, this dependency has direct implications for national security, operational resilience, and Australia's ability to maintain effective control of critical infrastructure without the cooperation of other nation-states.

This work confirms that electric vehicle charging infrastructure presents a significant cyber risk to Australia's future energy system. The project identified and assessed a range of threats affecting EVCI in Australia and internationally. These threats were systematically analysed using established cybersecurity methods and publicly available material. The work shows that vulnerabilities in these devices and their associated digital ecosystems can be exploited in ways that may lead to disruption at both the device and grid level.

The project also established a capability to simulate the behaviour of compromised DER devices and assess the impact on the power grid. A co-simulation environment was designed and developed to study cyber-attacks against DER devices and observe their operational consequences. This provides a practical platform for testing attack scenarios, assessing mitigation approaches, and evaluating security interventions in a controlled environment.

A further key outcome is the design, development, and validation of a proof-of-concept Trusted Sovereign Monitor. The TSM was implemented and tested within the co-simulation environment and shown to detect and mitigate many of the threats identified in this work. The concept demonstrates a practical mechanism through which a sovereign entity could provide security assurance for consumer-owned energy resources (CER) without requiring the cooperation of OEMs.

Taken together, these findings show that the Trusted Sovereign Monitor provides a viable pathway to address a growing security and sovereignty gap in Australia's future electricity system. The work points to two practical next steps: the development of a standard that supports verifiable integration by OEMs, and the establishment of a national authority responsible for core security functions for DER devices with potential critical impact on grid stability.

In practical terms, this would provide assurance to customers, aggregators and system operators that consumer-owned energy resources continue to operate securely and within defined network parameters. More broadly, it provides a credible path toward sovereign assurance of DER in a highly distributed and increasingly internationally dependent energy system.

1. Introduction

1.1 Significance of the Research

Australia's power system is undergoing a structural transformation driven by the rapid penetration of Distributed Energy Resources (DERs), including rooftop photovoltaic systems, distributed battery storage, and electric vehicles (EVs). The Australian Energy Market Operator (AEMO) Integrated System Plan (ISP) outlines a long-term transition toward an increasingly decentralised and inverter-dominated electricity system [1]. Complementary technical assessments emphasise that EV charging demand will form a significant and controllable load component in future distribution networks [2], [3]. High DER penetration reduces synchronous inertia, alters system strength characteristics, and narrows voltage and frequency stability margins [1], [2]. Under these conditions, distribution feeders become increasingly sensitive to rapid load ramps and coordinated demand activation. EV charging infrastructure, therefore, represents not only a decarbonisation enabler but also a stability-relevant asset class.

The increasing connectivity of EV charging infrastructure renders it an attractive target for cyber adversaries. Modern EVSE systems are not isolated industrial devices; they are hyper-connected grid-edge platforms integrating mobile applications, cloud-based charging station management systems (CSMS), billing and payment infrastructures, remote firmware update mechanisms, and multiple grid interface protocols [4–8]. The adoption of EVs and the expansion of EV charging infrastructure within the Australian DER ecosystem are evident from recent data trends, as shown in Figure 1. This deep vertical integration significantly expands the attack surface. EVSE systems expose interfaces across local wireless connectivity (Wi-Fi, Bluetooth), cellular and Ethernet backhaul communications, cloud APIs, authentication systems, and backend orchestration platforms. Vulnerabilities may arise at multiple layers, from embedded firmware and real-time operating systems to cloud-side command injection and identity misuse [5], [6], [8], [10].

Research examining EV charging infrastructure security identifies systemic risks associated with firmware governance, backend compromise, and coordinated load manipulation [4–10]. Supply-chain threat assessments further recognise that firmware compromise in distributed infrastructure can propagate rapidly across device fleets [14].

Importantly, these risks are not theoretical. Demonstrated vulnerabilities in charger firmware and CSMS platforms confirm that unauthorised remote-control pathways exist. Although some publicised incidents have involved non-disruptive misuse (e.g., display message manipulation), such events serve as proof-of-concept validation. The same access vectors could enable coordinated fleet manipulation, including load ramp synchronisation, charging limit modification, or suppression of protection logic, with measurable consequences for feeder voltage stability and system security margins. Although standards such as ISO 15118 and OCPP provide interoperability and baseline communication security [11], [12], they do not intrinsically enforce sovereign firmware governance or stability-aware operational constraints. This structural gap motivates the research presented in this report.

1.2 EV and EVSE infrastructure in Australia

Australia's transport sector is a significant contributor to national greenhouse gas emissions, and its electrification is central to the Federal Government's National Electric Vehicle Strategy [31]. Recent policy measures targeting affordable EV uptake, charging infrastructure expansion, and market stimulation have accelerated adoption nationwide. EV sales have grown rapidly, with cumulative vehicles exceeding 180,000 by 2023 and projected to surpass 300,000 by 2025 [32]. By April 2024, EVs accounted for 9.4% of new vehicle sales, reflecting sustained exponential growth.

This expansion has been mirrored by charging infrastructure deployment, with more than 3,300 public charging sites and over 3,700 fast-charging bays operating across Australia by 2025 [33]. Government-backed initiatives, including the National Electric Vehicle Charging Network, aim to ensure reliable coverage along major transport corridors [31]. Figure 1 illustrates the correlated growth of EV sales and charging infrastructure between 2020 and 2025. The expanding Electric Vehicle Supply Equipment (EVSE) network represents a critical national infrastructure intersecting transport and energy systems [34], [35]. Modern EVSEs are cyber-physical systems integrated with communication protocols, backend platforms, and grid control mechanisms [36], [37]. As distributed energy resources (DERs), EV chargers increasingly influence grid stability and enable advanced services such as demand response and vehicle-to-grid (V2G) integration [38], [39]. However, their connectivity introduces cybersecurity risks, including privacy breaches, coordinated load manipulation, and potential grid disruption [40], [41]. Ensuring the security and resilience of this infrastructure is therefore essential to maintaining Australia's electric mobility investment as a stable and secure national asset.

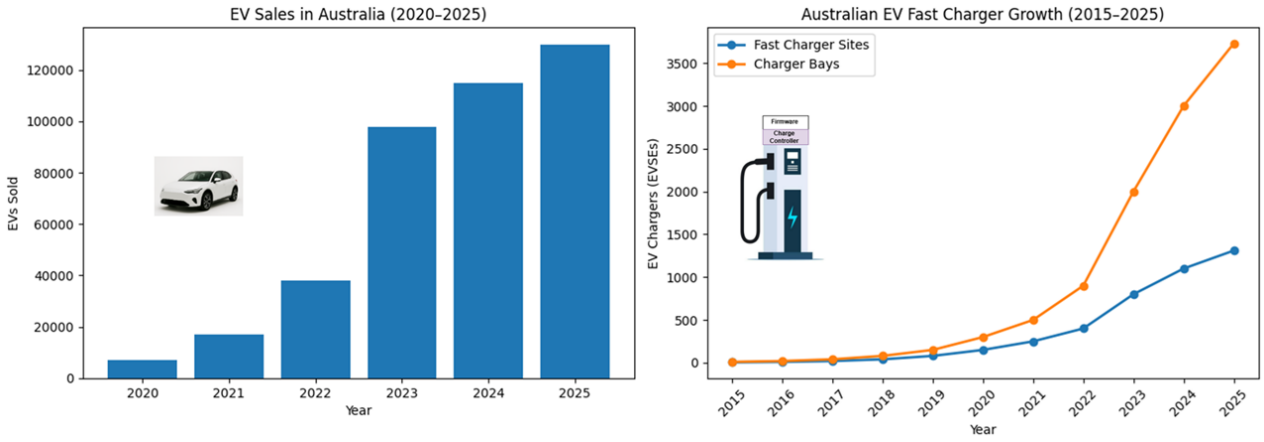


Figure 1 : ***EV Sales and Charging Infrastructure Growth Trends in Australia***

1.3 DER Stability in Previous AR-PST Stages

The Australian Research in Power Systems Transition (AR-PST) program provides a coordinated national research framework addressing Australia's electricity transition challenges [15]. Within this framework, Topic 9 – DER and Stability has delivered substantial advances in modelling inverter interactions, weak-grid behaviour, oscillatory modes, and system strength implications under high DER penetration [16], [17].

Stage-4 research established improved modelling fidelity for DER inverter dynamics and enhanced simulation frameworks for stability envelope assessment. These outputs significantly strengthen the physical evidence base for grid planning and operational analysis. However, three structural gaps remain with respect to cybersecurity integration.

- First, Topic 9 modelling is not explicitly structured around adversarial threat models aimed for cyber-to-physical causality mapping [16], [17]. While inverter behaviour under engineering disturbances is well characterised, deliberate firmware manipulation and coordinated cyber compromise scenarios are not formally integrated into stability simulations.
- Second, governance and operational recovery frameworks for DER ecosystems during cyber-induced stability events remain underdeveloped. Although national cybersecurity governance structures such as the Australian Energy Sector Cyber Security Framework (AESCSF) provide sector-level guidance [18], DER-specific cyber-physical recovery pathways are not yet embedded within stability research outputs.
- Third, standards and assurance mechanisms at the DER edge remain primarily interoperability focused. The Grid Cyber Security Roadmap highlights the need for coordinated uplift and security by design approaches [19], yet stability-aware firmware assurance and sovereign trust enforcement mechanisms are not systematically integrated into DER modelling frameworks.

These gaps establish the need for Stage-5 integration of cybersecurity assurance with DER stability research.

1.4 EVSE as Critical Cyber-Physical Infrastructure

EVSE systems operate at the intersection of cyber and physical domains. Architecturally, they combine characteristics of Cyber-Physical Systems (CPS), IoT deployments, and enterprise IT infrastructures [4–7], [9]. At the hardware layer, charging units incorporate real-time control processors, application processors, human-machine interfaces, cryptographic modules, and optionally secure elements or Trusted Platform Modules (TPMs). These components manage power electronics control alongside application-layer services and remote communication.

Connectivity is multi-layered and protocol diverse. Vehicle-to-charger communication is implemented via ISO 15118 overpower Line Communication (PLC) [12], while backend connectivity relies on OCPP over TCP/IP networks [11]. Data aggregation occurs within CSMS platforms, integrating REST APIs, OAuth2-based authentication, billing systems, and cloud analytics environments. EVSE systems may also interface with utility platforms via industrial protocols such as Modbus/TCP, IEC 61850, or DER coordination standards [13].

This hybrid IT–Operational Technology (OT) grid interoperability creates a deeply interconnected attack surface. A compromise originating in enterprise IT, such as credential phishing targeting a Charge Point Operator administrator, may propagate to the CSMS and subsequently to distributed charging assets. At fleet scale, malicious command injection could induce coordinated load activation, impact feeder voltage regulation, and increasing rate-of-change-of-frequency (RoCoF).

Firmware integrity is particularly critical. Firmware governs charging power limits, safety thresholds, communication handling, and protection logic. If compromised, firmware can override configured

constraints while appearing cryptographically valid. At high DER penetration, synchronised firmware manipulation could produce aggregate load ramps of multi-megawatt magnitude on distribution feeders.

1.5 Gaps in Existing EVSE Trust Models

Current EVSE security architectures rely primarily on OEM-issued digital signatures, TLS-protected communication channels, and certificate-based identity validation. While these mechanisms provide baseline communication integrity, they introduce concentration risk: compromise of a signing authority may propagate malicious firmware across geographically distributed device fleets.

Existing models lack:

- Independent sovereign hardware root-of-trust
- Deterministic anti-rollback enforcement
- Runtime mediation between firmware validation and physical actuation
- Grid-aware safety constraint enforcement
- Independent revocation governance

Supply-chain threat analyses emphasise increasing systemic risk associated with firmware compromise in distributed infrastructure [14]. However, no existing framework explicitly links firmware governance mechanisms to quantitative grid stability metrics such as voltage deviation (ΔV) or RoCoF.

1.6 Research Problem

Electric Vehicle Supply Equipment (EVSE) systems are increasingly embedded within Australia's critical energy infrastructure and operate at the convergence of cyber, supply-chain, and grid domains. They interface directly with distribution feeders while relying on cloud-based backend systems and firmware update mechanisms governed by Original Equipment Manufacturers (OEMs) via ISO 15118 and OCPP protocols [11], [12].

Figure 2 illustrates the structural trust concentration inherent in contemporary EVSE deployments. Firmware and charge controller logic remain under OEM control, while grid operators and distribution stakeholders lack independent mechanisms to verify, mediate, or constrain firmware behaviour before physical actuation. This creates a single-point trust dependency within a distributed DER ecosystem. EVSE systems are exposed to multiple cyber threat vectors, including backend compromise, protocol manipulation, authentication bypass, certificate misuse, firmware tampering, and supply-chain compromise [4–10], [14]. Among these, firmware integrity represents a uniquely systemic risk vector. Firmware governs charging limits, protection thresholds, communication handling, and actuation logic. If compromised, malicious firmware may remain cryptographically valid while altering physical load behaviour. At fleet scale, coordinated firmware manipulation could induce synchronised load ramps and feeder disturbances. For example, a feeder hosting 500 chargers operating at 11 kW could experience an instantaneous 5.5 MW load increase under coordinated activation. In high-DER, low-inertia environments [1], [2], such ramp events may degrade voltage stability, elevate RoCoF, and erode system security margins.

Existing OEM-centric trust models rely primarily on signature validation and transport-layer security. They do not provide independent hardware-rooted trust anchoring, deterministic anti-rollback enforcement, runtime mediation between firmware validation and actuation, or stability-aware constraint enforcement. The core research problem is therefore:

How can firmware governance at the DER edge be architected such that cyber compromise within the EVSE supply chain cannot propagate into measurable grid stability degradation?

This problem reframes EVSE cybersecurity as a DER stability assurance challenge, requiring architectural mechanisms that constrain the physical consequences of compromise within bounded and stability-safe envelopes.

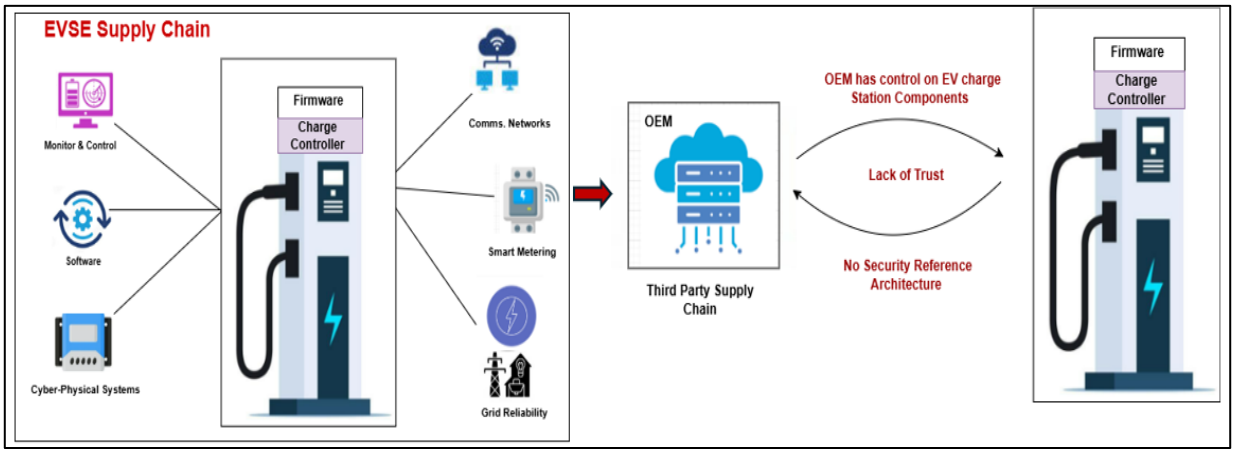


Figure 2 : ***EVSE supply-chain trust concentration and absence of security architecture***

1.7 Stage 5 Focus Topic 9-2

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 [31]. 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 [32]. Ensuring system security under such conditions requires not only improved models but also new architectural safeguards embedded directly within DER devices.

Our research addresses this need by analysing threats to EV charging infrastructure and developing a Trusted Sovereign Monitor (TSM). 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 AR-PST vision of maintaining system operability and resilience in the context of state-level cyber-attacks.

1.8 Research Contribution and National Relevance

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 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.

This Stage-5 AR-PST project introduces TSM, a device-level trust enforcement architecture designed to integrate sovereign firmware governance with stability-aware operational control. The TSM implements a dual-domain architecture separating Low Integrity Domain (LID) and High Integrity Domain (HID), enabling independent mediation of firmware admission and runtime actuation. Hardware-rooted trust anchoring, anti-rollback enforcement, certificate revocation validation, and deterministic write-enable gating are combined with grid-aware safety constraints.

Validation is performed within a HELICS-based cyber-physical co-simulation environment integrating EVSE fleet models with OpenDSS [42] distribution network simulation and threat injection scenarios. Experimental evaluation demonstrates that, under OEM-only firmware validation, malicious updates induce measurable load ramp amplification and voltage excursions. Under TSM enforcement:

- Voltage deviation remains within operational limits.
- Aggregate ramp magnitude is reduced.

- Frequency deviation and RoCoF are moderated.
- Unsafe firmware installation is deterministically blocked.

These findings directly link cybersecurity assurance to DER stability outcomes. Given Australia's projected EV adoption trajectory [1–3], proactive sovereign firmware governance reduces systemic fleet-level risk, mitigates infrastructure augmentation pressures, and strengthens resilience within the transitioning electricity system.

2 Methodology

DER Stability Topic 9-2 presents a uniquely challenging research domain. Unlike conventional stability studies focused solely on inverter dynamics or power system modelling [16], [17], this project addresses the stability implications of cyber-enabled DERs. Specifically, it investigates how Electric Vehicle Supply Equipment (EVSE), as grid-edge cyber-physical assets, may influence DER and grid stability under both normal and adversarial conditions. EVSE systems operate within a heterogeneous and deeply interconnected ecosystem comprising diverse stakeholders, including Original Equipment Manufacturers (OEMs), Charge Point Operators (CPOs), Distribution Network Service Providers (DNSPs), aggregators, DERMS platforms, cloud service providers, and end users. Each stakeholder introduces distinct trust boundaries, operational responsibilities, and technical dependencies. From a systems perspective, EVSE infrastructure integrates multiple technological domains:

- Cyber-Physical Systems (CPS) controlling real-time power electronics
- IoT-enabled connectivity and remote management platforms
- Enterprise IT systems governing billing, authentication, and orchestration
- Grid-interfacing operational technology (OT) components

This convergence creates a layered IT–OT–grid architecture with complex interdependencies. At the device level, EVSE units are embedded systems typically incorporating System-on-Chip (SoC) controllers (e.g., real-time control cores and application processors), Human-Machine Interfaces (HMIs), cryptographic modules, and in some cases, secure elements or Trusted Platform Modules (TPMs). These components manage power conversion, charging control, and communication functions simultaneously.

Connectivity is multi-layered and multi-protocol:

- Vehicle-to-charger interaction via ISO 15118 overpower Line Communication (PLC)
- Backend orchestration through the Open Charge Point Protocol (OCPP) over TCP/IP networks
- CSMS integration via REST APIs and OAuth2-based authentication
- Grid-facing integration through Modbus/TCP, IEC 61850, or IEEE 2030.5 for DER coordination

Each of these communication pathways carries distinct parameter sets, configuration variables, authentication models, and vulnerability profiles [5], [6], [10]. While individual protocol security properties have been studied in isolation [4–8], limited research has systematically explored how these components interact across cyber and power domains, particularly under coordinated or adversarial manipulation.

Critically, firmware forms the operational core of EVSE systems. Firmware governs charging limits, safety interlocks, communication handling routines, and power regulation logic. Its integrity and sovereignty are therefore central to device behaviour. However, firmware supply chains involve third-party software dependencies, signing authorities, and distributed update mechanisms, introducing systemic attack vectors [14]. In high-DER environments characterised by reduced inertia and tighter voltage margins [1], [2], coordinated firmware manipulation could induce synchronised load ramps, alter charging frequency behaviour, or suppress protection logic — thereby influencing feeder stability. The interaction between cyber compromise and power flow dynamics remains

insufficiently characterised in current literature. The central methodological challenge is therefore twofold:

1. To systematically model and quantify the cyber-physical risk pathways within the EVSE ecosystem.
2. To design and validate an embedded architectural mechanism capable of enforcing grid-safe operational constraints independent of primary firmware behaviour.

2.1 Scientific Exploratory Methodology

To address the DER cybersecurity and stability challenges, this project adopted a structured, evidence-based, and exploratory methodology grounded in systems security engineering and risk-informed design principles. Consistent with multidisciplinary security engineering guidance [26], the approach integrates architectural analysis, threat modelling, and validation within a unified engineering workflow rather than treating cybersecurity as a compliance overlay. Please refer to Figure 3 for the overall structure of the methodology. The methodology progresses systematically from ecosystem characterisation to empirical cyber–physical validation. Guided by structured risk assessment frameworks [27], the study began with formal modelling of EVSE architectural dependencies and trust boundaries, followed by adversarial threat mapping and stability-oriented impact assessment. Recognising that DER-edge infrastructure operates as an integrated cyber–physical system, digital compromise pathways were analysed in terms of measurable physical consequences, consistent with established smart grid CPS security research [28].

To ensure empirical grounding, the framework incorporated co-simulation as a validation mechanism. Co-simulation methodologies are widely recognised for analysing coupled electrical and communication dynamics in intelligent power systems [29], and federated modelling environments such as HELICS provide validated infrastructure for cross-domain synchronisation [30], enabling firmware governance and backend control logic to be evaluated against measurable stability metrics rather than theoretical assumptions.

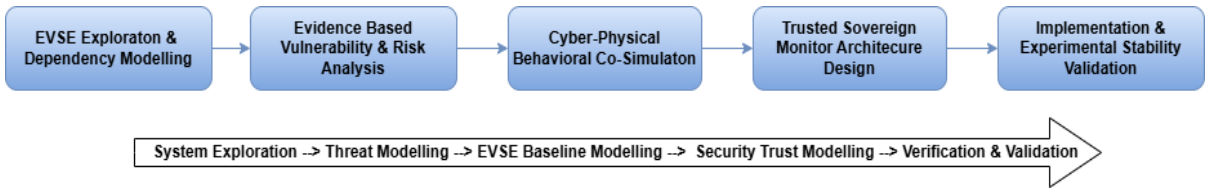


Figure 3 ***: Scientific Exploratory Methodology.***

Stage 1: EVSE Ecosystem Exploration and Dependency Modelling

The study began with a systematic exploration of the EVSE ecosystem as a cyber-physical DER asset class. This involved identification and decomposition of core architectural components, including firmware, charge controllers, embedded operating environments, communication stacks, backend orchestration systems, and grid interfaces. Stakeholder trust boundaries were mapped across OEMs, Charge Point Operators (CPOs), Charging Station Management Systems (CSMS), utilities, DERMS platforms, and end users. Information flows (e.g., firmware updates, charging session commands, authentication exchanges) and power flows (active and reactive load injection into feeders) were analysed concurrently to establish cross-domain dependencies.

This step developed a formal dependency model that captures interactions among firmware logic, communication protocols (e.g., ISO 15118, OCPP), backend control pathways, and distribution network behaviour. The model provides a structured view of how cyber-control decisions can influence the electrical system's state.

Stage 2: Evidence-Based Vulnerability and Risk Analysis

Building on the ecosystem model, a comprehensive vulnerability and risk assessment was conducted using empirical and documented threat intelligence sources. These included the CVE/NVD databases, MITRE ATT&CK (with ICS mappings), ENISA supply-chain threat analyses [14], and peer-reviewed research on EV and smart grid cybersecurity [4–10].

Attack vectors were systematically classified across:

- Firmware and boot integrity layers
- Communication protocols and session management
- Backend orchestration and CSMS control pathways
- Supply-chain and certificate governance mechanisms

Rather than treating vulnerabilities in isolation, this step focused on identifying causal pathways by which compromise at one layer could propagate to affect device behaviour and, at fleet scale, aggregate load dynamics. This analysis revealed concentration risks associated with OEM-centric firmware trust models and limited independent enforcement at the DER edge.

Stage 3: Cyber–Physical Behavioural Analysis via Co-Simulation

Recognising that cybersecurity risks must ultimately be evaluated in terms of physical system consequences, the methodology incorporated a cyber–physical co-simulation framework. A HELICS-based federated environment [30] was developed to synchronise EVSE behavioural models with OpenDSS distribution network simulation. The platform modelled internal charging logic, EV session dynamics, time-varying power consumption profiles, and feeder-level electrical responses. Stability-relevant parameters included active and reactive power (***P, Q***), aggregate fleet load (***ΣP***), voltage magnitude and deviation (|***V|, ΔV***), load ramp rate (***dP/dt***), frequency deviation (***Δf***), and transformer loading.

Controlled scenarios were executed to evaluate how manipulated firmware logic, such as the removal of ramp limits or altered power caps, affected feeder voltage regulation and dynamic stability. Examples included synchronised activation of large EVSE fleets and modified charging setpoints producing rapid aggregate load ramps.

Stage 4: Trusted Sovereign Monitor (TSM) Architecture Design

Based on systemic risks identified in earlier steps, a TSM reference architecture was developed to introduce non-bypassable governance at the DER edge. The architecture incorporated dual-domain separation (Low Integrity and High Integrity domains), hardware-rooted trust anchoring, deterministic firmware admission control, certificate revocation enforcement, and monotonic anti-rollback mechanisms. Importantly, the architecture was designed not merely for cryptographic correctness but for stability-aware operation. Firmware governance decisions were framed as control points to prevent unsafe behavioural modifications that could influence aggregate DER load.

Stage 5: Implementation and Experimental Validation

The TSM core logic was implemented and integrated into the co-simulation platform to enable experimental comparison between baseline OEM-only firmware validation and TSM-mediated enforcement. Under simulated threat conditions, measurable outputs included voltage deviation (ΔV), aggregate load ramp magnitude (dP/dt), frequency deviation and RoCoF, transformer loading variation, and firmware admission behaviour. Experimental results demonstrated that compromised firmware could materially influence aggregate load dynamics, whereas TSM enforcement deterministically blocked unsafe firmware admission and moderated stability-relevant perturbations.

2.2 Software and Platforms used

All methodological stages were implemented using open-source and publicly accessible platforms to ensure transparency, reproducibility, and scientific adequacy. Please refer to table below. No commercial or proprietary software tools were used. Vulnerability intelligence was derived from publicly available cybersecurity databases, and all cyber–physical simulations were conducted using open research-grade modelling environments.

Table 1*: Software stack and platforms used*

Software / Platform	Classification	Role in Research	Application
Microsoft Threat Modelling Tool	Public (free)	STRIDE-based structural threat modelling	DFDs, trust boundaries, threat enumeration
National Vulnerability Database (NVD)	Public (NIST)	Empirical vulnerability analysis	CVE identification and CVSS scoring
MITRE ATT&CK for ICS	Public framework	Adversarial technique mapping	Behavioural threat alignment
HELICS	Open-source	Cyber–physical federation	EVSE–grid co-simulation orchestration
OpenDSS	Open-source	Distribution network modelling	Voltage, load, and stability simulation
GridLAB-D	Open-source	EV charge scheduling	EV load profiling, session management
Python (NumPy, Pandas, Matplotlib)	Open-source	Data analysis and visualisation	Stability metric computation
Python Cryptographic Libraries	Open-source	Firmware validation modelling	Signature and admission checks
PyPSA (Python for Power System Analysis)	Open-source	Control layer between physical and communication layers	PyPSA (Python for Power System Analysis)

2.3 Reproducibility and Data Transparency

All cyber–physical modelling components were implemented using open-source simulation frameworks and standard scientific computing libraries. Vulnerability data were sourced from publicly accessible repositories (e.g., NVD, MITRE ATT&CK,). No confidential OEM firmware or proprietary datasets were incorporated. The modelling parameters, simulation configurations, and experimental procedures are documented in the associated technical reports and appendices, enabling independent replication by researchers with access to the listed platform

2.4 Project Structure

Guided by the overarching scientific exploratory methodology described in Section 2.1, the project is structured into four interrelated phases. Each phase is not an isolated activity, but a progressively deepening layer of analysis and validation governed by the same evidence-based, cyber–physical, and stability-aware methodological framework. The four phases are designed to move from analytical modelling to empirical validation, ensuring that architectural design decisions are grounded in measurable grid stability behaviour rather than theoretical cybersecurity assumptions.

2.4.1 Phase 1- EVSE Threat Modelling

This phase established the analytical foundation of the overall methodology by conducting a structured, domain-driven threat modelling and risk assessment of Electric Vehicle Supply Equipment (EVSE) as a cyber–physical DER. The approach was not limited to conventional IT-centric vulnerability scanning; instead, it systematically decomposed EVSE architecture, modelled adversarial behaviour, and analysed cross-domain propagation pathways from cyber compromise to physical grid impact. It involves systematic decomposition of EVSE components, hybrid threat modelling techniques mainly STRIDE and MITRE ATT&CK, attack graph construction, scenario development, and risk assessment. detailed threat modelling report is available in Appendix A. Overall, the Threat Modelling approach is depicted in the diagram below in Figure 4.

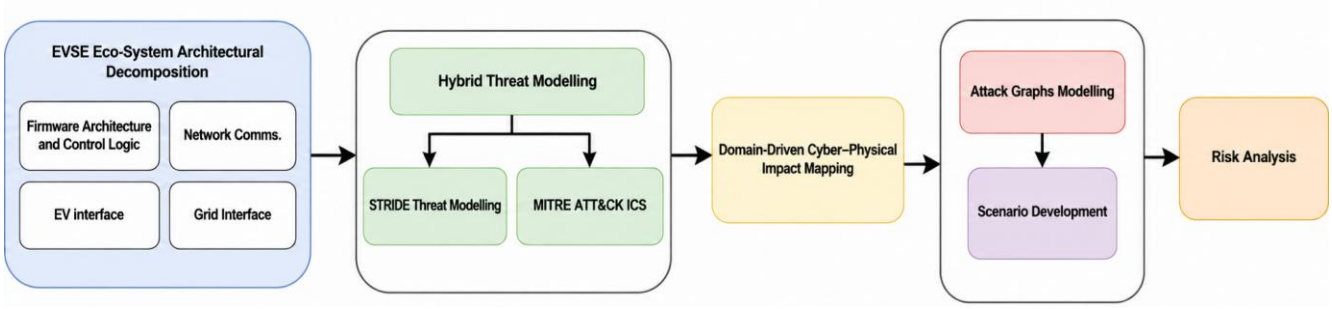


Figure 4: ***Threat Modelling Approach***

EVSE Architecture Decomposition

For structured threat modelling, the EV charging ecosystem was systematically organised and decomposed into functional domains, control pathways, and trust boundaries. The Electric Vehicle Supply Equipment (EVSE) operates as a cyber–physical system divided into two primary paths: the Power Path (high-voltage energy transfer) and the Control/Data Path (safety, communication, and session governance). Four interacting domains were identified: the EV User Domain (vehicle systems and driver applications), the CPO Domain (EVSE hardware and CSMS operations), the eMSP Domain (customer and billing services), and the DSO Domain (grid monitoring and control). For detailed architectural view please refer to figure 5.

The Power Path conducts three-phase AC from the grid through power electronics to the vehicle's charge port, where onboard charging systems regulate battery intake. In parallel, the Control/Data Path, anchored by the Main Control Board and Communication Module, manages authentication, interlocks, charge-rate algorithms, metering, and transaction processing. Standardised interfaces

define cross-domain interactions, including IEC 61851/J1772 (control pilot), ISO 15118 (PLC), Modbus/SunSpec (local energy coordination), OCPP (EVSE–CSMS), and REST APIs (external services).

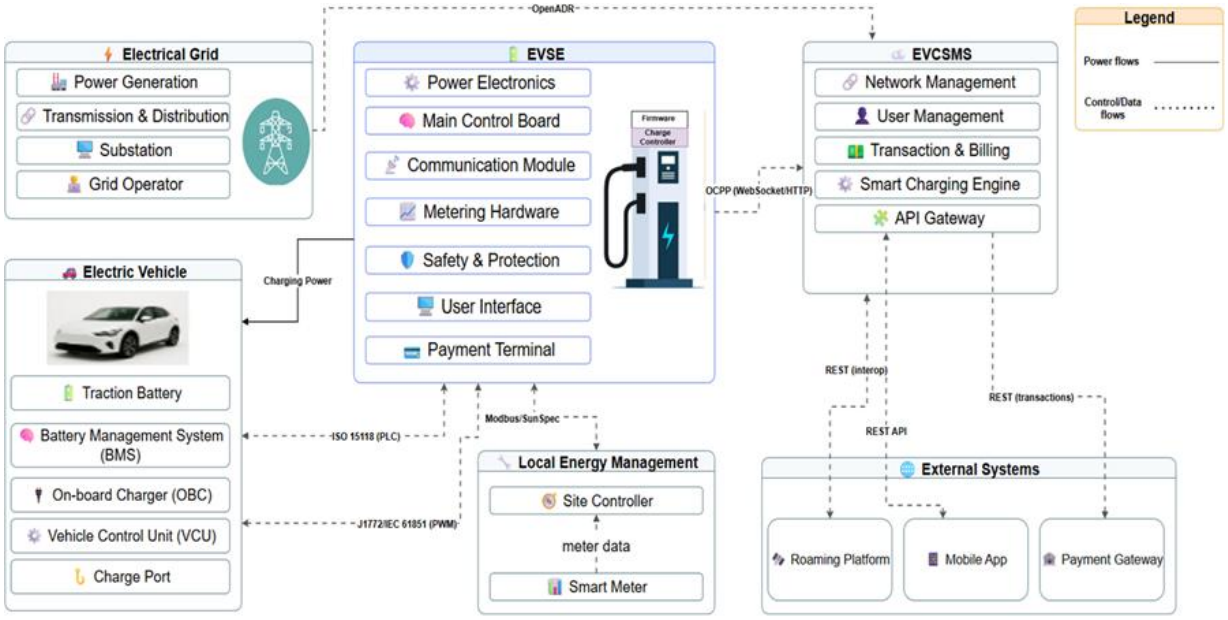


Figure 5*: EVSE Eco-System Architectural view*

The Table 2 summarises the core EVSE components identified during the architectural decomposition phase of threat modelling. It consolidates hardware, firmware/software, and external interface elements, highlighting their primary operational roles and associated security relevance. This structured view enables clear identification of critical EVSE assets and trust boundaries.

Table 2*: EVSE Core Architectural Components and their Security Relevance*

Category	Component	Primary Function	Security Relevance
Hardware	Power Electronics Module	AC/DC conversion, DC/DC regulation, high-voltage switching, thermal control	High-impact safety asset; potential manipulation affects grid and battery integrity
Hardware	Control & Logic Unit (SoC/MCU)	Executes firmware, charging logic, safety checks	Root of trust; firmware integrity and secure boot critical
Hardware	HMI (Display/Indicators)	User interaction, session monitoring	Potential physical access attack vector
Hardware	Authentication & Payment Module	RFID/NFC processing, EMV transactions	Sensitive financial data; PCI-DSS compliance required
Hardware	Connectivity Module (4G/5G, Wi-Fi, Ethernet)	WAN/backend communication	Primary remote attack surface
Hardware	Metering & Safety Systems	Energy measurement, RCD, breakers, and insulation monitoring	Billing integrity; electrical fault protection
Firmware/Software	Embedded OS (Linux/RTOS)	Resource management, process isolation	Vulnerability exposure via unpatched OS

Firmware/Software	Device Management Logic	Charging state machine, diagnostics, logging	Controls session lifecycle and safety interlocks
Firmware/Software	Communication Stacks (ISO 15118, OCPP, Modbus)	Protocol handling and interoperability	Protocol exploitation risk (MitM, spoofing)
Firmware/Software	Business Logic Layer	Tariff control, load balancing, and reservations	Policy manipulation risk; grid coordination impact
Interface	Vehicle Interface (IEC 61851, ISO 15118)	EV–EVSE negotiation and authentication	Certificate validation, TLS enforcement critical
Interface	Backend Interface (OCPP)	EVSE–CSMS communication	Firmware update channel; command injection risk
Interface	Roaming Interface (OCPI)	CPO–eMSP session & billing exchange	Data integrity and settlement risk
Interface	Grid/DSO Interface (OpenADR, IEEE 2030.5)	Demand response, DER coordination	Fleet-level control risk; grid stability impact

EVSE Vulnerability Modelling

Following the detailed architectural analysis, we develop a formal analysis of the inherent weaknesses within the EVSE ecosystem. The previous step established the EVSE as a critical cyber-physical system operating at the convergence of Information and Operational Technology (IT/OT). This unique position means that its vulnerabilities can have cascading consequences, extending beyond data breaches to threaten the stability of the power grid and the safety of end-users. Therefore, a systematic and evidence-based vulnerability analysis is the essential first step toward developing a resilient security posture.

Establishing the Threat–Vulnerability–Risk Relationship

A conceptual framework is established by defining threats, weaknesses, and potential harm, illustrating their interplay. This framework is crucial for analysing EVSE vulnerabilities, assessing security, and developing mitigation strategies.

Figure 6: Interplay of threat, vulnerability, and consequence in defining security risk

Definitions and Rationale

As depicted in Figure 6, risk only materializes where a credible threat overlaps with an exploitable vulnerability and produces a consequence. Understanding this triad lets us dissect complex security challenges into discrete, actionable elements.

Threat (T)

A potential cause of an undesirable incident that can harm a system or organization. In EVSE, this spans from opportunistic script-kiddies and financially motivated cybercriminals to sophisticated, state-sponsored APT groups targeting critical infrastructure.

Vulnerability (V)

A weakness in an asset or control, whether in design, implementation, or configuration, that a threat can exploit. An unencrypted communication channel between the charging station and central management is a classic example.

Impact (I)

The adverse impact or harm resulting from a successful exploitation, such as service disruption, financial loss, or safety hazards.

Risk (R)

The potential for loss or damage when a specific threat leverages a particular vulnerability to cause a consequence. As shown in figure 6, risk resides only in the intersection of all three circles. To quantify how these elements combine into overall risk, we adopt the classic multiplicative model:

$$\boldsymbol{R} = \boldsymbol{T} \times \boldsymbol{V} \times \boldsymbol{I} \qquad (1)$$

Where:

T is the likelihood of a threat occurring

V is the level of vulnerability exposure

I is the potential impact of a successful attack

Because the model multiplies all three factors, even a highly capable threat (high ***T***) yields little risk if the vulnerability exposure ***(V***) is near zero, or a severe vulnerability (high ***V***) poses no risk without a credible threat (***T*** = 0). This mirrors figure 6 with Venn diagram: risk only materializes where threat, vulnerability, and consequence overlap.

Methodology and Two-Pronged Strategy

To ensure the vulnerability assessment was both comprehensive and credible, a "two-pronged strategy" was employed. This methodology is designed to synthesize high-level, theoretical knowledge with low-level, empirical evidence from real-world systems. As illustrated in the figure 7 below, our approach combines two complementary streams, high-level theoretical insight and low-level empirical data to build a robust vulnerability assessment for EVSE systems.

Literature-Driven Exploration: This "top-down" or qualitative part of the research involved an extensive review of academic papers, cybersecurity vendor reports, and industry white papers. This prong answers the strategic question: "What are the known, theoretical, and architectural weaknesses we should be looking for?" It provides a high-level understanding of the problem space, identifying common flaw patterns and areas of concern highlighted by industry experts.

Empirical Data Mining: This "bottom-up" or quantitative, evidence-based part of the research involved systematically going through public databases, primarily the National Vulnerability Database (NVD), for CVEs related to EVSE products. This prong answers the tactical question: "What specific, verifiable security holes have actually been discovered in real products?" This data was consolidated into a master register to ensure the analysis is grounded in documented, verifiable security flaws.

Centralized Vulnerability Repository: Both the theoretical findings and NVD extractions converge in a unified "Vulnerabilities" database. Each entry is normalized with metadata fields for source, CVE ID (where applicable), affected component, and severity rating, to enable consistent analysis.

Evidence-Based Threat Modelling: Finally, the curated repository feeds into our threat-modelling engine (bottom of the figure below). By anchoring attack scenarios in both conceptual knowledge and real-world incidents, we ensure that downstream risk assessments and mitigation strategies are both comprehensive (covering novel threats) and credible (grounded in empirical evidence

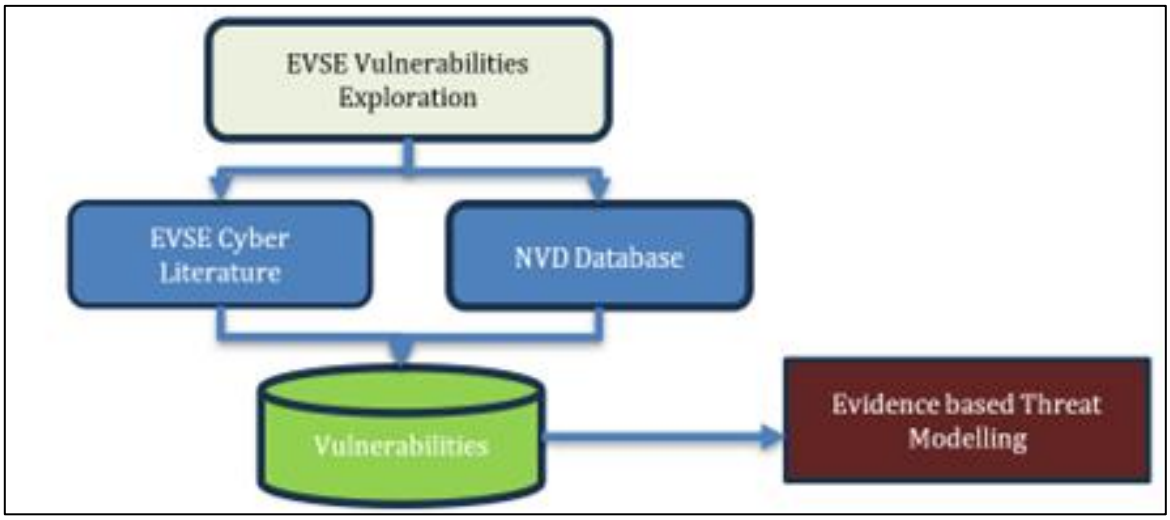


Figure 7: Two-pronged EVSE vulnerability exploration: literature survey and NVD mining converge in a centralized repository for evidence-based threat modelling

Attack Surface Categorisation

With vulnerability exploration from existing literature and various databases, followed by the EVSE Attack Surface Analysis. The attack surface was categorised into the following four categories in the Table 3.

Table 3*: EVSE-Attack Surface categories*

Physical	USB ports, UART/JTAG, weak enclosure locks, payment terminals	Direct firmware tampering, hardware compromise, persistent backdoor
Network – Vehicle	ISO 15118 PLC interface	Malformed packets, cert abuse, edge compromise
Network – LAN	Wi-Fi, Ethernet, admin portals	Weak credentials, lateral movement across chargers
Network – WAN	OCPP (legacy/non-TLS), backend link	MitM, command injection, fleet-wide manipulation
Software – Embedded	OS kernel, firmware, protocol stacks	Device takeover, key extraction, privilege escalation
Software – Backend (CSMS)	Web apps, APIs	Network-wide compromise via central control plane
Human	Phishing, social engineering, and malicious USB	Credential theft, insider-enabled attacks
Supply Chain	Malicious firmware updates, compromised libraries, OEM signing keys	Trusted update abuse, systemic fleet compromise

Hybrid Methodology for Threat Modelling

Threat modelling for CPS, such as EVSE, differs fundamentally from conventional IT security analysis. In addition to protecting confidentiality, integrity, and availability, CPS environments must ensure safe and stable physical operation. A cyber compromise may therefore propagate across the digital–physical boundary. For example, tampering with charging parameters could bypass protective logic and alter active power delivery, while coordinated denial-of-service or control manipulation could generate feeder overload or grid instability. Such cross-domain consequences require threat analysis to incorporate safety, operational continuity, and stability considerations, consistent with supply-chain and systemic risk observations in critical infrastructure environments [23], [24].

To address this complexity, a structured hybrid threat modelling approach was adopted. Data Flow Diagrams (DFDs) were first constructed to represent EVSE components, trust boundaries, and control pathways. STRIDE was then systematically applied to each DFD element to enumerate Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege threats [20], [25]. This ensured comprehensive structural coverage of firmware, communication interfaces, and backend orchestration layers. However, STRIDE alone may generate theoretical threats without contextual prioritisation. Therefore, identified threats were mapped to the MITRE ATT&CK [21] framework for Industrial Control Systems to align structural weaknesses with documented adversarial tactics such as Modify Control Logic, Valid Accounts misuse, and Inhibit Response Function. This behavioural overlay acted as a realism filter, enabling prioritisation based on observed attacker tradecraft.

2.4.2 TSM Reference Architecture Design

Following the completion of structured threat modelling and vulnerability–risk analysis, the project transitioned from risk identification to risk containment through architectural enforcement. The threat modelling phase systematically identified attack surfaces (***physical, firmware, communication, backend, and grid-interaction layers***), quantified systemic risks under high DER penetration scenarios, and revealed the potential for coordinated EVSE manipulation to induce grid instability. These findings demonstrated that conventional software-centric security controls were insufficient for grid-connected EVSE ecosystems. Instead, a formally enforced trust boundary with hardware-backed control authority was required. Trusted Sovereign Monitor (TSM) Reference Architecture was developed to:

- Establish device-level enforceable trust guarantees,
- Prevent low-integrity domains from directly influencing grid-critical functions,
- Ensure secure firmware lifecycle management,
- Enforce policy-based grid safety constraints, and
- Provide verifiable runtime monitoring and containment mechanisms.

The architecture was designed as a secure-by-design control overlay applicable to large-scale EVSE deployments within the DER ecosystem.

Architectural Design Principles

The TSM Reference Architecture was grounded in the following principles:

1. **Reference Monitor & Complete Mediation** – All safety-critical operations must pass through a trusted enforcement layer.
2. **Formal Domain Separation** – Partition EVSE into Low-Integrity Domain (LID) and High-Integrity Domain (HID).
3. **Hardware Root of Trust Anchoring** – Cryptographic and firmware integrity must originate from immutable trust anchors.
4. **Grid-Aware Policy Enforcement** – Charging behaviour must comply with feeder-level and DER stability constraints.
5. **Fail-Safe Operational State Control** – Unsafe conditions trigger deterministic containment mechanisms.
6. **Secure Firmware Lifecycle Governance** – Admission, validation, and activation follow cryptographic attestation.
7. **Scalable Fleet Governance** – Architecture supports coordinated fleet-level policy management.

Steps Involved in TSM Architecture Design

Step 1 – Threat-to-Control Derivation
The first step translated identified vulnerabilities and risk scenarios into explicit architectural control requirements. Attack vectors such as OTA firmware compromise, backend impersonation, coordinated load manipulation, and device tampering were mapped to enforceable control points within the EVSE system. This derivation process distinguished between device-local risks and grid-level systemic exposure, ensuring that architectural safeguards directly addressed the most critical risk amplification pathways identified during threat modelling.

Step 2 – Formal Trust Boundary Definition
A strict trust boundary was established by partitioning the EVSE into a Low-Integrity Domain (***LID***) and a High-Integrity Domain (***HID***). The LID contains network-facing components such as communication stacks, OTA update handlers, and user interaction interfaces. The HID contains safety-critical logic, cryptographic validation mechanisms, secure storage, and hardware actuation control. The design ensures that LID components cannot directly influence power delivery, firmware activation, or safety policies without mediation by the HID.

Step 3 – Trusted Sovereign Monitor Core Integration
Within the HID, the Trusted Sovereign Monitor (TSM) was defined as the authoritative decision engine. The TSM integrates a Policy Enforcement Engine for verifying grid safety constraints, a cryptographic engine for signature and certificate validation, secure storage for policy and revocation management, and hardware interface control for enforcing actuation decisions. This integration ensures that all safety-critical decisions are subject to complete mediation through a sovereign enforcement layer.

Step 4 – Secure Firmware Admission Lifecycle Design
A controlled firmware lifecycle was architected to prevent unauthorised code execution. The lifecycle progresses from OTA delivery to LID staging, followed by HID admission validation, flash commit, secure boot verification, and controlled runtime execution. Cryptographic validation occurs before firmware activation, and execution is permitted only after integrity verification and

policy compliance checks. This process enforces admission control and prevents compromised firmware from influencing grid-critical functions.

Step 5 – Grid-Aware Policy Enforcement Embedding
The architecture embeds grid stability constraints directly within the Policy Enforcement Engine. Charging operations are evaluated against predefined safety parameters such as load ramp limits, voltage and frequency deviation thresholds, and aggregation constraints. This ensures that even valid firmware cannot induce unsafe grid behaviour, thereby integrating cyber-security enforcement with power-system stability considerations.

Step 6 – Runtime Monitoring and Containment Logic
Continuous runtime evaluation mechanisms were incorporated within the HID to detect anomalous or policy-violating behaviour. When violations are detected, deterministic containment strategies are triggered, including controlled power derating, isolation of the LID, transition to safe operational states, and secure audit logging. This ensures fail-safe operation under both cyber compromise and abnormal operational conditions.

Step 7 – Alignment with Co-Simulation Validation Framework
Finally, the reference architecture was designed to be experimentally validated within a HELICS-based EVSE–Grid co-simulation environment. Baseline EVSE behaviour without TSM enforcement was compared against TSM-governed behaviour under identical threat injection scenarios. Grid-level stability metrics, including voltage deviation and load ramp characteristics, were used to empirically assess the architectural effectiveness in mitigating systemic DER-induced risk.

Details about the overall TSM design, TSM specifications, and alignment with the co-simulation platform can be found in Technical Report 2 (Appendix- A)

2.4.3 Phase 2: Cyber–Physical Co-Simulation Platform Development

To rigorously evaluate the cyber–physical stability implications of EVSE firmware compromise, a high-fidelity co-simulation environment was developed. The objective of Phase 2 was to establish a scientifically controlled baseline model of EVSE infrastructure interacting with a distribution network under realistic operational conditions. Unlike conventional cybersecurity studies that isolate communication-layer threats, this platform models the full causal chain from firmware logic to aggregate load dynamics and feeder stability behaviour. Complete details about the co-simulation platform can be viewed in Project Report of Phase 2 in Appendix-A.

The platform was implemented using a HELICS-based federation architecture, integrating:

- EVSE behavioural models
- Electric Vehicle (EV) charging session logic
- Distribution feeder simulation (OpenDSS)
- Backend communication workflows
- Charging Station Management System (CSMS) interactions

Time-synchronised co-simulation ensured preservation of cyber–physical causality between control decisions and electrical system response.

Stability, Safety, and Security Parameters Modelled

The co-simulation platform explicitly incorporated stability-relevant DER parameters and safety constraints summarised in Table 4.

Table 4: Safety and Security parameters modelled in Co-simulation Platform

Category	Parameter / Function	Description	Stability Relevance
Electrical Variables	Active Power (P)	Real-time EVSE charging power (kW)	Direct load contribution
	Reactive Power (Q)	Reactive power exchange	Voltage regulation impact
	Aggregate Fleet Load (ΣP)	Total charging demand across EVSE fleet	Feeder loading stress
	Voltage Deviation (ΔV)	Deviation from nominal voltage	Distribution regulation compliance
	Frequency Deviation (Δf)	Frequency response under load change	System dynamic stability
	Load Ramp Rate (dP/dt)	Rate of aggregate power increase	Transient disturbance indicator
	Transformer Loading (%)	Percentage utilisation	Thermal stress constraint
EVSE Operational Logic	Charging Power Limits	Configured max kW (7, 11, 22 kW)	Aggregate demand control
	Ramp-Up Profiles	Power increase gradient	Feeder shock mitigation
	SoC-Based Charging Behaviour	Dynamic load based on battery state	Realistic demand modelling
	Session Start/Stop Events	Charging concurrency timing	Synchronisation risk
Cyber–Physical Controls	Firmware Behaviour Logic	Charging limit enforcement rules	Integrity-dependent behaviour
	Backend Command Handling	OCPP-based control messages	Remote actuation pathway
	Protection Thresholds	Overcurrent / voltage logic	Safety boundary enforcement
	Synchronised Activation Scenarios	Fleet-level load coordination	DER stability risk
Observability Metrics	Firmware Admission State	Acceptance/rejection logging	Security traceability
	Stability Threshold Flags	Voltage / ramp violation indicators	Impact quantification

EVSE Behavioural and Fleet Modelling

The EVSE behavioural model implemented realistic charging sessions, including session initiation handshakes via ISO 15118, backend coordination through OCPP, configurable charging power setpoints in the range of 7–22 kW, controlled ramp-up sequences, and fleet-level concurrency modelling. A representative stress scenario evaluated the synchronised activation of 500 EVSE units operating at 11 kW each, resulting in an instantaneous aggregate load potential of approximately 5.5 MW. Such aggregation scenarios were systematically analysed in terms of feeder voltage deviation (***ΔV***), load ramp rate sensitivity (***dP/dt***), transformer loading stress, and frequency perturbation effects, thereby enabling a quantitative assessment of stability impacts arising from coordinated EVSE behaviour

Cyber–Power Interaction Modelling

To understand firmware-induced risk propagation, the platform enabled controlled behavioural modification of EVSE firmware logic, including removal of ramp-rate constraints, override of configured charging power limits, forced synchronised fleet activation, and modification of protection thresholds. These controlled manipulations allowed systematic examination of how embedded control logic directly influences physical system behaviour.

The causal evaluation chain was therefore structured as follows: firmware logic alteration leading to charging behaviour change, which in turn affects aggregate load dynamics and ultimately manifests as measurable stability metric deviations at the feeder and system level.

This enabled empirical assessment of how firmware compromise can:

- Increase ***dP/dt***
- Elevate ***ΔV*** beyond operational tolerance
- Stress distribution assets
- Amplify fleet-level synchronisation risk

2.4.4 Phase 3: TSM Implementation and Experimentation

This section presents the methodological framework used to implement, integrate, and evaluate the TSM within the EVSE–grid co-simulation environment. The methodology formalizes the TSM security model, enforcement algorithms, operational state supervision, and controlled adversarial evaluation strategy. The objective is to demonstrate deterministic security enforcement without degrading operational stability.

The TSM is designed as a formally structured supervisory control mechanism that enforces complete mediation over all security-sensitive operations within the EVSE. The security model operationalizes the outcomes of the architectural decomposition and threat analysis by transforming identified vulnerabilities into enforceable runtime constraints. Rather than functioning as a passive monitoring layer, the TSM is positioned as an active decision authority capable of intercepting, validating, and conditionally authorizing control actions prior to their execution by the underlying power electronics or firmware subsystems.

TSM Security Model

The security model is conceptually grounded in the reference monitor paradigm and is constructed to satisfy the properties of completeness, isolation, and verifiability. Completeness ensures that all security-relevant actions are subject to validation before execution. Isolation guarantees that enforcement logic cannot be bypassed by lower-integrity components. Verifiability enables deterministic reasoning about enforcement outcomes. The design is structured around five foundational principles:

Complete Mediation. Every action affecting firmware integrity, power delivery parameters, configuration registers, or external communication channels is intercepted before execution. No write operation to safety-critical resources is permitted without explicit validation by the TSM.

Domain Separation. Operational logic and enforcement logic are executed within distinct integrity domains. This separation prevents privilege escalation and ensures that compromised operational components cannot override supervisory decisions.

Deterministic Enforcement. All decisions are derived from explicit policy constraints evaluated against the current system state. This eliminates nondeterministic behaviour and ensures reproducibility of enforcement outcomes under identical conditions.

State-Aware Control. Enforcement decisions are dependent on the operational state of the EVSE. Actions that may be safe in one state (e.g., Idle) may be prohibited in another (e.g., Charging).

Hardware-Rooted Trust. Firmware authenticity and configuration integrity are validated through cryptographic mechanisms anchored in trusted root certificates and secure storage, ensuring continuity of trust across update cycles.

Together, these principles define a security model that is both preventive and supervisory, capable of constraining unsafe behaviour even under partial system compromise.

Dual-Domain Execution Architecture

To implement these principles, the EVSE runtime environment is partitioned into two logically and functionally distinct domains as depicted in the figure 8 below.

The **Low-Integrity Domain (LID)** comprises operational firmware logic, communication protocol stacks (e.g., OCPP, ISO 15118), session management routines, and device drivers interfacing with hardware components. This domain is responsible for normal charging operations but is considered potentially exposed to external inputs and adversarial manipulation.

The **High-Integrity Domain (HID)** hosts the Trusted Sovereign Monitor Core, the Policy Enforcement Engine, the Cryptographic Verification Module, and secure storage mechanisms for certificates, firmware hashes, and configuration metadata. The HID functions as the authoritative decision layer.

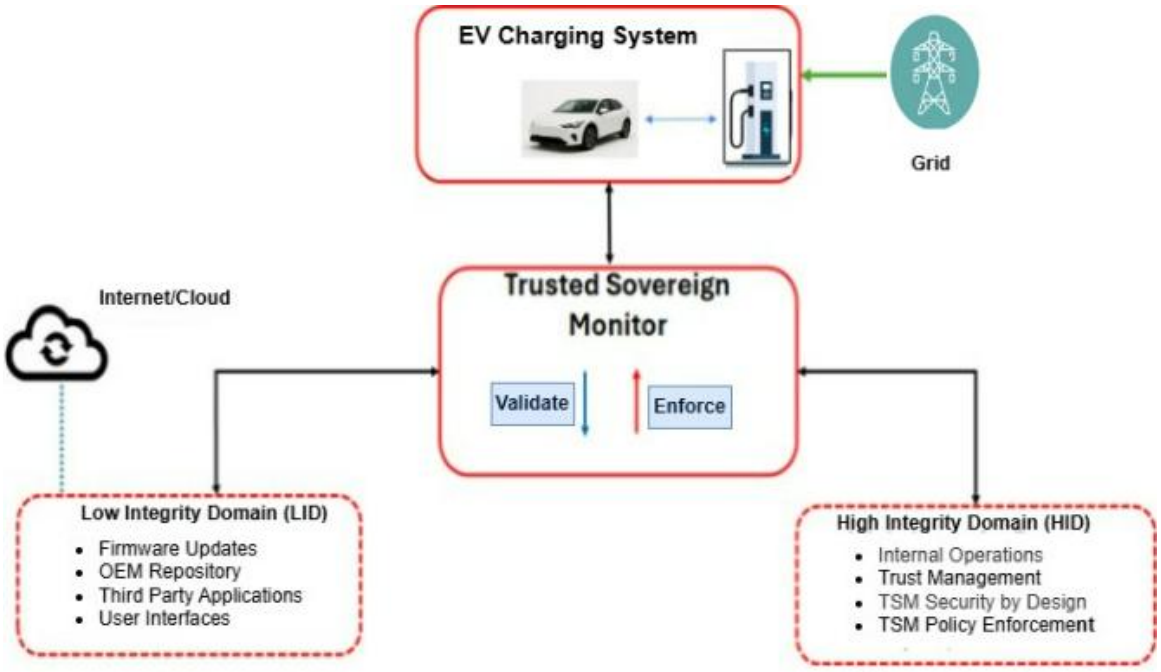


Figure 8*: TSM with Dual Domain Architecture*

All write-access to safety-critical resources, including firmware flash memory, power setpoint registers, and persistent configuration parameters, is gated through the HID. The LID may request actions, but execution is contingent upon HID authorization.

Let the system be formally represented as follows:

- ***S*** denotes the system state vector, encapsulating operational state, firmware version, power parameters, and session context.

- ***A*** denotes a requested action issued by the LID or an external entity.
- ***P*** denotes the policy constraint set defining permissible actions under each state.

The TSM enforcement mechanism can therefore be defined as a decision function:

E(A,S)E(A, S)E(A,S)

which produces one of four outcomes:

- **Allow** — the requested action satisfies all policy constraints for the current state.
- **Override** — the requested action exceeds policy bounds but can be corrected through bounded adjustment (e.g., power setpoint clamping).
- **Deny** — the action violates policy constraints and cannot be safely corrected.
- **Safe** — the system transitions to a predefined safe operational state due to detection of an unsafe or integrity-compromised condition.

Formally, the enforcement function can be expressed as follows:

E(A, S) =

Allow ***if A ∈ P(S)***

Override ***if*** *the violation is bounded and correctable*

Deny ***if*** *the action is unauthorized or policy-prohibited*

Safe ***if S*** *indicates an unsafe integrity condition*

Core TSM Algorithms

The TSM operationalizes its security model through a set of deterministic enforcement algorithms. These algorithms directly implement the formal decision function ***E(A,S)*** described above and ensure that policy constraints are evaluated prior to execution of security-sensitive actions. Each algorithm corresponds to a high-impact threat category identified during architectural threat modelling. The enforcement mechanisms are structured to preserve operational continuity where possible while preventing unsafe or unauthorized behaviour.

The algorithms implemented in the TSM include:

1. Secure Firmware Admission Control
2. Power Setpoint Enforcement
3. Authenticated Command Validation
4. State Transition Integrity Enforcement

Each is described below.

Secure Firmware Admission Control

Firmware integrity represents one of the most critical security boundaries within the EVSE. Compromise at this layer enables persistent manipulation of charging logic, safety checks, and communication protocols. The Secure Firmware Admission Control algorithm ensures that only authenticated and authorized firmware images are accepted for execution.

Algorithm 1: Secure Firmware Admission Control

***Input**: F (firmware image), σ (signature), v (version), v_current (installed version), S (state)*

***Output**: Accept or Reject*

```
if VerifySignature(F, σ) = False then
    return Reject
if ValidateCertificateChain(F) = False then
    return Reject
if CheckRevocationStatus(F) = Revoked then
    return Reject
if v ≤ v_current then
    return Reject
if S ≠ Idle then
    return Reject
CommitFirmware
CommitFirmware(F)
return Accept
```

If any validation step fails, the firmware update is rejected, and a policy violation is recorded. Importantly, validation occurs within the High-Integrity Domain and cannot be bypassed by Low-Integrity Domain components.

Power Setpoint Enforcement

The EVSE operates as a grid-connected cyber-physical system. Manipulation of power delivery parameters can impact both battery safety and grid stability. The Power Setpoint Enforcement algorithm ensures that commanded power values remain within policy-defined safety bounds.

Algorithm 2: Power Setpoint Enforcement

***Input**: P_req (requested power), P_max (policy threshold)*

***Output**: P_out (enforced power output)*

```
if P_req ≤ P_max then
    P_out = P_req
else
    P_out = P_max
LogEnforcement(P_req, P_out)
return P_out
```

The bounded override mechanism ensures that malicious or erroneous commands cannot induce unsafe behaviour. Unlike binary rejection, bounded override preserves service continuity while enforcing safety constraints.

Authenticated Command Validation

Backend communication channels represent a critical attack surface. Unauthorized commands transmitted over compromised channels could manipulate charging behaviour or initiate unsafe firmware updates.

Algorithm 3: Authenticated Command Validation
***Input**: M (control message)*
***Output**: Accept or Reject*
if VerifyTLS(M) = False then
return Reject
if ValidateClientCertificate(M) = False then
return Reject
if CheckAuthorizationRole(M) = False then
return Reject
ExecuteCommand(M)
***return** Accept*

Only commands satisfying all cryptographic and authorization checks are forwarded to execution.

State Transition Integrity Enforcement

The TSM enforces correctness of operational state transitions. Charging state transitions follow a defined state machine, and unsafe transitions are blocked.

Algorithm 4: State Transition Integrity Enforcement
***Input**: S_t (current state), S_next (requested state)*
***Output**: Allow or Deny*
if S_next ∉ ValidTransitions(S_t) then
return Deny
UpdateState(S_next)
***return** Allow*

TSM Operational State Model

The TSM operates as a state-aware supervisory controller that evaluates enforcement decisions in the context of the operational condition of the EVSE. Security-sensitive actions are not validated in isolation but are interpreted relative to the current execution state of the charger. This ensures that actions that may be permissible in one state are appropriately restricted in another. The operational state model, therefore, provides the semantic foundation for policy enforcement, transition validation, and safe execution control.

The EVSE under TSM supervision is modelled as a finite-state system ***M = (S, T, I),*** where S represents the set of operational states, T represents the permitted transition relation between states and represents the safety invariants that must hold within each state. The TSM continuously monitors state transitions and enforces invariant preservation through deterministic evaluation of requested actions. By integrating state awareness into the enforcement logic, the TSM ensures that runtime decisions are context-sensitive and aligned with operational safety requirements. The figure 9 illustrates the supervisory abstraction of the TSM state machine. At the highest level, the system transitions from ***BOOTING to OPERATIONAL*** only after successful secure boot validation and integrity verification. If an integrity failure or tamper condition is detected during boot, the system transitions directly to FAIL_SAFE, ensuring fail-secure containment. During runtime, any critical policy violation within the **OPERATIONAL** state similarly results in a transition to FAIL_SAFE. Recovery from FAIL_SAFE requires authorized manual reset, preserving administrative control and preventing automatic recovery from integrity compromise.

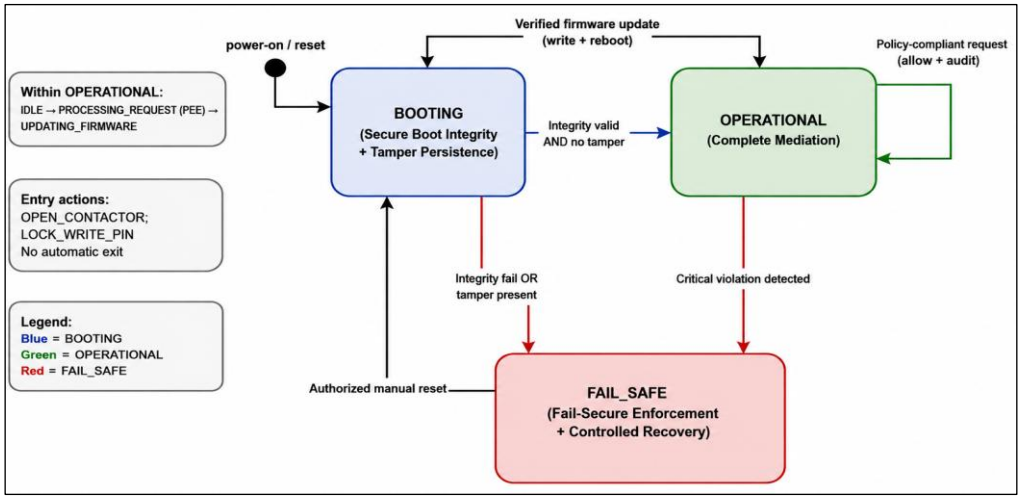


Figure 9*: TSM Abstract Operational States*

Operational States under TSM Supervision

The internal operational states supervised by the TSM are summarized in Table below. These states refine the high-level supervisory model and define the permissible runtime behaviour of the EVSE under policy enforcement.

Table 5: TSM internal operational states

Idle	Charger available; no active power delivery.	Firmware updates permitted; power output must remain zero.
Preparing	Session authentication and negotiation.	Configuration limited; firmware updates prohibited.
Charging	Active power transfer.	Power constrained (P ≤ P_max); firmware updates prohibited.
Finishing	Controlled session termination.	No configuration changes; controlled shutdown only.
Fault	Operational anomaly detected.	Power restricted or disabled.
Safe	Supervisory fail-secure containment.	Output minimized or disconnected; commands restricted.

The transition relation T defines the permitted successor states for each operational condition. Transitions not belonging to the valid transition set are rejected by the TSM. For instance, transition from Charging directly to a firmware update state is explicitly prohibited. However, transition from Charging to Finishing and subsequently to Idle is permitted under normal session termination. The TSM validates each requested transition ***S(t+1***) against the allowable transition set ***T(S(t))*** prior to execution. Safety invariants are defined for each state to ensure integrity preservation. During Charging, the active power setpoint must satisfy $\mathbf{P \leq P_{max}}$. In the idle state, power output must remain zero. In the safe state, output is clamped to minimal or disconnected entirely. Violation of any invariant results in immediate supervisory evaluation through the enforcement function ***E(A, S***), potentially triggering state transition to Safe.

TSM Integration within the Co-Simulation Platform

The TSM was integrated into the EVSE–grid co-simulation platform as a supervisory control component positioned between operational logic and safety-critical actuation layers. The objective of this integration was to evaluate enforcement behaviour under realistic cyber-physical conditions

without altering baseline system functionality. The co-simulation environment comprises three principal logical entities:

(i) the EVSE operational model,
(ii) the grid simulation model, and
(iii) the threat injection module.

The TSM is inserted as an intermediary enforcement layer that mediates all security-sensitive control paths. Specifically, all requests originating from the EVSE logic, backend communication channels, or simulated adversarial inputs are routed through the TSM before execution.

TSM Mediation and Integration Architecture

The TSM is integrated into the co-simulation environment as a supervisory mediation layer positioned between EVSE operational logic and safety-critical actuation components. All security-sensitive requests, including firmware updates, power setpoint changes, state transitions, and backend control commands, are intercepted before execution. The TSM is integrated into the HELICS co-simulation environment as a supervisory mediation layer between EVSE operational logic and grid-facing actuation components. As shown in the figure 10, requests generated by the EVSE Federate (Low-Integrity Domain (***LID***)) are routed through the TSM Federate before execution within the grid or power electronics model, establishing a clear trust boundary between operational logic and high-integrity enforcement.

Each requested action A is evaluated together with the current system state S using the enforcement function ***E(A,S).*** Only actions producing Allow or bounded Override outcomes are propagated to the power electronics abstraction layer. All other requests are rejected or result in transition to the Safe state, ensuring complete mediation of critical operations. Power control commands are validated against policy thresholds, enforcing the constraint **P≤Pmax** , with bounded override applied when necessary. Firmware updates are gated through cryptographic validation, monotonic version enforcement, and state eligibility checks (Idle required), followed by integrity re-verification upon reboot. Enforcement is executed synchronously within each simulation cycle before state commitment, preserving deterministic behaviour. The baseline EVSE logic remains unchanged; the sole architectural difference between configurations is the presence of the TSM mediation layer, enabling controlled evaluation of supervisory security impact.

Experimental Design and Threat Injection

Building upon the mediation architecture described in the previous section, a controlled experimental framework was established to evaluate the supervisory effectiveness of the TSM. Two configurations were executed under identical HELICS synchronization: (i) baseline EVSE operation without TSM enforcement, and (ii) supervised operation with the TSM mediation layer enabled. This structural consistency ensures that observed differences are attributable solely to enforcement behaviour. Threat scenarios were injected via the Scenario Manager and Threat Injector, including malicious firmware updates, power setpoint escalation, unauthorized backend commands, and invalid state transitions. Each scenario was triggered at predefined simulation timestamps to ensure deterministic and repeatable evaluation. System response was assessed through two evidence streams: grid-level stability metrics (ΔV, Δf, RoCoF, ramp rate, recovery time) and TSM enforcement traces, refer to figure below.

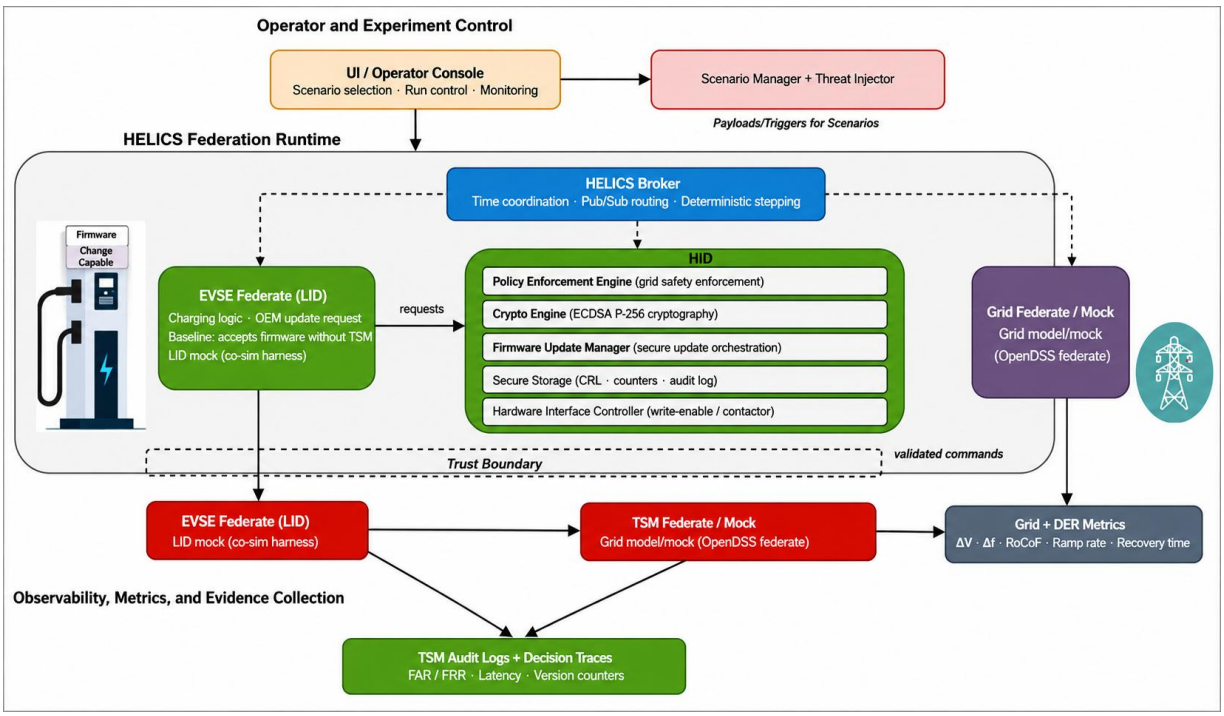


Figure 10*: Integration of the TSM within the Co-Simulation Platform employing supervisory mediation and trust boundary separation*

2.4.5 Phase 4. Policy Recommendations and Dissemination

The final phase of the project extends the technical and experimental findings toward policy implementation and sector-wide adoption. Building on the architectural validation and enforcement assessment conducted earlier, this stage aims to develop a practical roadmap for integrating TSM-enabled DER devices into Australia's energy system. This phase combines empirical insights from vulnerability analysis, formal security modelling, and co-simulation experimentation to guide governance, standards alignment, and regulatory pathways. Structured stakeholder consultation is conducted with AEMO, the Australian EV Council, DNSPs, and relevant standards organizations to ensure practical adherence to AS/NZS charger and inverter standards. Consideration is also given to regulatory mechanisms, including potential mandatory TSM functionality for higher-capacity DER devices.

2.5 Summary

The methodology establishes a structured progression from EVSE architectural exploration and empirical vulnerability analysis to hybrid threat modelling and TSM-based formal security modelling, culminating in supervised integration and controlled experimentation to assess DER stability and cyber-physical impact. The following section presents the consolidated results across all project stages, demonstrating the effects of threat modelling, architectural specification, and TSM enforcement under simulated adversarial conditions.

3 Results

This section presents the project outcomes across different phases outlined in Section 2 above. It provides threat modelling results, including vulnerabilities, attack surfaces, and systemic risk pathways, and related findings. EVSE baseline co-simulation results for the EVSE–grid platform under normal operations are presented next. Finally, it provides implementation and experimentation results, including threat injection scenarios and comparative evaluation (with and without TSM) to quantify security effectiveness and DER stability impacts.

3.1 EVSE Vulnerabilities Analysis

The EVSE ecosystem is very complex, and to aid vulnerability exploration, we adopted an evidence-based approach combining EVSE vulnerabilities from existing literature and NVD databases. An analysis of identified vulnerabilities is provided below.

3.1.1 Vulnerabilities Findings

The academic and industry literature reveals several recurring themes and classes of vulnerabilities that plague the EVSE ecosystem. These findings were drawn from the extensive surveys. With these findings EVSE attack surface is developed with key architectural components and interfaces. The attack surface is depicted in the figure 11 below.

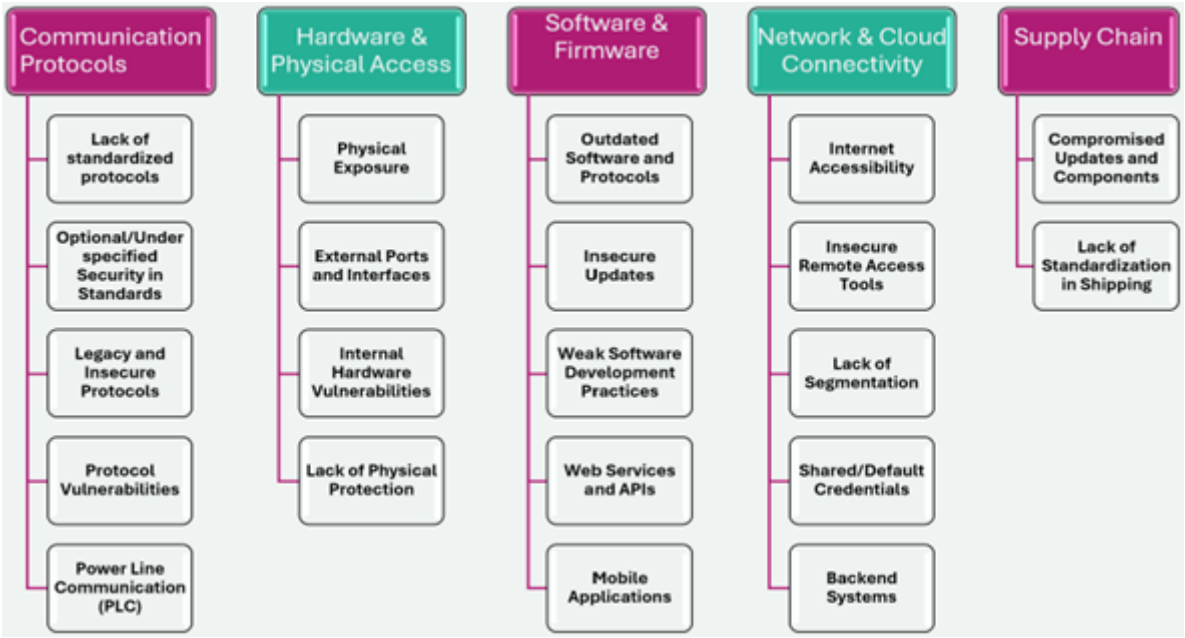


Figure 11: *Key Interfaces and Components that Contribute to the EVSE Attack Surface*

The literature consistently identifies systemic security weaknesses across EVSE communication, hardware, software, and supply-chain layers. Legacy protocols such as OCPP 1.6, MQTT, and

CHAdeMO often lack mandatory encryption, enabling MitM, DoS, impersonation, and false data injection attacks [43]. Even modern standards like ISO 15118 permit optional TLS in loosely defined "trusted" environments, increasing implementation risk. PLC-based communication is inherently susceptible to interception and manipulation. Physically accessible chargers expose USB, Ethernet, and debug interfaces, while many devices lack a hardware root of trust, enabling persistent firmware compromise. Weak authentication practices, hard-coded credentials, and unsigned firmware updates further exacerbate risk. Internet-exposed EVSEs and poorly segmented networks allow lateral movement and fleet-scale compromise. Additionally, supply-chain weaknesses and insecure factory configurations introduce pre-deployment risks. Collectively, these findings reveal a fragile trust model vulnerable to scalable cyber-physical disruption

Consolidated Vulnerabilities

The vulnerabilities identified through the literature review and NVD analysis are presented in a tiered approach to provide both a high-level overview and detailed traceability. Empirical CVE Analysis and Risk Implications. The empirical extraction of publicly disclosed CVEs associated with EVSE products confirms that the risks identified through architectural analysis are not theoretical abstractions but are actively manifested in deployed systems. The documented vulnerabilities demonstrate real-world exploitability across multiple architectural domains, reinforcing the systemic exposure outlined earlier.

Severity and Exploitability Trends.

A substantial proportion of identified CVEs enable Remote Code Execution (RCE) or privilege escalation, indicating high-impact compromise potential. Notably, vulnerabilities such as CVE-2024-11666 reveal that insecure cloud communication channels permit unauthenticated RCE, effectively enabling full fleet takeover. This demonstrates that backend weaknesses are not isolated configuration flaws but represent scalable control vectors capable of orchestrating coordinated disruption.

Vulnerabilities by Architectural Domain.

The Local Device domain accounts for approximately 36% of critical threats and presents the largest physical and embedded attack surface (average Residual Risk Score: 21.5). Vulnerabilities such as CVE-2025-5828, involving stack overflows via USB/BLE paths, illustrate how adjacent or local access can escalate to complete device takeover. Although the Backend/Cloud domain contains fewer total vulnerabilities (11%), it exhibits the highest average risk score (24.1). This reflects systemic amplification: a single backend compromise can propagate across an entire fleet, multiplying operational and grid-level consequences.

3.1.2 Vulnerability Type Concentration (CWE Analysis).

The weakness taxonomy reveals clustering in high-consequence classes. CWE-494 (Unsigned Firmware) enables persistent takeover through malicious OTA updates; CWE-295 (Improper Certificate Validation) allows DERMS impersonation and fraudulent load manipulation; and CWE-319 (Cleartext Transmission) facilitates MitM interception and command injection. The following tables summarize the most critical and representative vulnerabilities for each architectural domain.

Table 6 outlines critical vulnerabilities affecting the direct communication link between the Electric Vehicle and the EVSE, primarily concerning the ISO 15118 protocol.

Table 6: Critical Vulnerabilities in the EV to EVSE Domain

ID	CWE	Description	Potential Impact
V-001	CWE-287	Forged ISO 15118 certificate enabling unauthorized charging sessions.	Billing Fraud, False Load Demand
V-010	CWE-319	Cleartext transmission of sensitive information over PLC communication.	Data Leakage, Session Hijacking
V-031	CVE-2024-37310	Integer/heap overflow in EVerest V2G server affecting ISO 15118 session.	Denial of Service, Remote Code Execution
V-032	CVE-2022-0878	"Brokenwire" RF interference DoS attack against CCS PLC link.	Denial of Service

Table 7 details vulnerabilities inherent to the physical EVSE hardware and its local interfaces, which can be exploited by an attacker with direct or adjacent network access.

Table 7: Critical Vulnerabilities in the EVSE Local Device Domain

V-003	CWE-494	Unsigned firmware may allow persistent EVSE takeover.	RCE, Persistent Compromise
V-005	CWE-307	Denial-of-Service against local management API via repeated failed logins.	Denial of Service
V-011	CWE-284	No authentication on RS-232 commissioning port enabling direct shell access.	Full Device Takeover
V-027	CVE-2021-22729	Hard-coded admin password in Schneider EVlink products.	Full Device Takeover
V-033	CVE-2025-5828	Stack overflow via USB/BLE paths in Autel MaxiCharger wallboxes leading to RCE.	Full Device Takeover

Table 8 addresses vulnerabilities that can be introduced before the EVSE is even deployed, focusing on risks from the hardware and software supply chain.

Table 8*: Critical Vulnerabilities in the EVSE to Grid / DERMS Domain*

ID	CWE	Description	Potential Impact
V-009	CWE-295	Improper certificate validation allowing DERMS impersonation.	Grid Instability, Coordinated Disruption
V-019	CWE-290	Authentication bypass on grid control endpoints.	Manipulation of Grid Services
V-020	CWE-345	Insufficient validation of grid dispatch commands.	Load Oscillation, Feeder Perturbations

3.2 EVSE Attack Surface Analysis

The EVSE attack surface represents the aggregate of all physical, logical, and human interaction points through which an adversary may inject, manipulate, or extract data, or otherwise influence system behavior. The vulnerability evidence summarized in Tables (7-8) demonstrates that this surface is neither isolated nor narrowly confined to a single interface; instead, it spans embedded hardware, EV–EVSE communication channels, backend/cloud management systems, and grid-facing control interfaces. The domain-based graphical analysis further illustrates the concentration of

critical vulnerabilities across architectural layers, while the impact distribution visualizations in the graphs below (Figures 12, 13) highlight the prevalence of high-severity outcomes such as remote code execution, device takeover, and grid instability. Together, the tables and graphs confirm that EVSE infrastructure exhibits multi-layered exposure with clear pathways for cross-domain escalation, reinforcing its systemic cyber-physical risk profile.

The EVSE attack surface can be categorised into four interconnected domains:

- Physical: Publicly accessible hardware enables direct tampering and firmware compromise.
- Network: Multi-zone communications expose command injection and fleet-scale manipulation risks.
- Software: Firmware and backend flaws enable remote code execution and persistent takeover.
- Human: Operational workflows allow credential theft and privileged misuse.

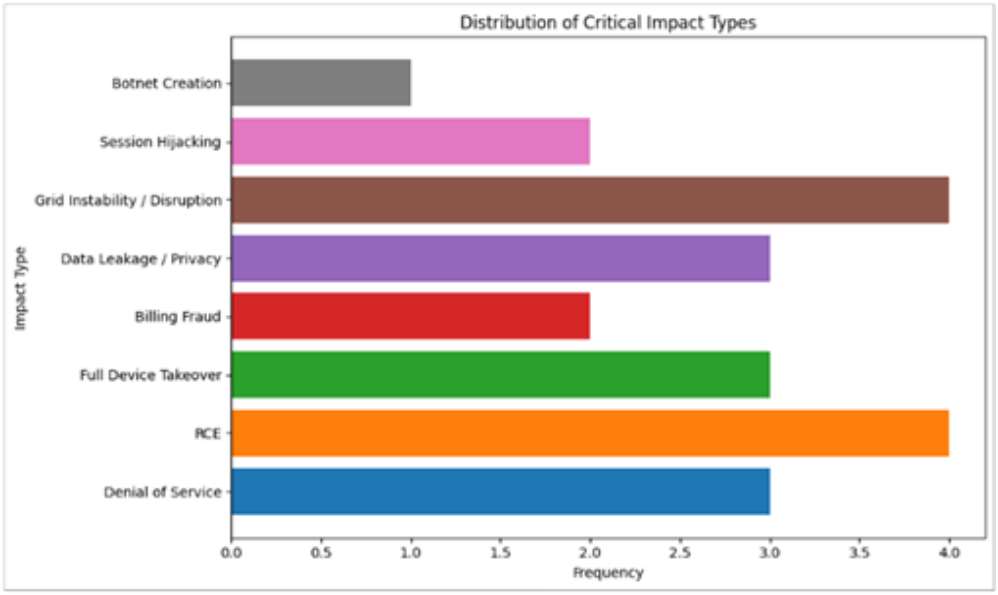


Figure 12*: Vulnerabilities distribution with cyber impact types for EVSEs*

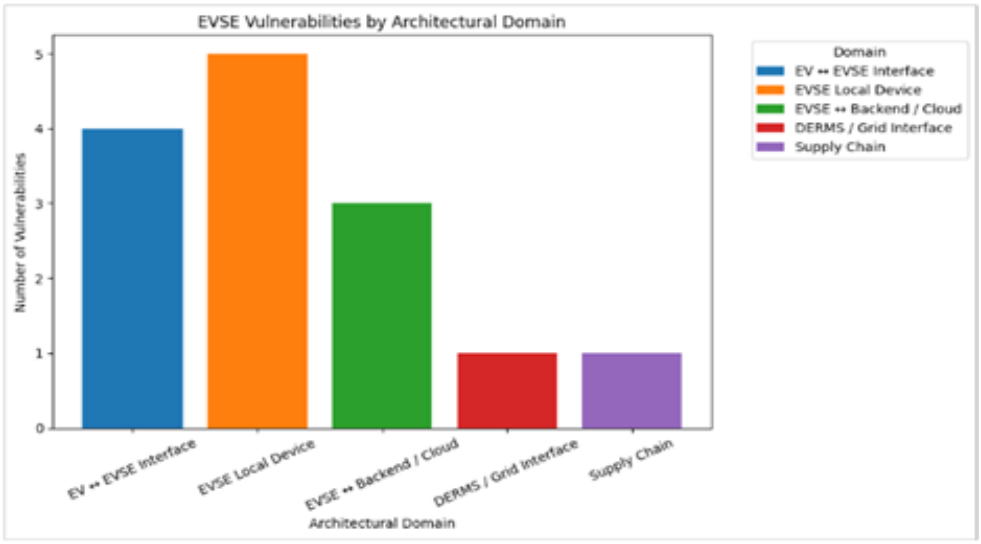


Figure 13: ***EVSE Vulnerabilities by Architecture Domain***

Firmware Governance and Trust Weaknesses:

Form analysis following EV charge station firmware governance-related weaknesses is identified:

- **Absence of Hardware Roots of Trust:** A critical finding is that many deployed devices lack hardware-based security features, such as a Trusted Platform Module (TPM) or secure boot mechanisms. This allows attackers with physical access to install persistent malicious firmware.
- **Insecure Update Validation:** The failure to cryptographically validate the signature of OTA firmware update files allows adversaries to intercept the process and push weaponized images to chargers, permanently compromising the device.

3.3 Attack Graphs Analysis

This section builds upon vulnerabilities and threats modelling to analyse attackers' tactics and techniques, leveraging identified vulnerabilities and the MITRE ATT&C ICS framework. It visualizes how a determined adversary would chain these disparate vulnerabilities and threats together into a coherent, multi-stage campaign. The attack paths are analysed for two selected scenarios as discussed below.

Firmware Compromise Attack

The firmware compromise attack graph demonstrates that EVSE risk is driven by amplification dynamics and trust-boundary convergence rather than isolated flaws. Although entry vectors differ, being remote, LAN, or physical, they converge on firmware integrity and the CSMS trust relationship, as illustrated in the attack graph below. Many of these high-leverage weaknesses are rooted in OEM-controlled mechanisms, including firmware signing governance, certificate provisioning, and OTA update validation. Identified exploitation paths include:

Remote Network Exploitation: A remote adversary exploits cloud-facing vulnerabilities (e.g., OCPP MitM, public-facing RCE, certificate abuse) to gain CSMS control, push malicious firmware via the OTA channel, and achieve scalable, fleet-wide compromise.

LAN / Proximity Compromise: An attacker with local network access performs service discovery, exploits privilege escalation or memory corruption flaws, and directly modifies controller tasking to implant malicious firmware, using the EVSE as a pivot toward backend systems.

Physical Access Compromise: A hands-on adversary leverages unsecured hardware interfaces (e.g., UART, default credentials) to obtain root shell access and overwrite firmware directly, bypassing all network-level defences for persistent device takeover.

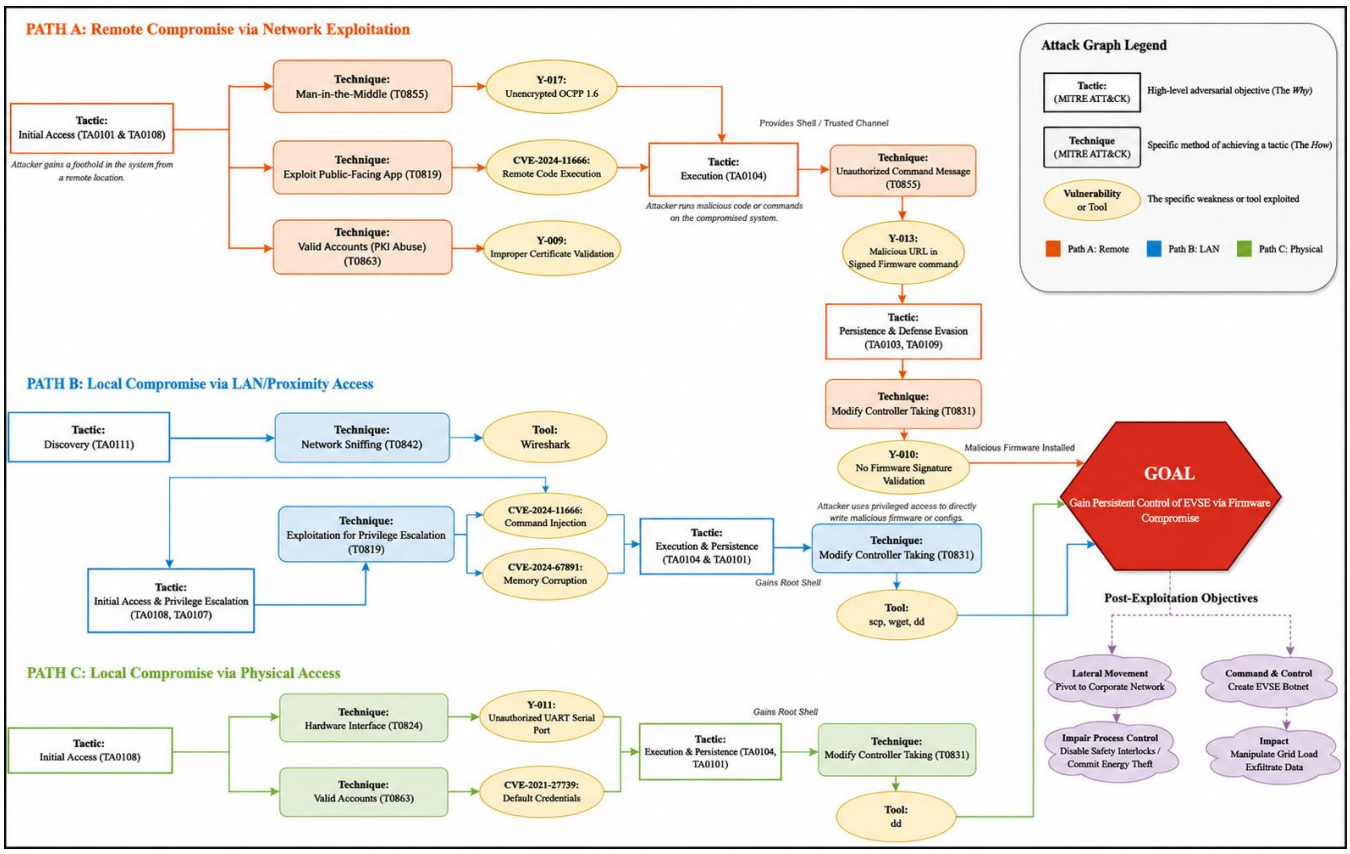


Figure 14: ***Firmware Compromise Attack Graph with multiple attack paths EVSE Cross-Domain Propagation***

A fundamental finding of this analysis is that EVSE vulnerabilities do not exist in isolation; they are highly interconnected. Adversaries chain these weaknesses together to traverse trust boundaries, pivoting from low-security IT environments to high-impact OT physical systems. The attack-chain diagram below illustrates how isolated EVSE vulnerabilities propagate across trust boundaries, enabling escalation from IT-layer compromise to fleet-wide manipulation and grid-level impact, thereby visually substantiating the cross-domain propagation patterns discussed above. Identified propagation patterns include:

Physical Attack Surface to Firmware and Network: An attacker exploits the physical attack surface by accessing an unsecured debug port, such as UART (V-011). They leverage this to overwrite the firmware, bypassing missing signature checks (V-003). The newly compromised charger then uses its trusted Wide Area Network (WAN) connection to launch lateral attacks against the CPO's backend CSMS.

Backend Compromise to Fleet-Wide Control: An attacker exploits an IT-layer web vulnerability, such as a persistent Cross-Site Scripting (XSS) flaw in the CSMS portal (CVE-2024-21550), to hijack an administrator's session. Using these privileges, the attacker exploits a remote code execution flaw (CVE-2024-11666) to push a malicious firmware update to the entire fleet simultaneously.

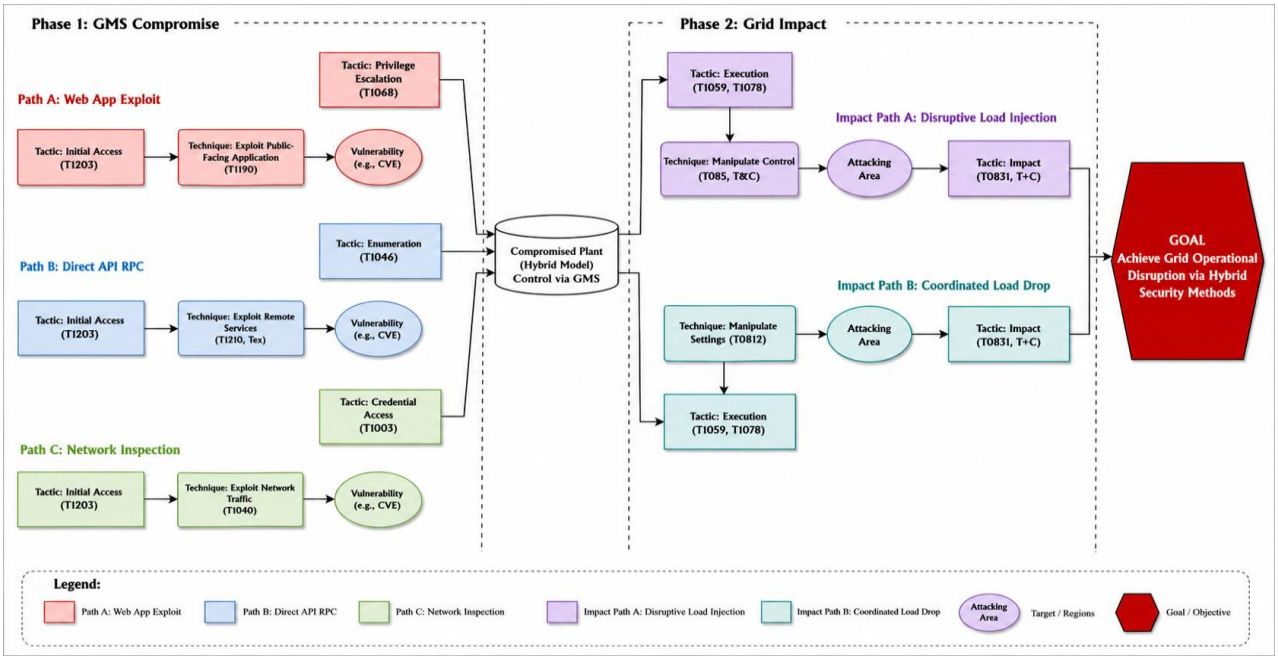


Figure 15: ***EVSE attack-chain model demonstrating cross-domain propagation from backend compromise to fleet-wide control and grid-level disruption.***

3.4 Risk Analysis

Following the structured threat modelling phase using Data Flow Diagrams (DFDs) and the STRIDE framework, the analysis transitioned from identifying static vulnerabilities to quantifying adversarial impact across architectural trust boundaries. The objective of this phase was not merely to enumerate threats, but to evaluate their systemic propagation potential across firmware, controller, communication, and grid-interfacing components of the EVSE ecosystem. Risk scoring incorporated impact, exposure breadth, and exploitability, enabling differentiation between inherent risk (pre-control exposure) and residual risk (post-control exposure). This quantitative evaluation provides architectural insight into where structural weaknesses persist, particularly at firmware trust boundaries and grid-facing command interfaces. The results are visualised through distribution, severity, concentration, and driver-based analyses.

3.4.1 EVSE Threat Distribution Across STRIDE Categories

The graph in figure 16 presents the distribution of EVSE threats mapped against STRIDE categories. Firmware update mechanisms and controller interfaces exhibit the highest concentration of identified threats, particularly under Tampering, Elevation of Privilege, and Spoofing. This distribution confirms that firmware integrity and command-path manipulation represent dominant attack vectors. These components operate at convergence points between device logic and external communication channels, making them structurally attractive to adversaries.

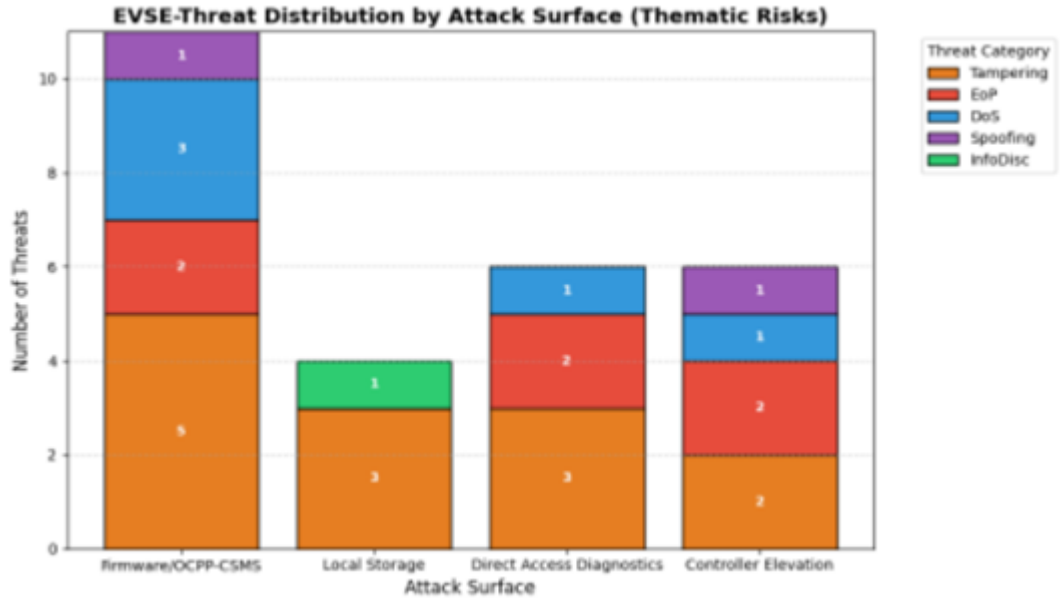


Figure 16: ***EVSE-Threat Distribution with STRIDE Model***

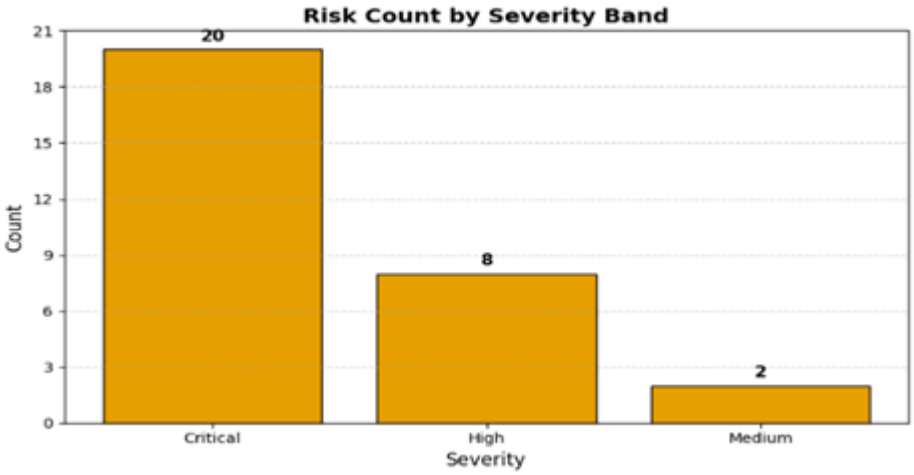


Figure 17***: Risk Count by Severity: overall distribution of identified risks by severity level.***

To further quantify the seriousness of these findings, figure 17: Risk Severity Distribution Across Identified Threats presents the overall distribution of risks by severity level. The graph shows that a significant proportion of identified threats fall within the high-severity category, indicating substantial potential impact on system integrity and grid stability.

3.4.2 Structural Dynamics of High-Risk Threats

The analysis reveals a concentration of high-impact threats within firmware integrity mechanisms, controller logic, and grid-command interfaces. As shown in figure 18 (Top 10 Threats by Residual Risk Score), grid-facing communication channels (e.g., IEEE 2030.5/OpenADR) and firmware validation weaknesses dominate the highest exposure tier. These risks are structurally embedded at architectural trust boundaries, where compromise enables influence over both local device behaviour and upstream grid coordination.

The persistence of elevated risks after assumed mitigation is illustrated in figure 19 (Comparison of Inherent vs Residual Risks). Threats positioned above the diagonal line indicate limited suppression due to detection difficulty, exposure breadth, or systemic amplification. Backend-mediated command manipulation remains particularly persistent, whereas single-device disruptions show comparatively constrained propagation. This confirms that escalation potential, rather than exploitability alone, drives sustained residual exposure. Further decomposition in figure 20 (EVSE Risk Drivers) shows that Impact (I), Exposure (E), and Business/Systemic Consequence (B) consistently dominate the highest-ranked risks, while Detection (D) and Control Strength (C) remain weaker. This imbalance explains the recurrence of firmware tampering, controller privilege escalation, and grid-command interruption among top threats, confirming that exposure is anchored in firmware trust boundaries and grid-interaction interfaces capable of fleet-scale cyber–physical impact.

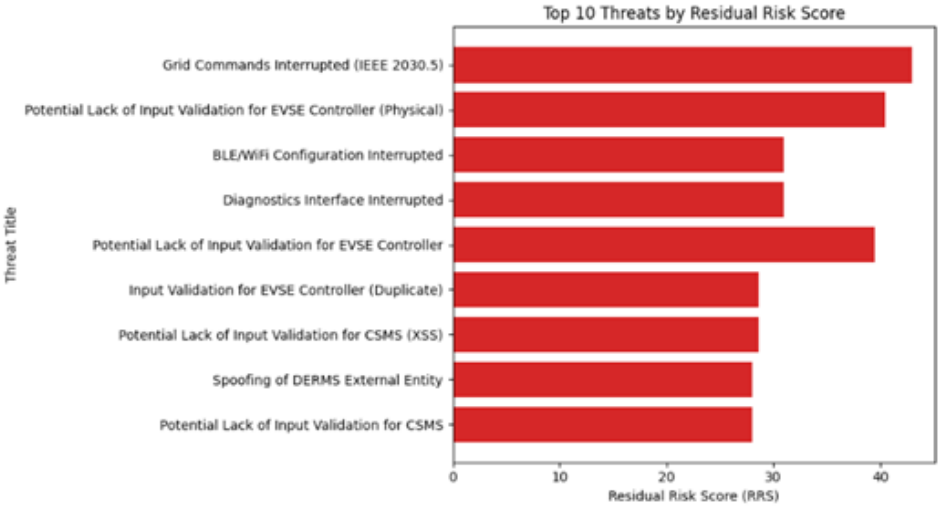


Figure 18 ***: Top 10 Threats***

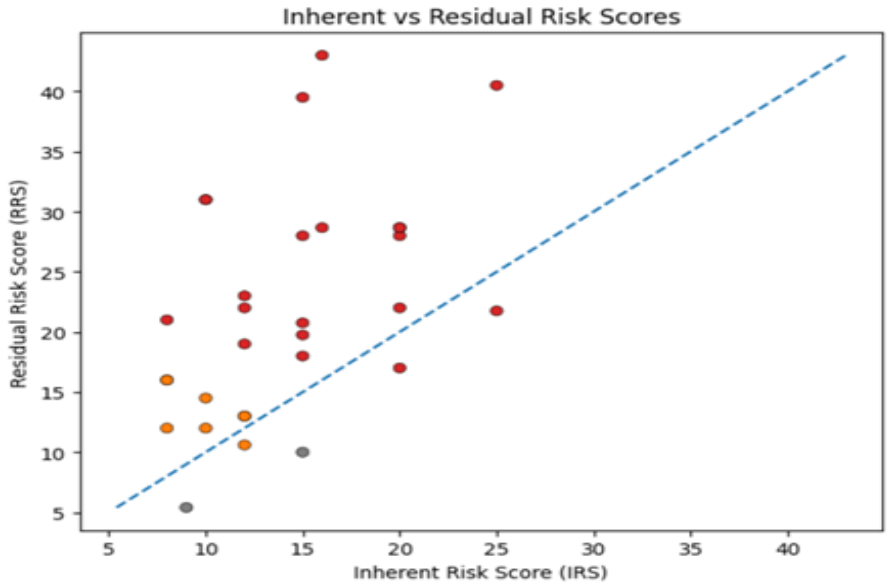


Figure 19***: Comparison of Inherent vs Residual Risks***

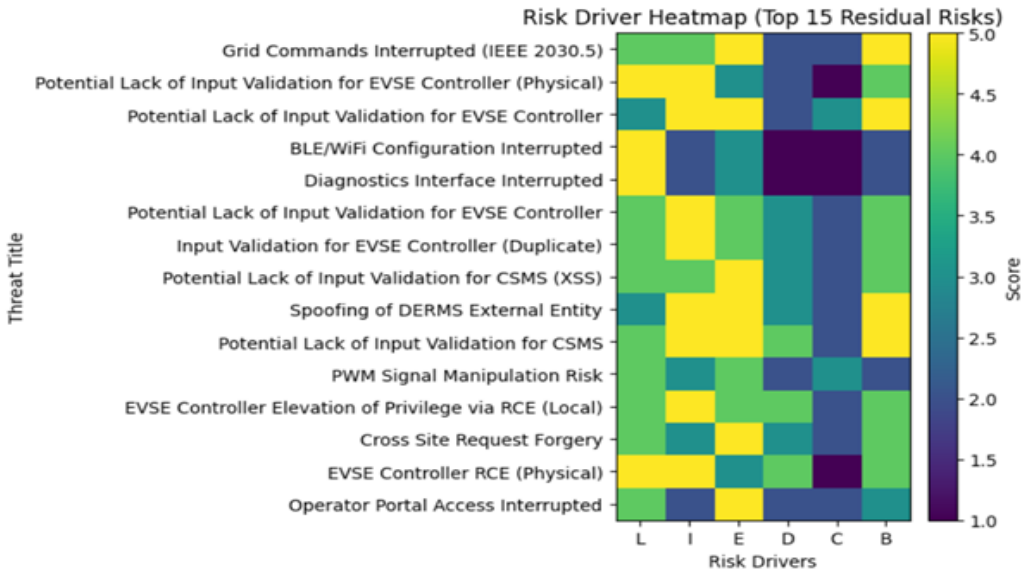


Figure 20: ***EVSE Risk Drivers***

3.5 TSM Reference Architecture

This section presents the TSM Reference Architecture, its structural composition, integration into the co-simulation platform, and enforcement guarantees. The focus is on architectural design validity rather than empirical performance outcomes.

3.5.1 Architectural Design Realisation

The TSM Reference Architecture was realised as a dual-domain security model separating externally exposed EVSE components from safety-critical control logic. The design formalises trust boundaries, defines enforcement responsibilities, and embeds functional requirements directly into architectural components rather than post-deployment controls. The Table 9 below presents core TSM components with their functions.

Table 9: Core Architectural Components and Functional Alignment

Component	Domain	Architectural Role	Enforced FRs	Trust Boundary Responsibility
TSM Core Monitor	HID	Central mediation controller	FR-1	Complete mediation of privileged operations
Policy Enforcement Engine	HID	Command validation & constraint evaluation	FR-4	Grid-command policy compliance
Cryptographic Validation Engine	HID	Firmware authentication & integrity checks	FR-2	Firmware trust anchoring
Firmware Admission Manager	HID	OTA lifecycle control	FR-2, FR-3	Update-path authorisation
Secure Storage Module	HID	Policy, key & log integrity	FR-6	Trust anchor persistence
Hardware Interface Controller	HID	Actuator signal gating	FR-5	Prevents LID bypass
OTA Receiver	LID	Firmware ingestion	—	No execution authority
Grid Communication Stack	LID	External protocol handling	—	Requires HID validation

FRs enforced in TSM are described below in Table 10.

Table 10*: TSM Functional Requirements*

	Functional Requirement	Description
FR-1	Complete Mediation	All firmware updates, remote commands, and actuator-level requests originating from the LID must traverse the HID boundary for validation before execution.
FR-2	Firmware Integrity Enforcement	Only cryptographically authenticated and policy-compliant firmware images are permitted to proceed through the admission process and be authorised for execution.
FR-3	Secure Boot Anchoring	Runtime execution is permitted only when the firmware state has been verified against trusted integrity references during boot initialization.
FR-4	Grid-Command Policy Compliance	All grid-originating or backend-issued commands must be evaluated against predefined stability, safety, and operational constraint policies prior to actuation.
FR-5	Escalation Containment	Compromise within the Low-Integrity Domain must not directly propagate to actuator-level or grid-interactive control layers without High-Integrity Domain authorisation.

3.5.2 TSM Integration with CO-Simulation Platform

The TSM architecture was integrated into a HELICS-based co-simulation federation comprising EVSE, grid, backend, and monitoring federate. The table below presents integration points. Integration inserted the HID mediation layer between federated inputs and EVSE state variables, ensuring deterministic enforcement prior to actuator or power-state propagation.

Table 11*: TSM integration with co-simulation platform*

Integration Layer	Connected Federate	Mediation Mechanism	Controlled State Variable	Enforcement Effect
Firmware Update Channel	Backend Federate	Firmware Admission Manager	Runtime firmware image	Prevents unvalidated execution
Grid Command Channel	Grid Federate	Policy Enforcement Engine	Charging power setpoint	Enforces stability constraints
EVSE Controller Logic	EVSE Federate	TSM Core Monitor	Control state transitions	Mandatory validation before execution
Actuator Interface	Physical EVSE Model	Hardware Controller	Contactor/modulation signals	Blocks unauthorised switching
Telemetry Channel	Monitoring Federate	Log & Integrity Module	Enforcement events	Signed state reporting

This ensures that all HELICS-published signals affecting physical behaviour are intercepted and validated prior to federation-wide propagation.

3.5.3 Architectural Enforcement Properties

The structural validity of the TSM architecture is characterised through mediation, isolation, and containment principles. These properties are embedded in the design to guarantee that no external or low-integrity input can directly influence actuator or grid-interactive behaviour without validation. Enforced properties are summarised in the Table below.

Table 12: *TSM Architectural Enforcement Properties*

Enforcement Property	Description	Implementing Component	Architectural Guarantee
Complete Mediation	All privileged operations pass through HID	TSM Core Monitor	No direct LID-to-actuator path
Domain Isolation	Logical separation between LID and HID	HID boundary controls	LID cannot access secure storage or actuator gating
Firmware Integrity Anchoring	Execution depends on verified firmware	Cryptographic Engine + Secure Boot	Blocks unauthenticated runtime
Command Policy Enforcement	Grid commands are evaluated pre-actuation	Policy Enforcement Engine	Prevents unsafe power modulation
Escalation Containment	Compromise confined within LID	Hardware Interface Controller	Prevents cross-domain amplification

3.6 EVSE Co-simulation Baseline Model Results

This section presents the results obtained from the EVSE co-simulation baseline model developed in Phase II (Co-Simulation Platform Development). The simulations capture realistic configurations of EVSE components, grid dynamics, EV charging behaviour, and their interconnections as defined in the architectural decomposition described earlier. The baseline model establishes the reference operational behaviour against which subsequent supervisory enforcement and adversarial scenarios are evaluated.

Single EVSE with Grid Integration

In this scenario, a single EVSE operates under grid conditions to observe the functional stability and grid dynamics. In this case, it is a reference model to investigate for further complex behaviour and stochastic grid dynamics. The objective in this scenario is to evaluate current and voltage constraints, charging dynamics, adherence to communication protocols, and stable operation in a co-simulation federation environment.

Simulation Configuration

The simulation configuration of a single EVSE supports three connectors with a capacity of 50 kW each, and the power station capacity is 100 kW. Two EVs of nominal battery capacity of 60 kWh each are configured with an initial SoC of 20%. The power grid is modelled with a distribution feeder of 12.47 kV, and the feeder capacity limit is 150 kW. The duration of the simulation is 120 minutes, and a 1-minute interval is used for capturing temporal resolution to observe steady-states and transient responses.

Execution Framework

The simulation EV charging system package and Simulator classes are used for the concurrent operations of EVs, EVSE, and power grid feeders. To capture real-time results, the dashboard launches with *Enhanced Messages Server* for the visualization of execution events, communication interactions, and operational constraints. The communication protocols enable interactions among EVs, EVSE, and the power grid. The logging metrics record telemetry exchanges, event traces, operational control, and performance metrics in the runtime of the simulation.

The single EVSE is integrated with the IEEE 13-bus distribution system through the HELICS co-simulation framework. figure 21 illustrates the grid integration architecture, where the EVSE federate interfaces with the power distribution network through OpenDSS, exchanging real-time

power flow data, voltage measurements, and control signals. The EVSE operates as a controlled load on the distribution feeder, with bidirectional communication enabling dynamic power management and grid stability control. The integration ensures compliance with grid constraints, including voltage limits (±5% of nominal), feeder capacity (150 kW), and power quality standards.

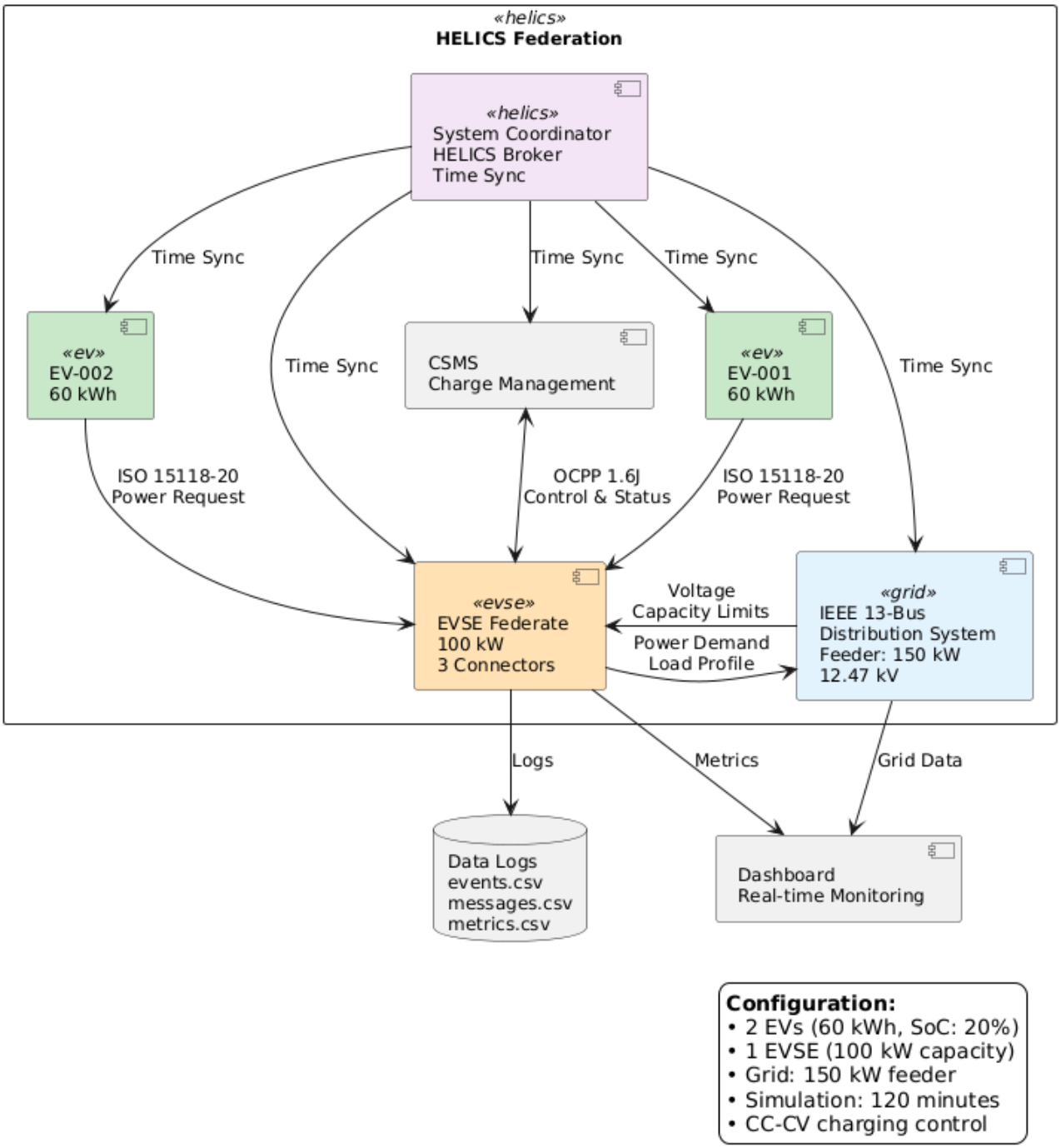


Figure 21*: Grid integration architecture for single EVSE showing HELICS federation, OpenDSS power flow interface, and bidirectional communication pathways.*

3.6.1 **Performance Evaluation**

Once the simulation execution is complete, three datasets are generated, such as events.csv, messages.csv, and metrics.csv. The datasets capture logs of communication events, EV charging dynamics, and aggregated power system profiles. The results show that the stable operation of EV charging according to the power grid capacity of 150 kW. Figure 22 shows EV load profiles, power utilization, and load behaviour according to the grid feeder dynamics and control limits. The power utilization is calculated as follows: The grid utilization factor, computed as:

$$P_{feeder} = \frac{P_{sys}(t)}{P_{\lim it}} \times 100 \quad (2)$$

To keep the operational stability of the power grid, the utilization factor must be kept under 80% in the entire simulation process to keep reserve margins and safe limits. To capture long-term demand patterns and short-term oscillations, a rolling window of 10 minutes is applied in the simulation process.

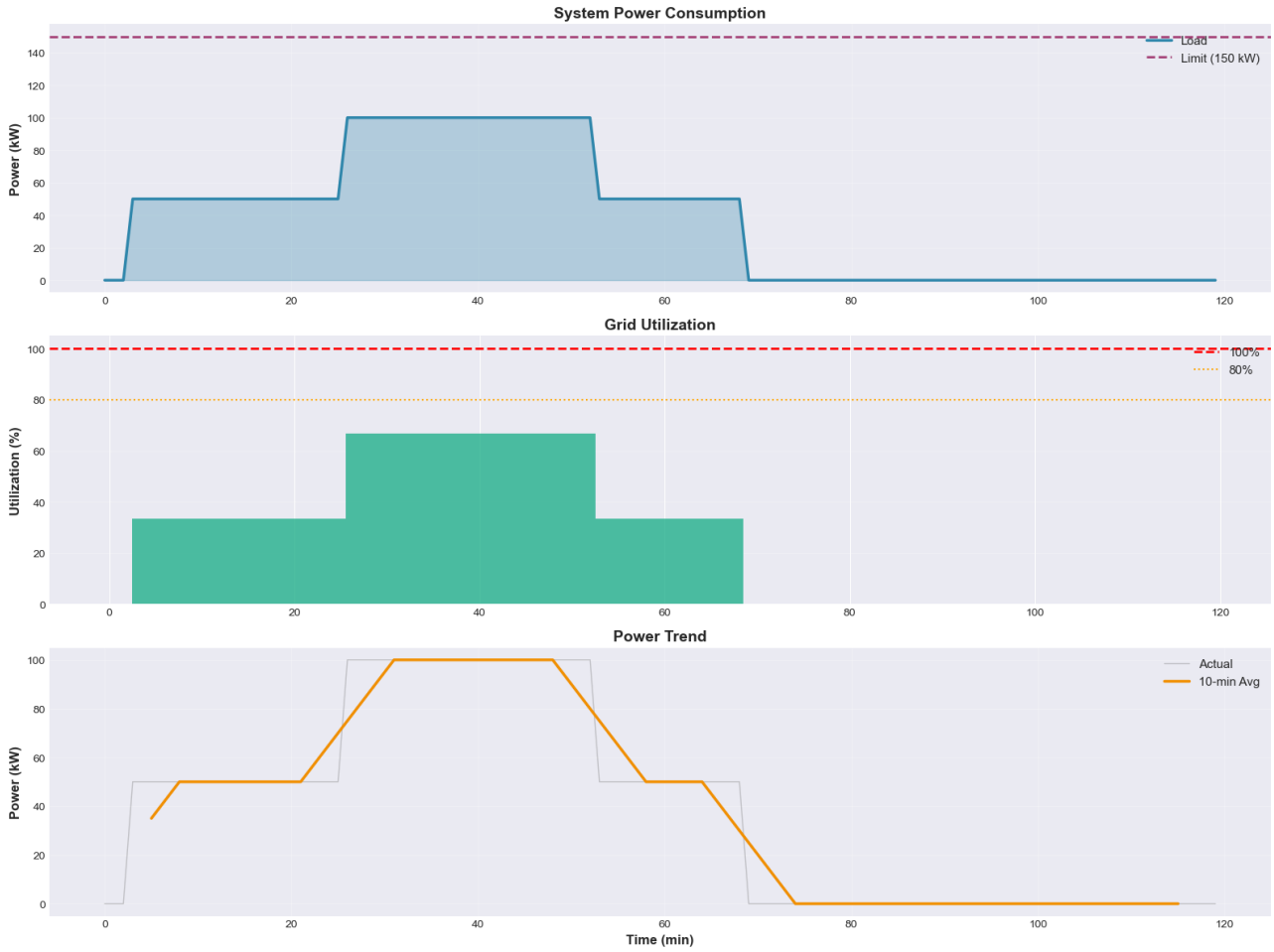


Figure 22*: Top panel shows total system power demand over time. Bottom panel displays grid utilization factor (percentage of feeder capacity) demonstrating stable operation below 80% threshold, with shaded regions indicating charging phases and reserve margins.*

3.6.2 EV Charging Dynamics

The EV charging behaviour is analysed with active sessions and the number of EV charging sessions. Every EV follows the design charging progression, charging dynamics, power grid control limits, and power tapering. The energy delivered and SoC computation are estimated as follows:

$$E_i = \left(\mathrm{SoC}_{i,\mathrm{final}} - \mathrm{SoC}_{i,\mathrm{initial}}\right) \times C_{\mathrm{ev}} \qquad (3)$$

Where the EV battery capacity is represented with $C_{\mathrm{ev}} = 60{\sim}kWh$, $\mathrm{SoC}_{i,\mathrm{initial}}$ is initial SoC of EVs while $\mathrm{SoC}_{i,\mathrm{final}}$ is final SoC of the EVs. Figure 3 illustrates active sessions of EVs and instantaneous EV charging. The results confirm that EV charging profiles do not violate power grid level constraints and charging station control limits. The EV charging dynamics demonstrate coordinated control and power tapering mechanisms. Figure 23 presents two key aspects:

1. The active charging sessions timeline showing when each EV is connected and drawing power.
2. The instantaneous charging power profiles for both EVs.

The power profiles exhibit the expected CC-CV (constant current-constant voltage) charging behavior, with initial constant current phase at maximum power, followed by voltage-limited tapering as the battery approaches full charge. The coordination ensures that aggregate power demand remains within grid and EVSE capacity limits while maximizing charging efficiency.

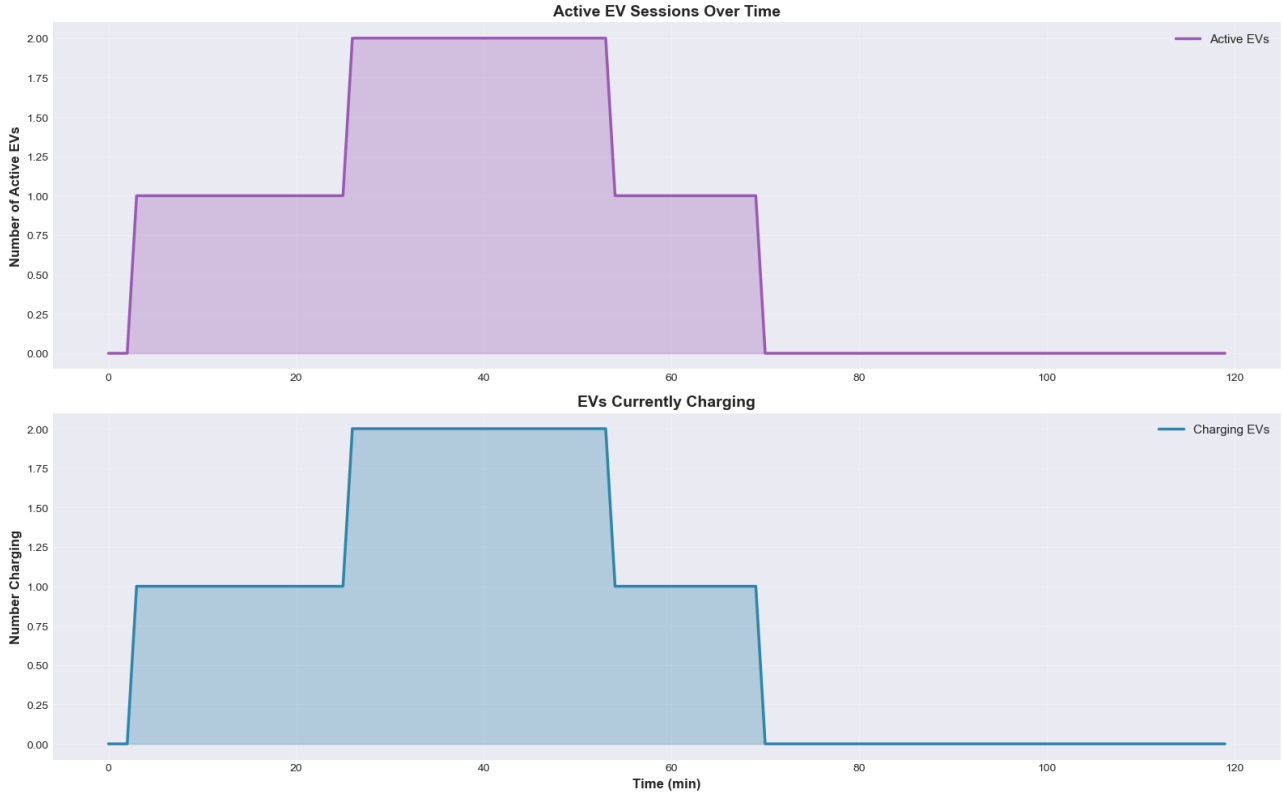


Figure 23*: The charging dynamics of two EVs and their control trajectories in a single EVSE scenario*

Figure 24 reflects the energy consumption profile evaluated for the EVSE and power grid, estimating both individual EV charging energy and total system energy consumption. In case of total system energy, it captures the cumulative energy streams from SYSTEM federates in which the energy delivered to the EVSE federate is computed. The results illustrate an exponential increase at the initial state due to the SoC constraints and charging demand. The shaded region reflects a progressive increase of energy transfer due to ramp-up profile, steady-state charging patterns, and power tapering for full charge of EVs. It provides a significant inductor to capture grid utilizations, considering EVSE operational limits, feeder capacities, demand response, and total energy throughputs.

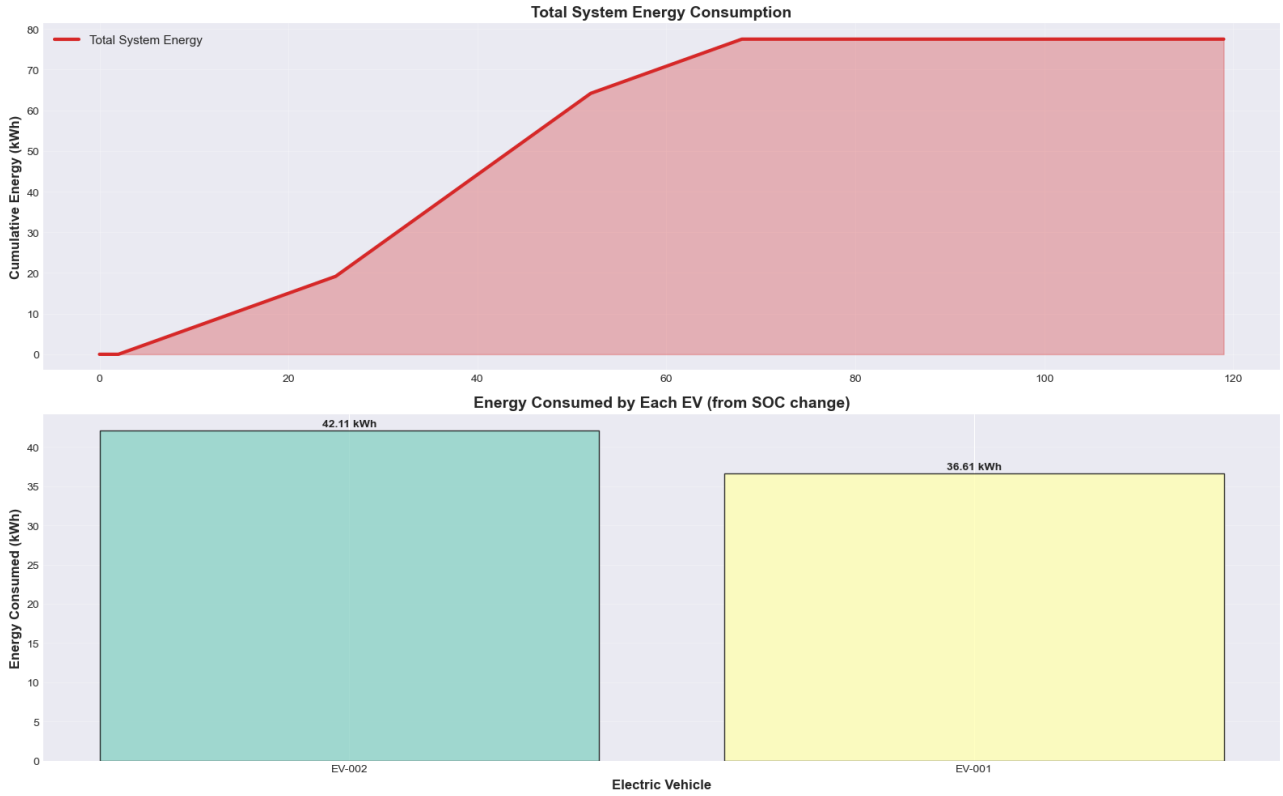


Figure 24*: The total energy consumption of the system and individual EVs in a single EVSE scenario.*

The lower part of figure 4 evaluates energy consumption of individual EVs, estimated from differential SoC and nominal capacity of EVs. This estimates the exact energy drawn in the single EVSE scenario and presents it in bar graphs. The individual EV presents its energy drawn from its active sessions of the charging system. The energy consumption accumulates energy allocation, prioritization of EV charging, uneven charging behaviour, and power grid impacts. In addition, it allows granular and aggregate charging performance to assess scalability, charging fairness, and EVSE efficiency for peak demand and normal operational scenarios.

3.6.3 Communication Interactions

For the single EVSE with grid-connected operation, the communication layer handles control messages of OCPP 1.6J and ISO 15118-20, capturing telemetry statistics and information exchange

during this scenario. The synchronization between federates is still deterministic, with no loss of control data and packets. Starting from the communication handshake, request-response, authentication, and connection establishment, approximately 44 messages are exchanged in this scenario, capturing 36 messages of OCPP 1.6J and 8 messages of ISO 15118-20. The type of messages includes heartbeats, session setup requests, session setup responses, start transactions, start transaction responses, and stop transactions. Figure 25 illustrates the statistics of the communication logs, confirming charging session and EVSE transition Idle → Charge → Complete in the simulation.

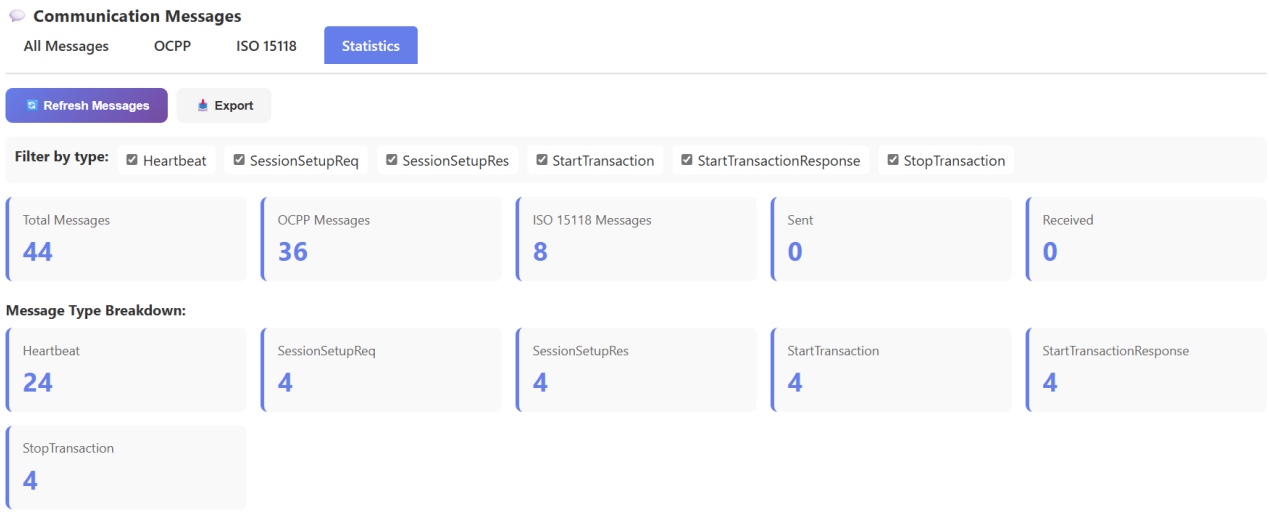


Figure 25*: The communication protocols, statistics, and message exchange in the single EVSE scenario.*

In conclusion, the scenario of single EVSE grid integration validates the baseline be- haviour, cyber-physical control dynamics, communication interactions, and operational stability. The testing scenario confirms compliance with EVSE envelope behaviour, EV modelling, operational limits, power grid dynamics, and synchronization across HELICS-enabled federates. The generated datasets provide a benchmark and foundation for fleet-level complex scenarios where control dynamics and power grid impacts are more challenging. Moreover, it provides a reference for the communication message exchange in complex scenarios and its evaluation for in-depth analysis.

3.6.4 EVSE Fleet with Grid Integration

In the second scenario, the EVSE fleet with grid integration is analysed in the co-simulation environment, in which different extreme test cases are demonstrated. Under high-demand conditions, it provides stability evaluation, scalability assessment, and end-to-end resiliency control for EVSE fleet to grid integration. It extends foundational baseline behaviour discussed in scenario one, considering real-time EVSE and grid dynamics such as grid overloading, charging station concurrency, battery thermal challenges, complications in communication networks, and EVSE system scalability heatmaps.

In this scenario, EVSE federates operate with unique operational behaviour and random starting time for charging to exercise realistic behaviour of the fleet's operation. In the EVSE fleet analysis, the coordination and congestion control under the HELICS environment were also examined for

real-time synchronization, interactions, and communication resiliency. In addition, the provision of quantitative insights for high-demand conditions, grid control behaviour, performance degradation trends, and scalability limits is also investigated. Furthermore, the robustness of the cyber-physical simulation environment is evaluated on a scale to assess the operational control limits, its cyber resiliency, and scalability in complex EVSE and grid interaction scenarios.

3.6.5 Simulation Configuration

For the EVSE fleet configurations, there are ten EVSE fleets (EVSE 1–EVSE 10), having multiple connectors to entertain EV charging sessions simultaneously. There are numerous EVs with different battery capacities starting from 40 kWh to 80 kWh that are initialize having random SoC ranging from 10% and 40%. The aggregate feeder capacity is set to 600 kW while the capacity of each EVSE unit is configured with 100 kW. The simulation time spans from 180 minutes and is adjusted dynamically, capturing temporal results after every minute in the simulation runtime. It captures steady-state and transient dynamics of the EVSE fleet with grid integration. To replicate uncertainty at a large-scale EVSE fleet, temperature derating effects, voltage instabilities, and communication latencies are randomly injected in the simulation runtime. In the HELICS environment, the EVs, EVSEs, grid, and other federates are orchestrated and synchronized in the co-simulation setup. The global simulation run file executes and generates manifest files to record EVSE charging dynamics and events. The telemetry of EVSE fleet performance is logged with CSV datasets such as communication throughput, active power, currents, and voltage control.

The EVSE fleet integration extends the single-EVSE architecture to a distributed multi-point configuration. Figure 26 illustrates how ten EVSE stations are distributed across the IEEE 13-bus feeder, with each station connected to different buses to evaluate load distribution, voltage profiles, and aggregate power demand. The HELICS federation coordinates all EVSE federates, EV actors, and the grid model, ensuring time-synchronized operation and communication protocol adherence. This distributed architecture enables evaluation of fleet-level impacts on grid stability, voltage regulation, and feeder loading under high-demand scenarios.

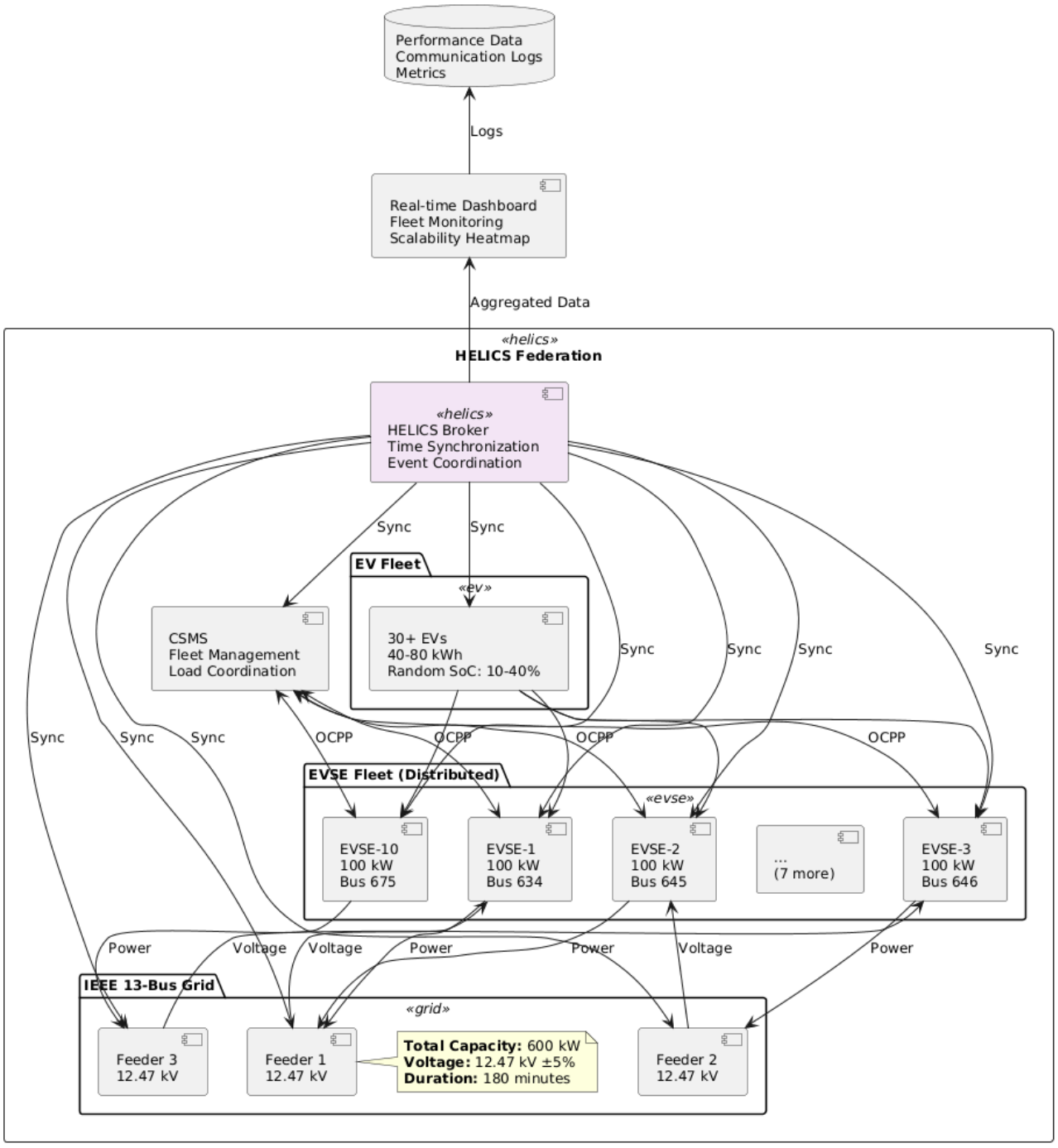


Figure 26*: EVSE fleet grid integration architecture showing distributed deployment across IEEE 13-bus system, HELICS federation coordination, and aggregate load management.*

There are five test scenarios developed for the stability and robustness of the EVSE fleet and grid integration, enabling overall system control and adaptive control logic. The details of five test scenarios in the EVSE fleet with grid integration are provided in the following sections.

3.6.6 Grid Overload Analysis

In the Grid Overload Scenario test, the power grid response is evaluated for the EVSE fleet, considering simultaneous EVs charging demand at EVSEs and high charging demands. The EVs are randomly connected with EVSE fleets across distributed power grid feeders 12.47 kV of the grid limit

800 kW for each EVSE unit. The charging profiles in the EVSE units are initiated simultaneously for the demonstration of a sudden load increase on the distribution grid. The performance metrics for system-level total power kw capture quantified power drawn, power utilization, overload detections, and power grid violations with $P_{sys}(t) > P_{limit}$. Figure 27 illustrates grid overload analysis, including grid capacity, system limits, power grid violations, power grid utilization, and overload detections.

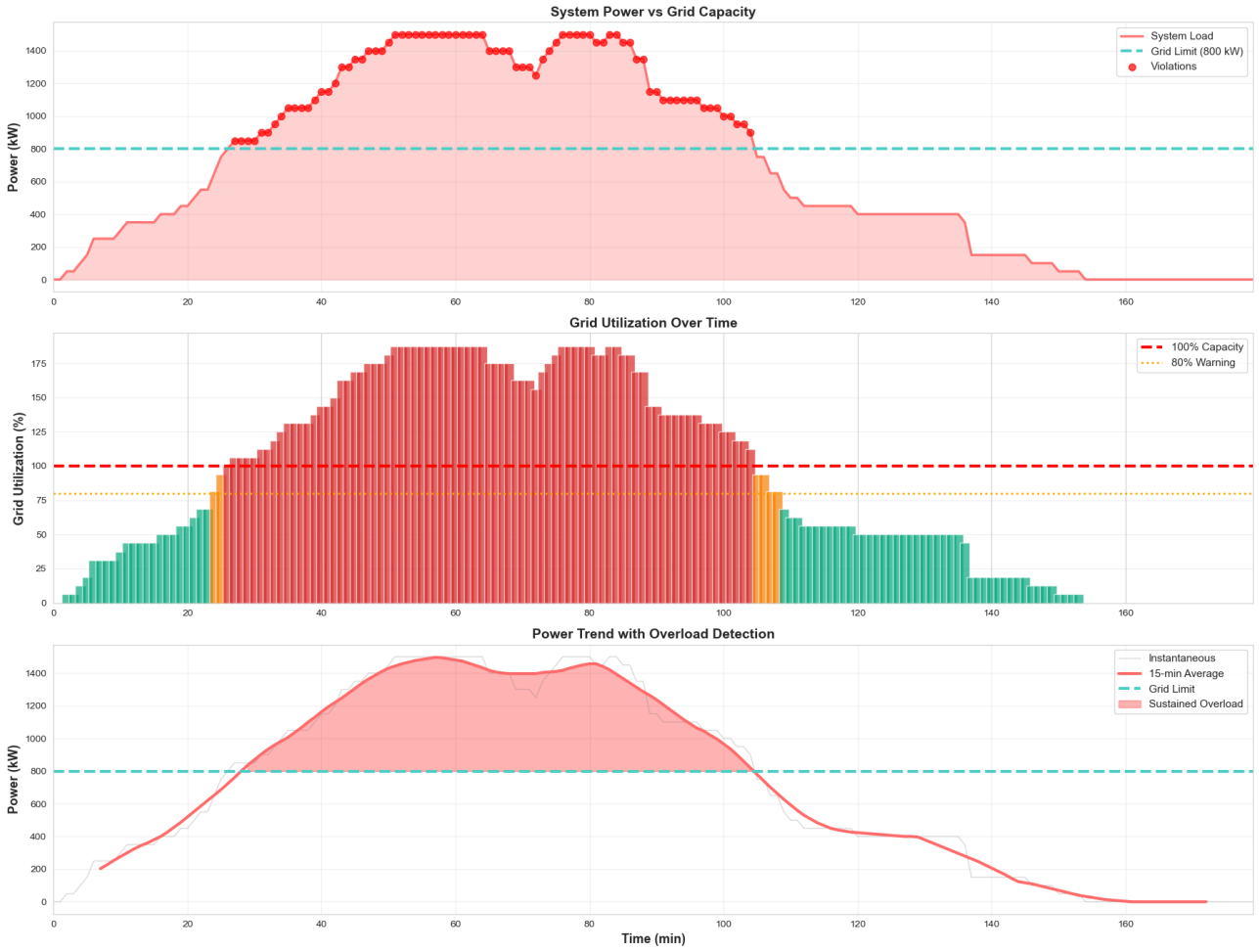


Figure 27*: Estimating power grid capacity, grid utilization, and grid overload detection in the EVSE fleet scenario.*

The grid capacity and system load are evaluated initially to trace real-time power traces, system demands, and grid violations for the runtime simulation window. The initial results reflect the successful detection of system load violations for the specified distribution power feeder capacity. It is also estimated that the aggregated charging demands so that the power dispatch would be adjusted accordingly. In the second result, the distribution power grid utilization factor is estimated. The baseline threshold of power grid utilization is configured at 80% for the stable operation and control stability, enabling accurate estimation of feeder overload during real-time surge of EVSE unit demands.

The results indicate power grid experiences a transient overload capacity of approximately 1500 kW beyond its limit of 800 kW. The average load records 662.72 kW, representing 58.20% power grid utilization and feeder loading, while the grid violations are 41.80% of consecutive 75 occurrences

during runtime simulations. The maximum overload capacity is recorded as 700 kW in the peak demand conditions, estimating 41.80% grid capacity violation. The accurate estimation of overload conditions enables optimal dispatch conditions, capturing extreme events for adaptive control logics, and supports us in mitigating EVSE tapering phases. It reflects the co-simulation environment for grid overload conditions, effectively captures real-time high-demand conditions for the EVSE fleet. These finding enables adaptive control strategies for entertaining EVSE fleets and coordinate charging mechanisms for managing peak loads in large-scale EVSE fleets connected with power distribution systems.

3.6.7 **Charging Station Concurrency**

In the Charging Station Concurrency test, the EVSE fleet and grid capacity are assessed for handling real-time charging operations. It quantifies concurrent charging loads, concurrent utilization of charging station capacity, EVs distribution across the charging stations, and EV charging sessions. The test demonstrates numerous charging stations, configured with EV connectors, to estimate charging capacity $\mathrm{N_{total}} = N_{\mathrm{stations}} \times N_{\mathrm{connectors}}$. The performance metrics of charging station concurrency are monitored with number of charging and active EVs, enabling further insights for the detailed analysis of charging station utilization and real-time charging sessions. The concurrent charging stations visualize EVSE fleet behaviour, evolving in the runtime, and capture the maximum load condition in the saturation period of power demands.

The results in figure 28 demonstrate EVSE fleet stability achieves operational stability near saturation, facilitating maximum charging sessions in the peak demand, supporting 95–98% connector availability for EV charging. It is obvious from the active charging sessions that maximum EVs serve to manage concurrent charging load at the EVSE fleet during the peak demand situations. For station capacity utilization, the maximum number of connectors facilitates EV charging to meet the charging station capacity in a normal distribution pattern. It reflects an average 85% connector utilization to maintain optimal usage of station capacity. For single charging station evaluation, the performance metrics (EV ARRIVED) capture optimal load balancing, enabling EVSE fleet stability and power grid capacity. The 80% stations load balance EV charging sessions while the remaining 20% facilitates EVs in the stochastic control scenarios. Despite a random arrival profile of EVs, the concurrent charging stations enable synchronization, queue management, connector assignment, and control interactions between EVs, EVSEs, charging stations, and power grid federates. The quantification of these findings confirms *Charging Station Concurrency robustness*, enabling coordinated charging connectivity, optimization of EV charging profiles, connector allocations, adaptive queue control, and optimal utilization of charging station capacity.

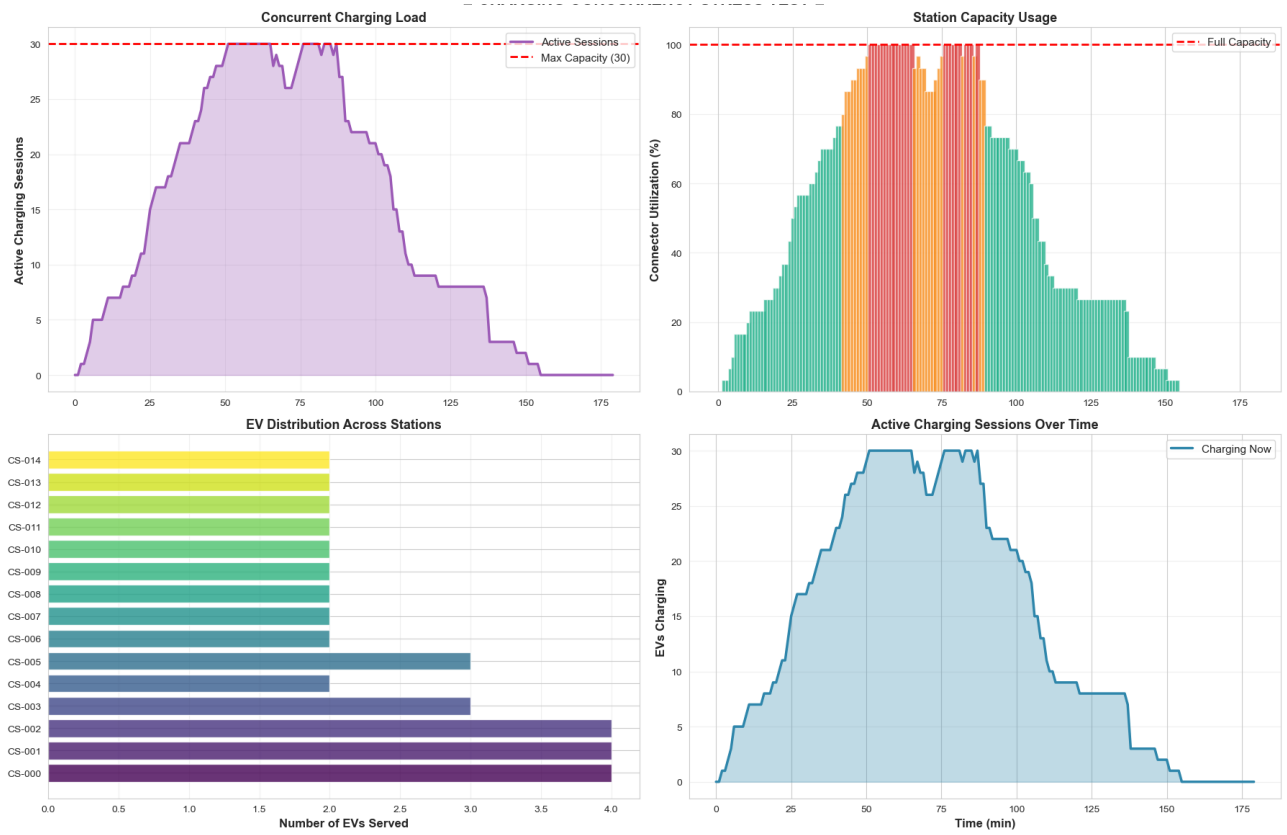


Figure 28*: Charging station concurrency estimation for charging loads, station capacity, EV distribution in the charging stations, and active sessions of EVs in the EVSE fleet scenario.*

3.6.8 Battery Thermal Management

In the test scenario of Battery Thermal Management, the EV batteries' temperature at the EVSE fleet is evaluated under high load charging dynamics. It reflects the temperature sensitivity across EV batteries for critical and average limits in the battery charging cycles. The temperature metrics enable EV batteries' instantaneous temperature and overall temperature in the EVSE fleets. The normal range of temperature during EV battery charging is between 59–86°C and varies upon SoC dynamics. The warning temperature ranges from 86–90°C, enabling battery management control to observe the controller and battery dynamics for safe charging and operation. The critical temperature limit is beyond 95°C, reducing the charging performance and posing potential risks in the routine charging of EVs.

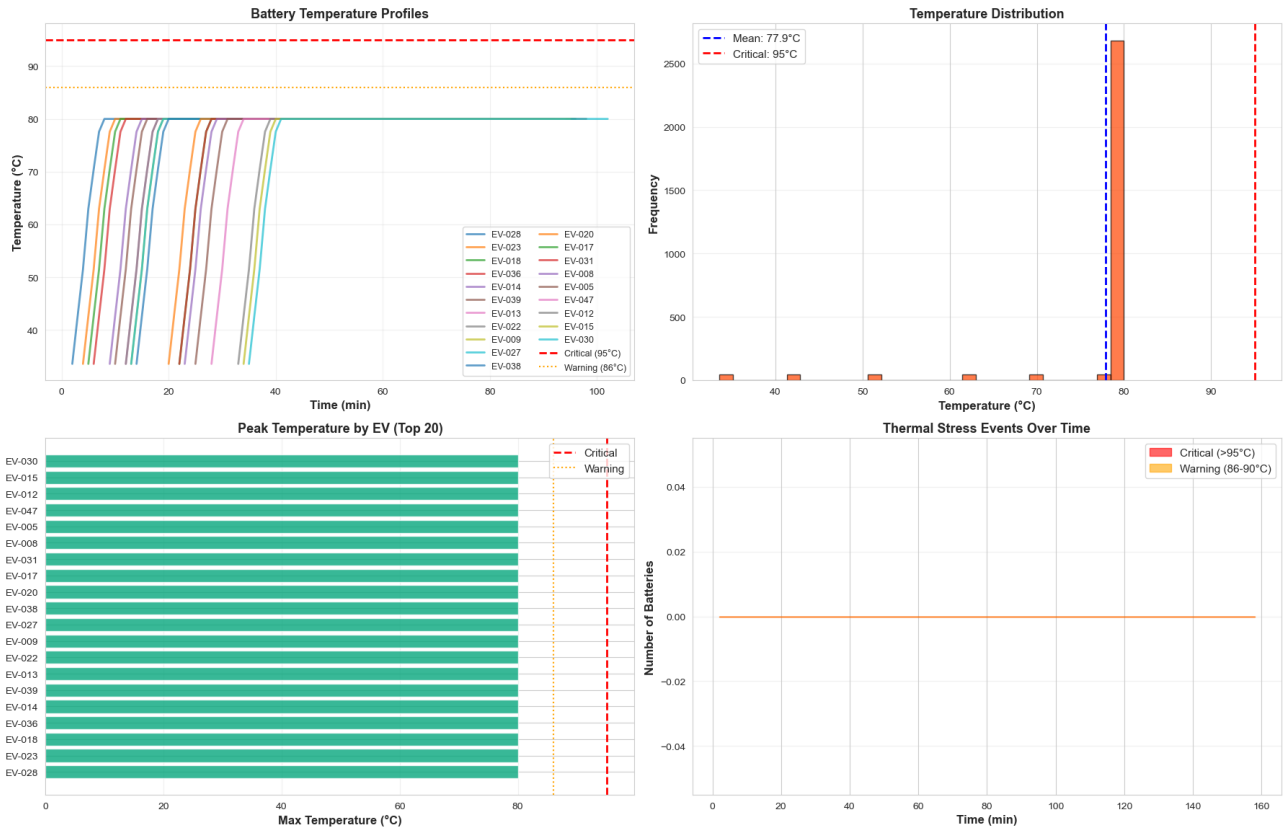


Figure 29*: Battery thermal management for estimating individual EV battery temperature, the frequency of temperature limit, peak temperature of EVs during charging, and temperature distribution in the span of EV charging in the EVSE fleet scenario.*

The results in figure 29 reflect the EVSE fleet for thermal management, enabling battery temperature of EVs under the desired limit to keep safe and operational stability. In battery temperature profile management, ten EVs are randomly selected to evaluate thermal distribution during peak demand of the EVSE fleet. It is observed that most of EVs' charging operates in the safe limit, enabling the robustness of EVSE fleets to handle thermal management risks. In the temperature distribution profile, the highest frequency of most EVs is 80°C as the charging process progresses, while some of the EVs operated under 80°C due to their battery dynamics and initial SoC states. In the peak temperature case, twenty EVs are randomly selected with different SoCs and their overall temperature. It is observed that EVSE fleet dynamic charging profiles and queue management keep the temperature limit in the normal range. For the thermal stress events, the EV battery temperatures rise initially due to charging dynamics and SoC status. Once the charging mechanism is coordinated in the EVSE fleets, the battery temperature becomes balanced and avoids warning and critical limits. These finding of the thermal management indicates temperature-enabled load dispatching algorithms and adaptive charging scheduling without a cooldown interval in the peak demand in the EVSE fleets scenarios.

3.6.9 **Communication Network Analysis**

This test evaluates the performance of Communication Network Analysis, focusing on communication resiliency for latency characteristics, protocol distribution, and message traffic under extreme network load. The key aspects in the communication network are communication message rates, protocol distribution for communication interactions, message latency distribution,

and types of messages exchanged in the EVSE fleets' communications. For evaluating communication messaging rates, substantial variation is observed over time due to high load intervals of EV charging in the EVSE fleets, as reflected in figure 30. The highest message rate records as **77 messages per minute** in the peak demand load as compared to average **13 messages per minute** in normal charging situations. The message rate is even higher for distinct EVSE-grid security events due to synchronization updates, communication handshakes, and event-driven updates. In the protocol distribution case, the exchange of communication messages is purpose-driven, suggesting maximum utilization of OCCP protocols over ISO 15118-20. From EVSE to CSMS and other entities, OCPP interactions exchange communication messages **85.4% OCPP** while ISO 15118-20 exchange **14.6% ISO 15118-20**. It demonstrates EVSE edge and central control are fully equipped with communication control interactions, ensuring efficient synchronization and telemetry in large-scale EVSE fleet networks.

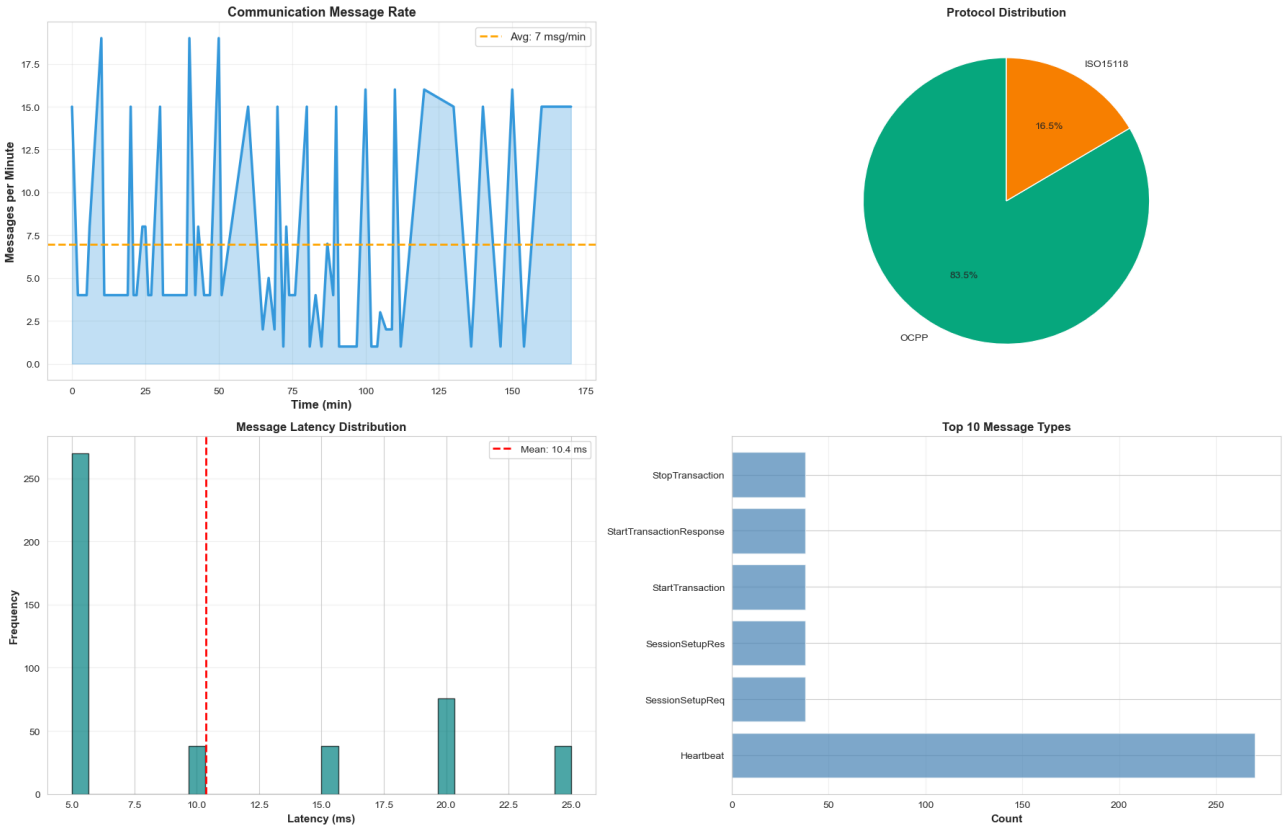


Figure 30*: Communication protocol analysis for estimating rate of communication messages, utilization of protocols, latency of communication messages, and frequency of popular control interactions in the EVSE fleet charging scenario.*

To evaluate the frequency of message latency distribution for real-time communication, the maximum latency **25 ms** is recorded during peak load demand, while average latency is **9.7 ms** for routine communication. The smallest latency is recoded as **5 ms** for the frequency of 1265 messages of OCPP and ISO 15118-20. It shows the communication resiliency of EVSE fleets during traffic bursts and the successful delivery of packets in the end-to-end communication interactions. In addition, it ensures QoS and network stability with minimum latency for frequent control interactions, adhering to real-time communication for EVSE fleets and the grid. For analysing different types of messages

in the peak load of EVSE fleets, the frequency of handshake messages and heartbeat is **60%** higher than others due to constant engagement during the entire simulation process. It emphasises concurrency of data transactions and system resiliency to demonstrate net- work robustness with the lowest communication delay **5 ms** under maximum network loading conditions. These findings validate EVSE fleet capabilities to handle complex and large-scale communication networks for more frequent communication control interactions.

3.6.10 System Scalability Heatmap

The EVSE fleet scalability test assesses concurrent EV charging sessions on the EVSE fleet and system response to handle them. Refer to figure 31, there are two heatmaps to generate charging power and SoC for concurrent charging of thirty EVs. For the charging power heatmap, the EV charging demands dynamically distribute across the EVSE fleets during peak load intervals. The horizontal line with the highest density reveals coordinated EV charging sessions and energy transfer, and the low power zone indicates completion of charging cycles for the top thirty EVs. The transition between the lowest and highest charging intensities indicates the optimal scheduling and EVSE control robustness to handle EV clusters without compromising on communication and control interactions. Furthermore, the shift from red to orange and then green suggests fast coordinated charging activities, fair load distribution, and scalable EVSE fleet management.

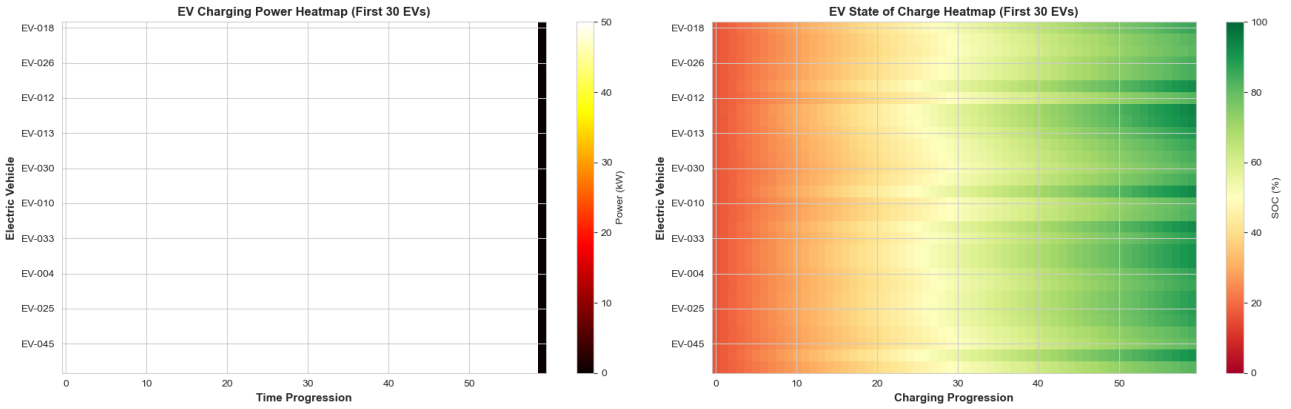


Figure 31*: System scalability heatmap for power and SoC of EV charging in the EVSE fleet charging scenario.*

In the SoC heatmap, the monotonic increase of smooth EV charging complements energy management efficiency, enabling consistent charging schedules and coordinated control operations. During the time progression, the EV charging shifts from low SoC to moderate SoC and then high SoC as the simulation advances. It achieves full charging of EVs within the simulation time frame through adaptive charging behaviour and optimal schedule management. Some variations are observed in these transitions due to the priority charging mechanism of EV federates in real-time grid conditions. The deterministic control of EVSE scalability is maintained in a progressive pattern for charging the initial thirty EVs, enabling predictable energy delivery and optimal scheduling on large-scale EVSE fleet deployments. In both heatmaps, the scalability of the EVSE fleet demonstrates how co-simulation architecture handles concurrent EV charging operations,

considering communication delays, adaptive scheduling, and coordinated control on large-scale EVSE fleet deployment with power distribution systems.

3.6.11 Performance Metrics and Observations

In both scenarios of EVSE and grid integration, the performance metrics and potential observations are as follows:

- Real-time control of power grid stability and safe EV charging systems.
- The delivery of actual charging power and its accurate estimation in real-time sessions.
- Communication network resiliency by managing time synchronization, messaging rates, network latencies, and interaction throughputs efficiently.
- Battery thermal management for estimating charging rates and derating limits for improving battery health and performance.
- Computational resource utilization for the cyber-physical co-simulation to scale up EVSE across numerous federates.

3.6.12 Summary

Overall, the results in single EVSE and EVSE fleets with grid integration exhibit robust resiliency across communication protocols, battery thermal management, and physical characteristics of EV infrastructure. Furthermore, the modularity of the distributed control federation environment significantly improves for handling communication disturbances, grid overload conditions, real-time grid stabilization, and adaptive EV charging management. Numerous tests in both scenarios confirm operational stability regardless of communication impairments, battery thermal variations, concurrency peaks in charging stations, and efficient management of grid overload conditions. The results confirm the robust design of the EV ecosystem baseline behaviour model in terms of scalability, operational stability, communication resiliency, and fault tolerance, enabling its suitability for the extension into the TSM functional model integration in the later stages.

3.7 TSM Implementation and Experimentation Results

This section provides implementation-specific details of TSM. It first describes deployment architecture, followed by integration with the co-simulation platform, experimental results, and TSM validation.

3.7.1 Deployment Architecture

It provides the deployment of TSM design in the EVSE co-simulation environment, enabling TSM to have a concrete, executable, and multi-dimensional architecture that mediates all EVSE components during critical operations. The co-simulation deployment architecture should follow these characteristics:

1. The TSM security pipeline works as a mediator for controlling all components and security-critical operations. TSM should not bypass within the EVSE control architecture and should be explicitly integrated with the baseline co-simulation model.
2. The EVSE co-simulation system must produce multi-layer telemetry and control information required to evaluate the co-simulation framework operation.
3. The EVSE co-simulation platform must be reproducible to enable results verification independently.

The deployment goals are categorized into five streams:

1. **Complete runtime mediation:** The PEE intercepts each required from LID to HID during design and execution time. For example, safety-critical configurations for hardware actuators, changing contactor states, and updating firmware must pass through PEE policies.
2. **Deterministic and reproducible traces:** For the identical scenario inputs and configurations, the co-simulation framework produces similar traces for evaluation among three layers: Cybersecurity control layer, EVSE behaviour layer, and power grid impact layer.
3. **Structured threat injection:** For the implementation of use cases, the use case engine injects protocol anomaly attacks, power disturbances, tamper events, and firmware attacks without modification of the core simulation platform to preserve the threat injector and core simulation framework separation.
4. **Real-time observability:** For real-time observability, all co-simulation states, including power flow, battery dynamics, protocol interactions, and TSM decisions, are observed through the dashboard to demonstrate real-time interaction and evaluation.
5. **Comparative evaluation:** The comparative evaluation is made with TSM-enabled and without TSM modes to enable the comparison of the control operation for hypotheses H1-H4.

There are four design principles of the deployment architecture:

1. Layered separation: There are explicitly distinct layers with specific interfaces, such as the TSM security layer, protocol stack layer, physical layer, simulation engine, API, and presentation layer. Each layer is communicated upward and downward for the control functions and event propagation.
2. Event-driven architecture: The architecture is event-driven, in which system state changes are propagated over a central event bus. The system uses subscribers such as metrics collections, logging, and dashboard entries asynchronously and observes the EVSE system behaviour.
3. Fail-secure by default: In case of failure due to TSM policies, the system shifts to a safe state. The PEE policies by default DENY any error according to TSM-FUN-301 policies.
4. Single source of truth: The co-simulation system is state-owned with a simulation engine, while the REST API and dashboard provide states projections by triggering scenarios and do not mutate system states.

The platform deployment must require the following prerequisites:

- Python 3.11 recommended or higher than 3.8 required for the EVSE co-simulation environment.
- Python packages: fastapi, uvicorn, numpy, pandas, scipy, networkx, cryptography, ocpp, pyyaml for developing core simulation.

- Frontend packages: react 18, react-router-dom, chart.js, tailwindcss, vite 5 for designing interactive dashboard.
- Power Systems: GridLab-D and OpenDSS for charging session dynamics and power system distribution studies, running IEEE test cases for power flow analysis using the HELICS coordinator to operate within a federated co-simulation environment and coordinate with external tools.

The FastAPI application, along with Uvicorn, is used to implement the backend server running on port 8000. The entry point for the backend server is ev_charging_system.dashboard.dev_server. The API endpoints are summarized in Table 13.

Table 13*: The group categorization and summarization of REST API endpoints.*

Prefixes	Purpose	Endpoints
/api/components/*	State retrieval and component discovery	GET /evs, GET /stations, GET /grid, GET /tsm
/api/simulate/*	Simulation control and operation	POST /connect-ev, POST /start-charging/{ev id}, POST /reboot
/api/tsm/*	Grid metrics, validations, and use case scenarios	GET /status, POST /toggle, GET /latency-timeseries
/api/grid/*	Grid metrics, validations, and use case scenarios	GET /metrics, GET /history, POST /use-case/v2g-discharge
/api/audit/*	Exporting and auditing of log retrievals	GET /log, GET /export/csv
/api/verification/*	Test results and formal verifications	GET /results, POST /run
/api/performance/*	Overhead benchmarks for TSM	GET /benchmarks, POST /run-benchmark

The endpoints are returned as structured JSON format. The simulation operation, such as scenario triggers, TSM toggling, and simulation control, produces a stream of events to synchronize with the backend server and reflect on the dashboard in real-time. The frontend development is configured through *cross-origin resource sharing* to access the API using port 5173.

For real-time communication between the backend and the dashboard, server-sent events (SSE) serve as the primary channel, and *SSEManager* maintains a collection of connected client queues to broadcast events to the corresponding subscribers. The five primary event types are:

- Events: Includes all event notifications such as TSM transitions, system states, scenario triggers, and component state changes.
- Telemetry: It provides the telemetry updates about grid measurements, station power output, and EV battery states.
- Messages: It provides detail messages of protocols such as OCPP, ISO 15118, IEC~61851, and others having latency, payload, and directions.
- Logs: It records all system logs and highlights severity levels with source components.
- Ping: It keeps alive messaging to ensure the connection stability within co-simulation.

3.7.2 TSM Integration Within the Runtime

During system initialization, TSM is activated before EVCI components are activated. In the runtime simulations, the TSM enforcement direction is as follows:

$$\text{LID Commands} \xrightarrow{\text{intercepted}} \text{PEE} \xrightarrow{\text{evaluation}} \begin{cases} \texttt{ALLOW} \rightarrow \text{HID Actuations} \\ \texttt{DENY} \rightarrow \text{Rejections + Auditing} \\ \texttt{FAIL\_SAFE} \rightarrow \text{Activate Safe State} \end{cases}$$

The classification of PEE requires 21 types and groups them into six categories: session management, attestation/firmware, configuration, power grid, charging, and cryptographic, to assign five levels of TSM security as shown in Table 14. After classification, one of the seven PEE actions is selected: RATE_LIMIT, QUARANTINE, DENY_WITH_ALERT, ALLOW_WITH_MODIFICATION, ALLOW_WITH_AUDIT, DENY, or ALLOW.

Table 14*: TSM PEE policies and classification of security levels.*

Levels	Scope	Default Actions	Requests
PUBLIC	For read only queries	ALLOW	EVSE status and discovery
INTERNAL	For command Operation	ALLOW WITH AUDIT	To start or stop charging
CONFIDENTIAL	For changing configurations	ALLOW WITH AUDIT	To write parameters
CRITICAL	For critical operations	DENY	Contactors and firmware updates
EMERGENCY	For fail-safe	DENY WITH ALERT	To tamper and stop emergency

$$\text{FW}_{\text{accept}} = \bigwedge_{i=1}^{10} V_i(\text{fw}) \qquad (5)$$

The TSM-enabled firmware verification pipeline encompasses sequential steps to formalize and enforce each policy, as reflected in figure 32 and presented in Eq. 5 as follows:

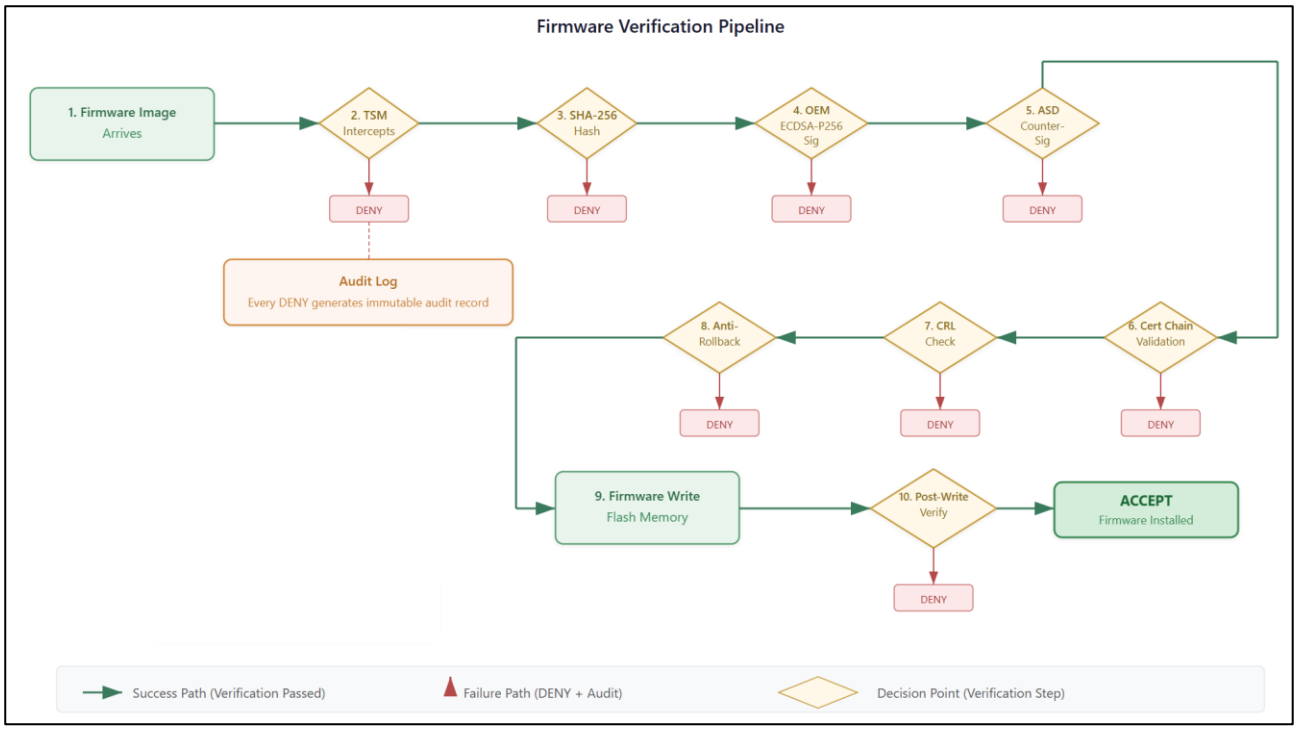


Figure 32*: The formulation of sequential steps for the firmware update verification in the TSM-enabled pipeline*

In case of failure at any Vi step, the TSM pipeline V_j for j > i is not evaluated, and record auditing is initiated. The details of the sequential steps are as follows:

1. Intercepted and entered UPDATING state.
2. HA-256 hash verification with V_2:
3. OEM signature validation with ECDSA-P256 V_3:
4. SD counter signature validation with V_4 :
5. Validate certificate chain with leaf → OEM CA → sovereign root.
6. Checking CRL revocation list.
7. Enforcement of anti-rollback with $v_{new} > v_{installed}$.
8. Writing firmware in bounded critical sections.
9. Re-measurement of post-writing.
10. Restarting by re-validating the secure boot process.

In the event of any step failure, the firmware write operation is denied, an audit log is initiated, and a state transition is triggered, switching to FAIL_SAFE or OPERATIONAL depending on the level of severity.

The TSM operates through six states: BOOTING to verify secure boot, OPERATIONAL for normal validated operation, UPDATING to monitor and verify firmware update progress, FAIL_SAFE to suspend charging and open contactors, ERROR to handle general system errors, and MAINTENANCE for authorized service operations. Experimental validation of the TSM state machine confirms that, under the scenario *invalid_signature*, the system correctly transitions to the FAIL_SAFE state. In contrast, the *valid_firmware_update* scenario proceeds through the update process and returns to

the OPERATIONAL state within the TSM pipeline. The TSM pipeline has five stage trust chain evaluated during initialization re-attestation as follows:

1. Hardware Root of Trust (HRoT) -- Hardware identity, key derivation, HSM, and PUF.
2. Secure Boot -- TSM integrity, LID firmware, firmware hash, bootloader signature, and Boot ROM.
3. Runtime TSM -- Auditing, enforcement, attestation, cryptographic engine, and policy engine.
4. Secure Operations -- Firmware authentication, grid safety, charging sessions, and contactor authentication.
5. External Validation -- Remote attestation, CRL, dual signatures, sovereign certificates, and ASD trust anchors.

3.7.3 Protocol Layer Integration

The deployed architecture implements eight industrial protocols across 28 modules, as summarized in Table 15. Statistical analysis of the protocol communications confirms message exchanges as follows: OCPP 1.6 (6,301 TX / 4,819 RX), CHAdeMO (7,900 TX / 9,516 RX), OCPI (9,844 TX / 4,288 RX), OpenADR (9,367 TX / 3,401 RX), Modbus TCP (6,315 TX / 4,912 RX), IEC 61850 (9,059 TX / 3,833 RX), IEC 61851 (8,463 TX / 2,659 RX), and ISO 15118 (7,433 TX / 6,027 RX).

Table 15*: TSM interceptions and protocol inventories in the protocol layer.*

Protocols	Role in EVCI	TSM Interactions
OCPP 1.6/2.0	For CSMS backend communication	For intercepting firmware update messages
ISO 15118	Plugging, charging and V2G	Crypto engine for certificate validations
IEC 61851	For CP states and PWM signalling	States transition
IEC 61850	GOOSE and MMS	Inform TSM regarding protection events
OpenADR	For demand response	validate DR signals
CHAdeMO	DCFC and V2G	Enforcing power limits
OCPI 2.2	For CPO/eMSP information exchange	Indirect TSM interactions
Modbus TCP	For energy metering	Gated safety registers

The TSM intercepts protocol messages at six key points: the TSM fail-secure logic monitors IEC 61850 GOOSE events; GridSafetyEnvelope processes OpenADR demand response signals; TSM enforces authorization for safety-critical registers in Modbus; TSM policy clearance governs IEC 61851 state transitions (B→C, C→D); the TSM CryptoEngine handles ISO 15118 plugging and charging certificates; and the TSM pipeline verification oversees OCPP commands that trigger UpdateFirmware.

3.7.4 Grid and Power System Model

The power grid is modelled with a base voltage of 12.47 kV, an apparent power rating of 10 MVA, and a nominal frequency of 50 Hz. Test cases are conducted on IEEE 13-bus, 123-bus, and 339-bus networks. The network topology is represented using NetworkX graphs, with the following data structures: Load — power factor and active power; Transformer — tap changer, turns ratio, and kVA rating; Line — capacity and impedance; Bus — operational limits, per-unit values, and voltage levels. The deployment architecture supports two modes of power flow: a high-fidelity mode using OpenDSS and a simplified built-in power flow mode based on IEEE bus networks. Voltage deviation is estimated using Eq. 8, and the voltage drop across buses is calculated using Eq. 9.

$$\Delta \mathcal{V} = \frac{PR + QX}{\mathcal{V}_{\text{nom}}} \tag{8}$$

$$\mathcal{V}_{\text{bus}} = \mathcal{V}_{\text{nom}} - \Delta \mathcal{V} \quad \text{(p.u)} \tag{9}$$

The EVSE inverter computes load and generation balancing for estimating frequency deviation using swing Eq. 10 as follows:

$$\frac{d(\Delta f)}{dt} = \frac{f_{nom}}{2\mathcal{H}\mathcal{S}_{\text{base}}} (\mathcal{P}_{\text{gen}} - \mathcal{P}_{\text{load}}) \tag{10}$$

where H represents the inertial constant and Sbase represents the apparent power, so the RoCof is estimated with Eq. 11:

$$\text{RoCoF} = \frac{d(\Delta f)}{dt} \quad \text{(Hz/s)} \tag{11}$$

The power dynamics include aggregate power, line loading (%), system frequency (Hz), and bus voltages (p.u) is estimated with default OpenDSS power flow solvers. The EVSE fleet load aggregation is computed by adding individual EVSE station load profiles and considering realistic efficiency loss across each station as presented in Eq. 12 as follows:

$$\mathcal{P}_{\text{fleet}}(t) = \sum_{i=1}^{n} \mathcal{P}_i(t) \cdot \eta_i \tag{12}$$

Where instantaneous power is $P_i(t)$ and station i efficiency is $\eta_i = 0.95$. The V2G capability across each station is negative load $P_i(t) \leq 0$ to discharge the EV connected to station i. The overall power grid impact is estimated in the Eq. 13

$$\mathcal{P}_{\text{net}}(t) = \mathcal{P}_{\text{fleet}}(t) + \mathcal{P}_{\text{base\_load}}(t) - \mathcal{P}_{\text{generation}}(t) \tag{13}$$

The safe operating regions are defined in the grid safety envelope (GSE) as presented in Eq. 14 and boundaries are given in Table 16:

$$\mathcal{G} = \left\{ (\mathcal{V}, f, \dot{f}) \;\middle|\; \mathcal{V}_{\min} \leq V \leq \mathcal{V}_{\max},\ f_{\min} \leq f \leq f_{\max},\ |\dot{f}| \leq \text{RoCoF}_{\max} \right\} \tag{14}$$

Table 16*: Grid Safety Envelope parameter bounds.*

Parameters	Symbols	Boundaries	Units
Voltage lower limits	V_{min}	0.940	p.u.
Voltage upper limits	V_{max}	1.060	p.u.
Frequency lower threshold	f_{min}	49.50	Hz
Frequency upper threshold	f_{max}	50.50	Hz
RoCoF absolute limit	$RoCoF_{max}$	1.00	Hz/sec

The composite metrics of the grid stability score (GSS) is estimated in Eq. 15 as follows:

$$\mathrm{GSS} = 100 \times \min\left(\frac{\mathcal{V}_{\max} - |\mathcal{V} - \mathcal{V}_{\mathrm{nom}}|}{\mathcal{V}_{\max} - \mathcal{V}_{\mathrm{nom}}},\ \frac{f_{\max} - |f - f_{\mathrm{nom}}|}{f_{\max} - f_{\mathrm{nom}}},\ 1 - \frac{|\mathrm{RoCoF}|}{\mathrm{RoCoF}_{\max}}\right) \qquad (15)$$

Ideally, a 100 score of GSS indicates that the grid safety envelops operate under normal conditions, linearly degrade GSS score when boundary conditions are changing. The experimental results show grid safety envelop operate withing boundaries for voltage, power, and frequency stabilities due to TSM-enabled enforcement operation.

3.7.5 Runtime Execution Flow

The EVSE system is initializes with ten step sequence: server started → instantiate simulator → Power system model → charging stations → HAL initiated → initialized TSM (HRoT provision, secure boot, PEE engine, Crypto Engine, BOOTING → OPERATIONAL) → protocols handler → events bus → SSE connection established in frontend → LIVE indicator. The scenarios in the co-simulation setup are triggered and executed in the dashboard → Scenario Manager → inject events → tick pipeline initiated → TSM intercepting and evaluating → propagate decisions → grid dynamics updated → SSE streams updated. For recovery paths and failure investigations, there are four patterns:

1. TSM policies violations → open contactors → FAIL SAFE is first option.
2. For firmware verification and update failure → deny and initiate auditing.
3. For GSE violations → open contactors or curtailment initiated.
4. For recovery, the diagnostic initiated → re-attestation evaluated → OPERATIONAL.

The simulation results confirm that operational state restores when tamper injection is triggered, and TSM enforces fail safe using force operational policies.

To ensure consistent configuration and reproducibility of results, the main configuration file, config/config.yaml, defines the primary configuration settings. It includes grid performance data, IEEE bus network models, nominal frequency, and distribution voltage profiles; station performance parameters such as efficiency and rated capacity; communication protocols including ISO 15118 and OCPP 1.6; and relevant optimization flags.

The scenarios consist of sequences of time-constrained actions, with defined preconditions and evaluation criteria. They specify what inputs or events need to be injected into the co-simulation and what responses are expected from the TSM pipeline and trust chain.

To ensure reproducibility guarantee, the deterministic execution provides audit logs export CSVs, complete data export in JSON format, seeded randomness, and real-time clock synchronization for real timestamps. In addition, it provides JSONL metrics data for offline analysis and post-simulation evaluation.

3.7.6 Scenario Manager and Threat Injector

The threat injection capabilities are provided by the scenario manager to evaluate the TSM enforcement policies under realistic conditions. In this section, scenario definitions, threat injections, workflow execution in the dashboard, and TSM-enabled and bypass modes are discussed. The scenario framework supports twenty-three scenarios across different categories. The categorization of these scenarios is presented in Table 17 and the scenario execution framework is illustrated in figure 33.

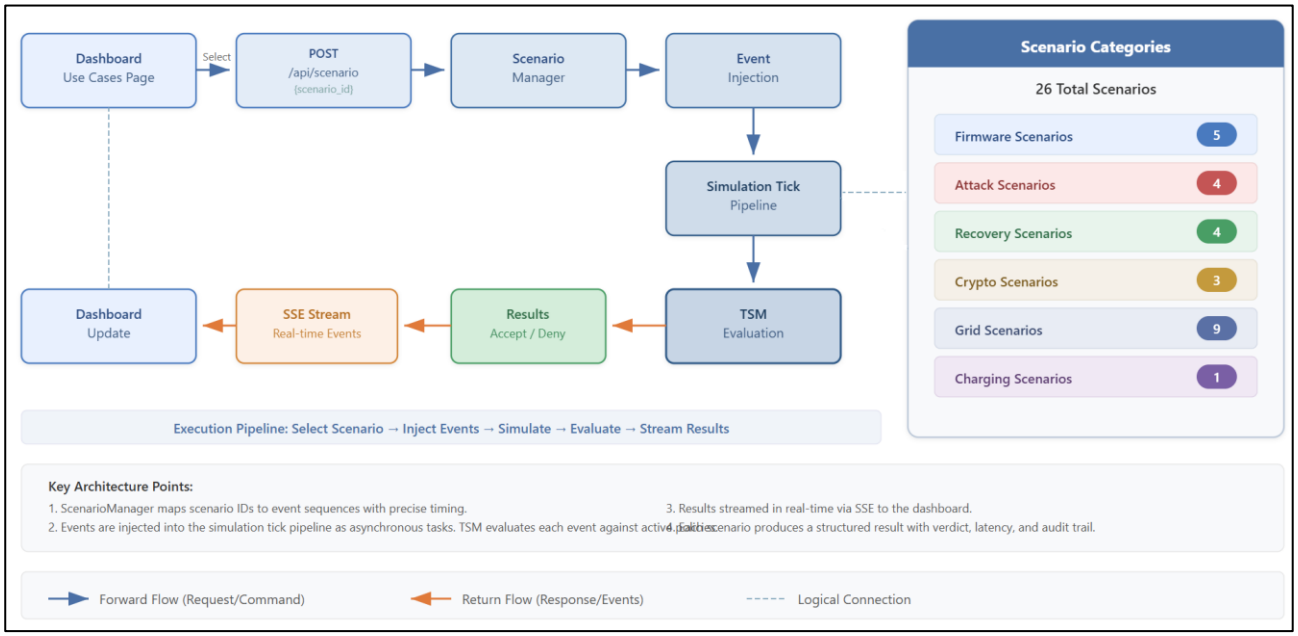


Figure 33: *The scenario categorization and execution framework within the co-simulation platform.*

Table 17*: Scenario categorization, sub scenarios, and types.*

Categories	Sub Scenarios	Scenarios Description
Firmware Update	5	valid firmware update, firmware anti-rollback, invalid oem signature, missing asd signature, revoked signer.
Security	6	power fluctuation, voltage spike, tpm compromise, replay attack, man in middle, tamper attack.
Power Grid	7	smart charge, v2g discharge, load shedding, demand response, islanding event, frequency anomaly, grid overload.
EVSE Charging	5	pre-conditioning, scheduled charge, session pause, normal charge complete, normal charge start.

Threat injection mechanisms in the co-simulation framework is demonstrated on different levels as follows:

1. Firmware level injection: In this level of threat injection, a malicious firmware envelope with revoked signer certificates, incorrect version number, and manipulated signatures are injected through the OCPP firmware update handler as well as POST /api/simulate/tsm-update API of TSM policy enforcement.
2. Physical level injection: In this level of threat injection, the debug API POST /api/debug/tamper is used for configurable tamper severity and types to record tamper events. The temper types are frequency anomaly, temperature anomaly, voltage glitches, and physical changes.
3. Protocol-level injection: In this level of threat injection, the scenario API is used for TPM spoofing, replay, and man-in-the-middle attacks to interrupt session integrity and protocol authentication.
4. Grid level injection: In this level of injection, the grid disturbances are injected using scenario API, such as islanding operation, grid overloading, frequency disturbances, and voltage fluctuations.

3.7.7 End-to-End Demonstration Design

The TSM Enforcement is evaluated on different scenarios and sub-scenarios. The evaluation of the co-simulation model is compared in a paired experimental design to evaluate its behaviour without TSM and with TSM to validate the TSM enforcement policies and functions.

In the bypass mode of TSM, the scenarios of different categories are run directly in the installation handler. For instance, the firmware updates process is directly accepted, having malicious envelopes to enforce excessive charging events, coordinated load attacks, and policy violations to disturb the normal behaviour of the EVSE infrastructure. It impacts grid-level disturbance such as elevated RoCoF, frequency deviations, and voltage excursions.

In the TSM enforcement mode, the scenarios are run by enforcing the TSM trust chain and policies and ensuring safe and stable operation of EVSE infrastructure. For instance, the process of updating firmware, the five-stage trust chain is implemented within the TSM security pipeline. The firmware update process is rejected when TSM-enforced policies are not compliant to ensure the secure and stable operation of EVSE and the power grid. The EVSE infrastructure operates within TSM policy-compliant, ensures grid stability, and operates within GSE boundaries. Figure 34 illustrates the comparative architecture of the system without TSM and with TSM modes within the co-simulation environment.

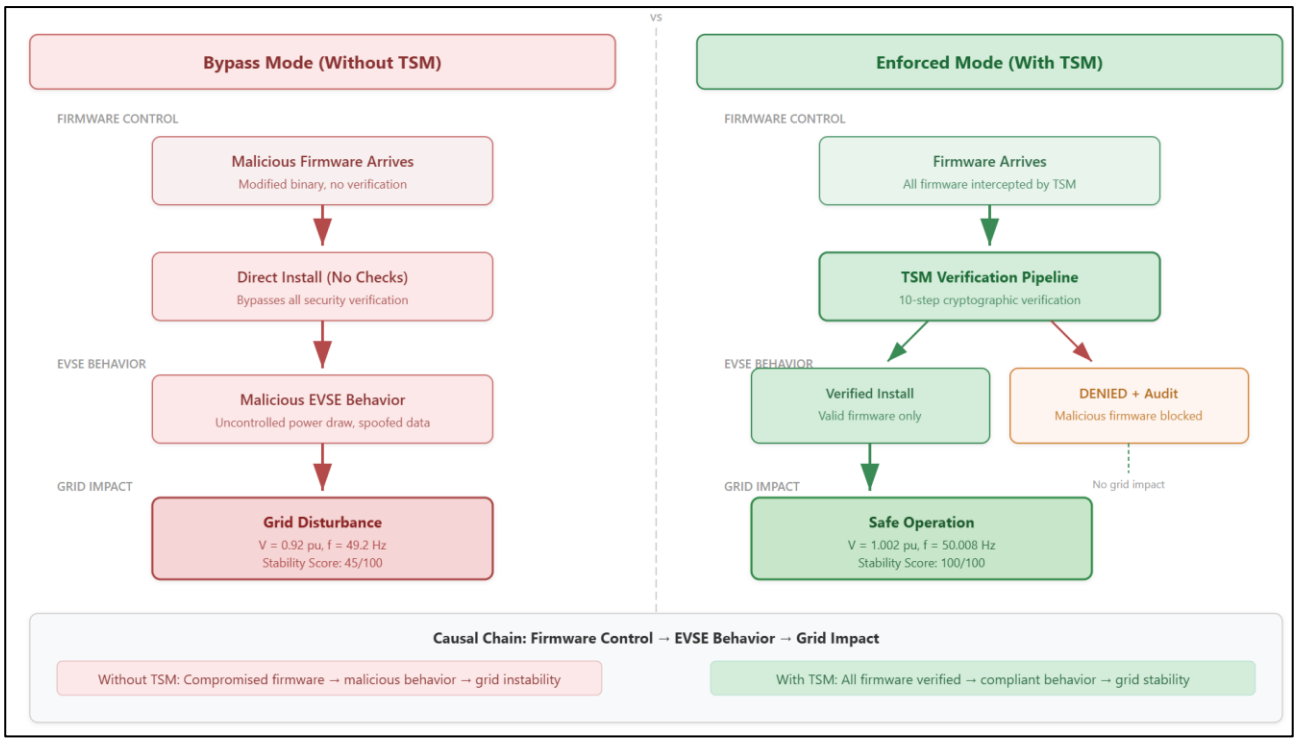


Figure 34*: The comparative analysis of scenario running without TSM and with TSM enforcement.*

The demonstration workflow follows six steps within the co-simulation environment as presented in figure 35. The details of the steps involved in the demonstration process are:

1. Initialize system: Starting backend and frontend server of the co-simulation platform. Ensure the status of TSM with OPERATIONAL and trust chain enforcement with healthy.
2. Infrastructure Deployment: The EVSE infrastructure can be deployed by adding several charging stations, adding some EVs, selecting appropriate charger types, connectors, type of charging stations, and battery chemistry.
3. Charging session establishment: The charging process is started by clicking **Run** to initiate the simulation process. It shows active sessions, total power delivered, average SoC, temperature, and uptime. The fleet can be selected to establish charging sessions.
4. Inject firmware threat: In the meantime, the firmware update scenario is run to observe the malicious firmware update with invalid OEM signatures, missing ASD signatures, revoked signers, and anti-rollback attacks.
5. Observe TSM response: The TSM enforces the OPERATIONAL state for each scenario, permitting valid firmware updates while rejecting all malicious variants. The system

successfully detects the invalid_signature attack, triggering the FAIL_SAFE operation, and subsequently resumes normal operation of the EVSE infrastructure.

6. Measure grid impact: The grid impact is measured in TSM bypass and TSM enforced modes. The grid stability is maintained within GSE boundaries due to TSM enforcement trust chain pipeline.

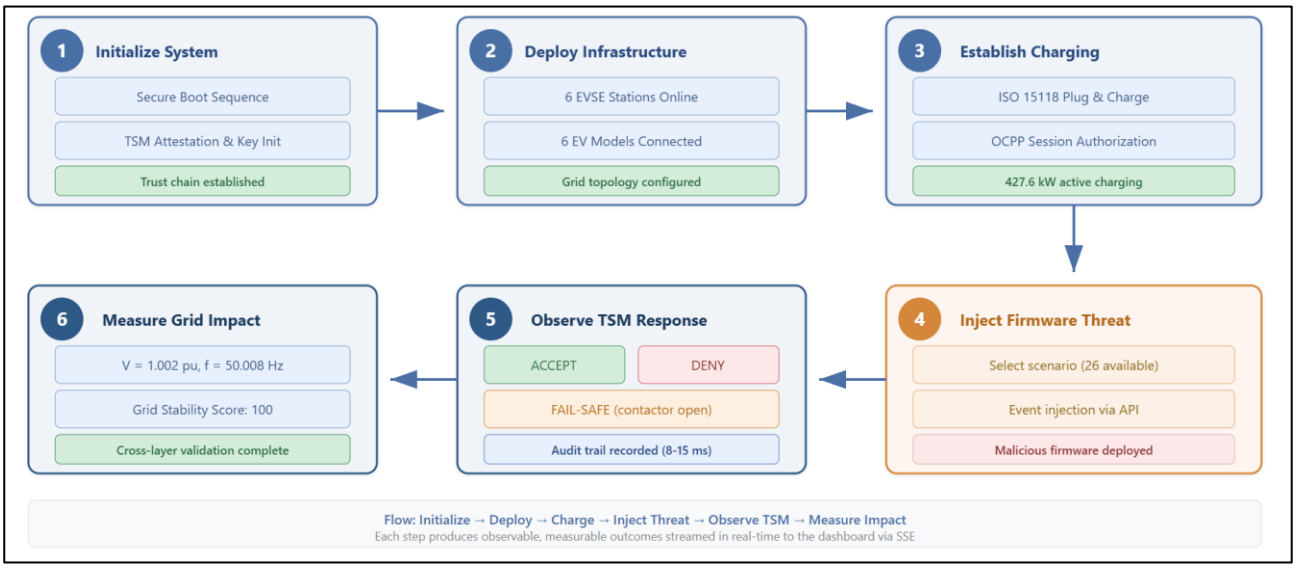


Figure 35:***The sequence of six steps demonstration flow for running simulation scenarios.***

3.5.7.1. Demonstrated Firmware Update Scenarios

In the demonstration of firmware update scenarios, five sub-scenarios are considered to evaluate the successful enforcement of TSM policies and the trust chain.

Scenario 1 — TSM-enabled Firmware Update: The TSM enforcement firmware update process allows legitimate firmware version 2.1.0 having valid OEM signatures, ASD counter signatures, version counting policies, hash matching, and validating trust chain complaints. The TSM enforcement checks and validates the process and updates firmware by executing the TSM-enabled security pipeline and ensure TSM state is OPERATIONAL.

Experimental result: The TSM enforcement allows the process of firmware update, the trace ID TRACE-000013 is generated, and the whole telemetry and events are recorded.

Scenario 2 — Missing ASD Counter Signature: In this scenario, the firmware image is signed only by the OEM and requires a sovereign authority to provide a counter-signature. When the ASD counter-signature is missing, the external validation trust anchor fails, breaking the trust chain.

Experimental result: The firmware update process is denied, all protocol-related interactions are captured, and the relevant events are recorded.

Scenario 3 — Firmware Rollback Attack: In this scenario, an attacker attempts to install an older, vulnerable firmware version. The golden hash is computed, and the anti-rollback counter detects the discrepancy. The update process fails within the secure boot trust chain, resulting in rejection of the firmware update.

Experimental result: Anti-rollback policies are triggered, and the Update TSM enforces anti-rollback measures to restore the previous, secure firmware version.

Scenario 4 — Invalid OEM Signatures: In this scenario, the OEM signature is forged or corrupted during a firmware update request. Within the TSM security pipeline, the trust chain is activated, and the ECDSA-P256 verification fails at the secure boot stage. The TSM enforces the FAIL_SAFE state.

Experimental result: The charging process is suspended, and the contactors are opened due to the TSM being in the FAIL_SAFE state.

Scenario 5 — Revoked Signer Certificate: In this scenario, the firmware image is signed with an ASD key that has been compromised and listed in the CRL. Verification against the revocation list fails, and the firmware update process is denied.

Experimental result: The TSM enforces the trust chain and maintains the OPERATIONAL state within the co-simulation platform.

3.7.8 Evaluation and Results

The results evaluation is conducted using the co-simulation environment described in deployment Section. The experimental setup consists of the following components:

- **Infrastructure:** The EVSE infrastructure is scalable, allowing the addition of varying numbers and types of charging stations, as well as multiple EVs with diverse charging connectors. The EVs are based on different OEMs, including Nissan, Ford, Hyundai, and Tesla. Battery chemistry types can be selected, and the initial state of charge (SoC) ranges from 10% to 55%.
- **Grid configuration:** The distribution power grid is modeled using an IEEE 13-bus network with a base voltage of 12.47 kV, a transformer rated at 10 MVA, and a nominal grid frequency of 50 Hz.
- **TSM configuration:** The TSM trust chain policies are enabled, and the grid safety envelope is activated.
- **Instrumentation:** The co-simulation platform instrumentation is enabled to capture TSM decision audit trails, record all protocol messages, log JSONL metrics, and collect SSE telemetry for all events.

The execution of all scenarios and sub-scenarios to record events, metrics, and protocol interactions with TSM verification tracing and audit trails.

Layer 1: Cybersecurity Enforcement Results: The outcomes of the firmware update scenarios are summarized as follows:

The main observations from the firmware update scenarios are:

- False Accept Rate (FAR) is 0% during the firmware update scenarios due to TSM policy enforcement, ensuring that no malicious firmware is installed or allowed to progress.
- False Reject Rate (FRR) is also 0%, as the TSM-enforced trust chain guarantees that legitimate firmware updates are applied correctly.
- In the invalid OEM signature scenario, triggered by invalid_OEM_signature, the EVSE system responded with the most severe action, entering the FAIL_SAFE state.

The overall results of cybersecurity enforcement are presented in figure 36, illustrating scenario verification, key performance metrics, and scenario-based decision latencies. These results validate the sovereign firmware mediation hypothesis (H1), confirming its effectiveness in preventing malicious firmware updates and mitigating associated adversarial conditions.

Figure 36*: The results of Layer 1: key performance metrics, decision latencies for each scenario, and firmware update verification scenarios.*

Firmware update and various security attack scenarios were executed successfully within the co-simulation platform. Tampered attack scenarios triggered the FAIL_SAFE state, opening contactors, after which the system transitioned to recovery mode via FORCE_OPERATIONAL, ultimately restoring the OPERATIONAL state. Other attacks, including MiTM and TPM spoofing, were also successfully detected, while the TSM security pipeline maintained the OPERATIONAL state. Details of these security scenarios, along with TSM trust chain and policy enforcement, are illustrated in figure 37 and table 18.

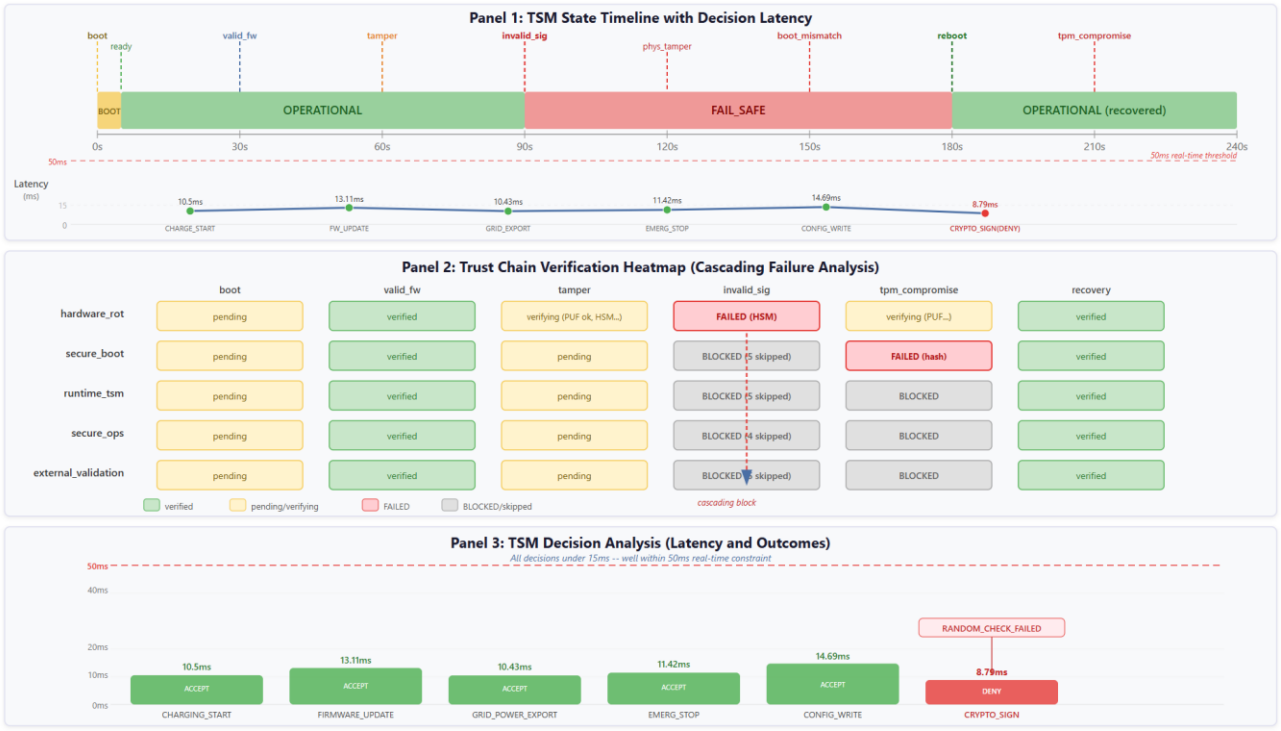


Figure 37: ***TSM policies enforcement and trust chain for decision latencies, cascade failure analysis of TSM policy enforcement, and decision metrics analysis for different attack scenarios.***

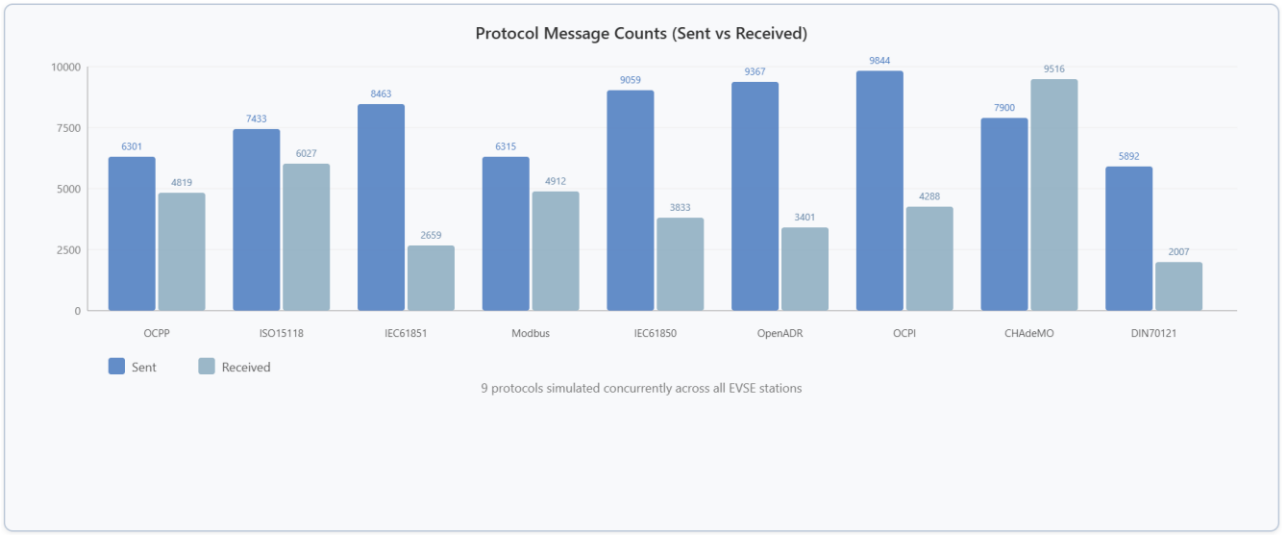
Table 18: ***The summarization of attack scenarios and their impact on TSM enforced trust chain***

Scenarios	Attack Vectors	TSM Responses	Post State	Chain Impact
Invalid signatures	Malicious firmware	DENY + FAIL_SAFE	fail_safe	Stage two + BLOCKED
TPM compromised	Hardware spoofing	DENY + ALERT	fail_safe	Stage one + BLOCKED
Tampered attack	Physical intrusions	DENY + FAIL_SAFE	fail_safe	Stage four + BLOCKED
MiTM attack	Protocol interceptions	DENY + AUDIT	OPERATIONAL	No impact

Layer 2: EVSE and DER Operational Results: In Layer 2, the operational performance of EVSE and DER systems is evaluated. A fleet of six EV chargers is connected to the charging station, with all connections established and grid parameters synchronized to ensure a stable power supply. The EV charging profiles track metrics such as target state of charge (SoC) percentage, peak power delivered to each EV, charging status, and active sessions. During operation, nine communication protocols exchange control information concurrently across the EV fleet. A detailed illustration of this setup is provided in figure 38, while real-time telemetry of EVSE operations—including total SoC, power delivery, and battery temperature during charging—is shown in figure 39.

EV Fleet Charging Status (6 Active Sessions)

Vehicle	SOC	Power (kW)	Status	SOC Bar
Tesla Model 3	50.0%	72.8	Charging	50%
Rivian R1T	34.2%	71.8	Charging	34%
BMW iX	36.8%	70.6	Charging	37%
Hyundai Ioniq 5	44.8%	71.9	Charging	45%
Ford F-150 Lightning	22.4%	70.1	Charging	22%
Nissan Leaf	43.7%	70.5	Charging	44%
Fleet Totals:	**Avg: 38.7%**	**Total: 427.6 kW**	**6/6 Active**	



Fleet summary: 6 EVs, total power 427.6 kW, average SOC 38.7%, all 9 charging protocols active and exchanging messages.

Figure 38*: Layer 2 results: EV fleet charging profiles and statistics of communication protocols interactions*

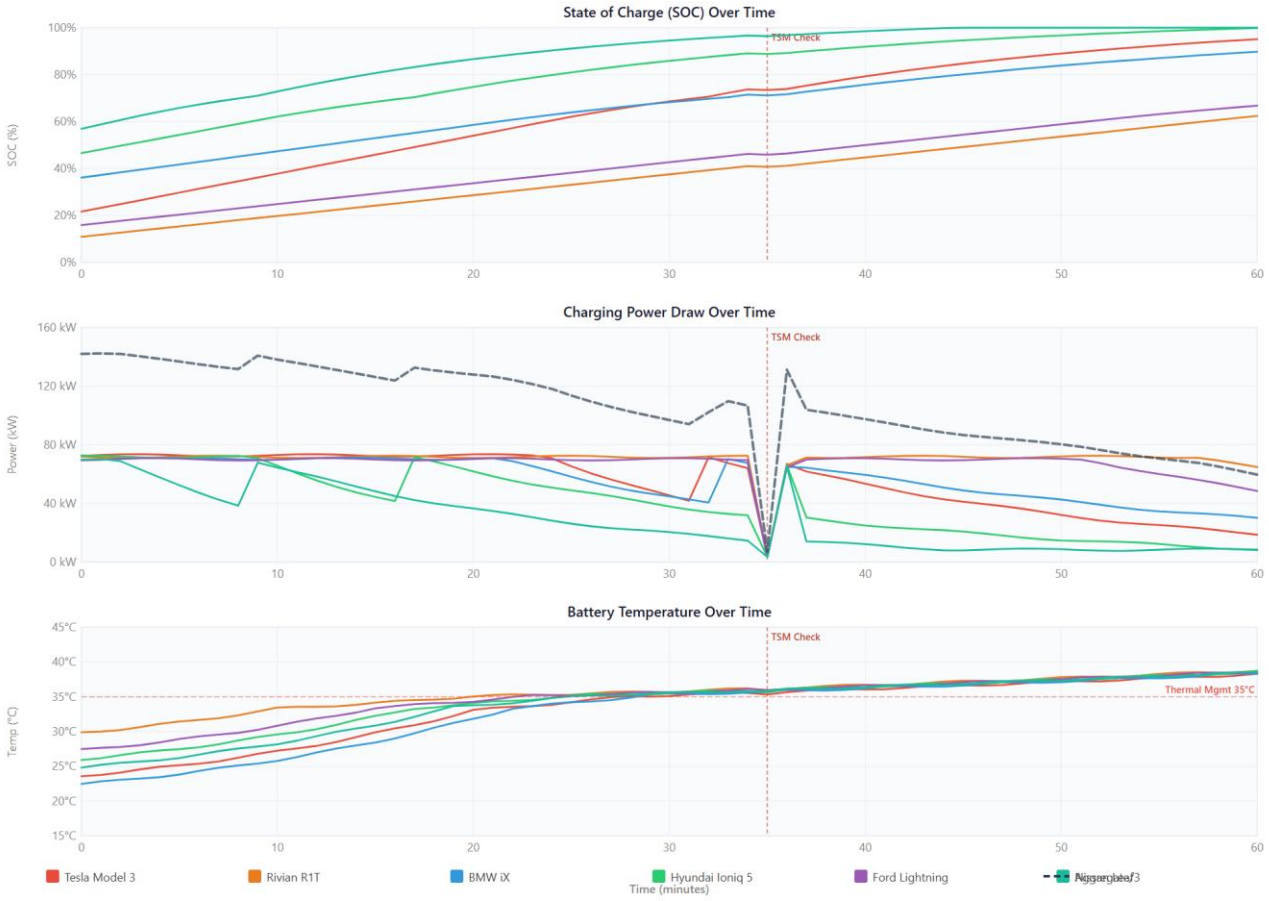


Figure 39*: Real-time charging profile of EV fleet: the SoC charging profile over sixty minutes, total power delivery to EV fleets, and temperature distribution for individual EV across the EVSE fleet.*

Key findings: The results reveal several important observations:

- All EVs in the fleet operate within the limits of charging station capacity, load demand, and battery charging dynamics.
- Active sessions are established for all EVs, ensuring full utilization of EVSE capacity.
- All EVs maintain stable charging states throughout the operation.
- TSM policy enforcement successfully governs the entire process, with no violations detected.

These findings demonstrate the effective prevention of unsafe EVSE behavior. Furthermore, the results support hypothesis H2, confirming that firmware enforcement constraints successfully prevent risks associated with malicious firmware update attempts.

Layer 3: Grid Level Impact: Grid stability during EV fleet charging is maintained through TSM-enforced policies and the trust chain. Figure 40 illustrates frequency and voltage stability during EV fleet charging, demonstrating the effectiveness of TSM policies in preserving power grid stability.

Figure 40*: Layer 3 results: TSM enforced frequency and voltage stability of power grid.*

3.8 TSM Validation Results

In this Section, verification and validation (V&V) framework of the TSM framework is discussed and introduces structured threat classes (TC1–TC4) for firmware updates, establishing a scenario model for end-to-end firmware update operations, multiple scenarios for power grid validation, and quantitative security metrics. The V&V approach evaluates the TSM security pipeline across three dimensions: (1) assessing TSM capabilities to block threats, measuring TSM security effectiveness; (2) evaluating system behaviour under attack to determine system resiliency; and (3) analyzing the impact of EVSE-level security to ensure power grid stability.

Firmware Update Threat Classes

The threat model analysis defines four distinct threat classes for firmware update scenarios:

TC1 — Forged/Invalid Firmware: An attacker injects a firmware image signed with untrusted keys or tampers with existing signatures. This type of attack is intercepted within the trust chain during ECDSA signature verification, CRL checks, and certificate chain validation.

TC2 — Malicious but Validly Signed Firmware: The attacker provides a validly signed firmware image from the OEM but embeds malicious logic, such as bypassing safety protections, overriding

power dynamic limits, or altering EVSE control parameters. This attack passes cryptographic verification but is intercepted by the runtime TSM pipeline enforcement.

TC3 — Rollback/Downgrade Attack: Here, an attacker attempts to reinstall an older, vulnerable firmware version to degrade system operation. Detection occurs through monotonic version counters, golden hash key matching, and HRoT validation stages, preventing the rollback.

TC4 — Trust Anchor Compromised: This class involves attacks on the hardware root-of-trust, including resetting monotonic counters, modifying golden hashes, replacing secure boot keys, or injecting rogue root certificates. Such attacks are detected and mitigated through remote attestation and runtime TSM validations.

The escalation of risks follows a predictable cascade model: **Devices** experience issues during normal charging sessions → **Sites** are affected by events such as transformer overheating → **Fleet** experiences coordinated load surges → **Grid** sees deviations in frequency and voltage. This model illustrates how localized attacks can propagate and impact system-wide operations.

TC1 — Invalid or Forged Firmware: Figure 41 illustrates a scenario where an attacker injects a firmware image with an invalid signature into eight EVSE chargers via the OTA channel at (t = 30) sec. The TSM pipeline's HID intercepts the firmware image and performs sequential validation checks, including ECDSA-P256 signature verification, CRL lookup, and certificate chain validation from leaf → OEM CA → sovereign root. These checks fail for the invalid or forged firmware image, and the TSM rejects the update before it reaches the flash storage writing stage.

The top panel shows cumulative firmware update acceptance. In TSM bypass mode, the forged firmware is accepted and installed within 10 sec. In TSM-enabled mode, the count of malicious firmware updates remains zero at all times due to TSM policy enforcement. At (t = 120) sec, two valid firmware updates are injected and successfully processed through the TSM trust chain, demonstrating that legitimate updates pass without restriction.

The middle panel depicts the compromised status of the EVSE chargers: in TSM bypass mode, all eight chargers accept the malicious firmware at (t = 70) sec, whereas with TSM enabled, no charger is compromised. The bottom panel compares cryptographic validation scores, showing 98% with TSM enabled versus approximately 15% without TSM, where only a basic checksum is applied.

Key results:

- False Reject Rate (FRR) for valid firmware updates = 0.00
- False Accept Rate (FAR) for malicious firmware= 0.00
- True Positive Rejection Rate (TPR)= 1.00

These results confirm that TSM enforcement reliably prevents forged or invalid firmware from being installed while allowing legitimate updates to proceed.

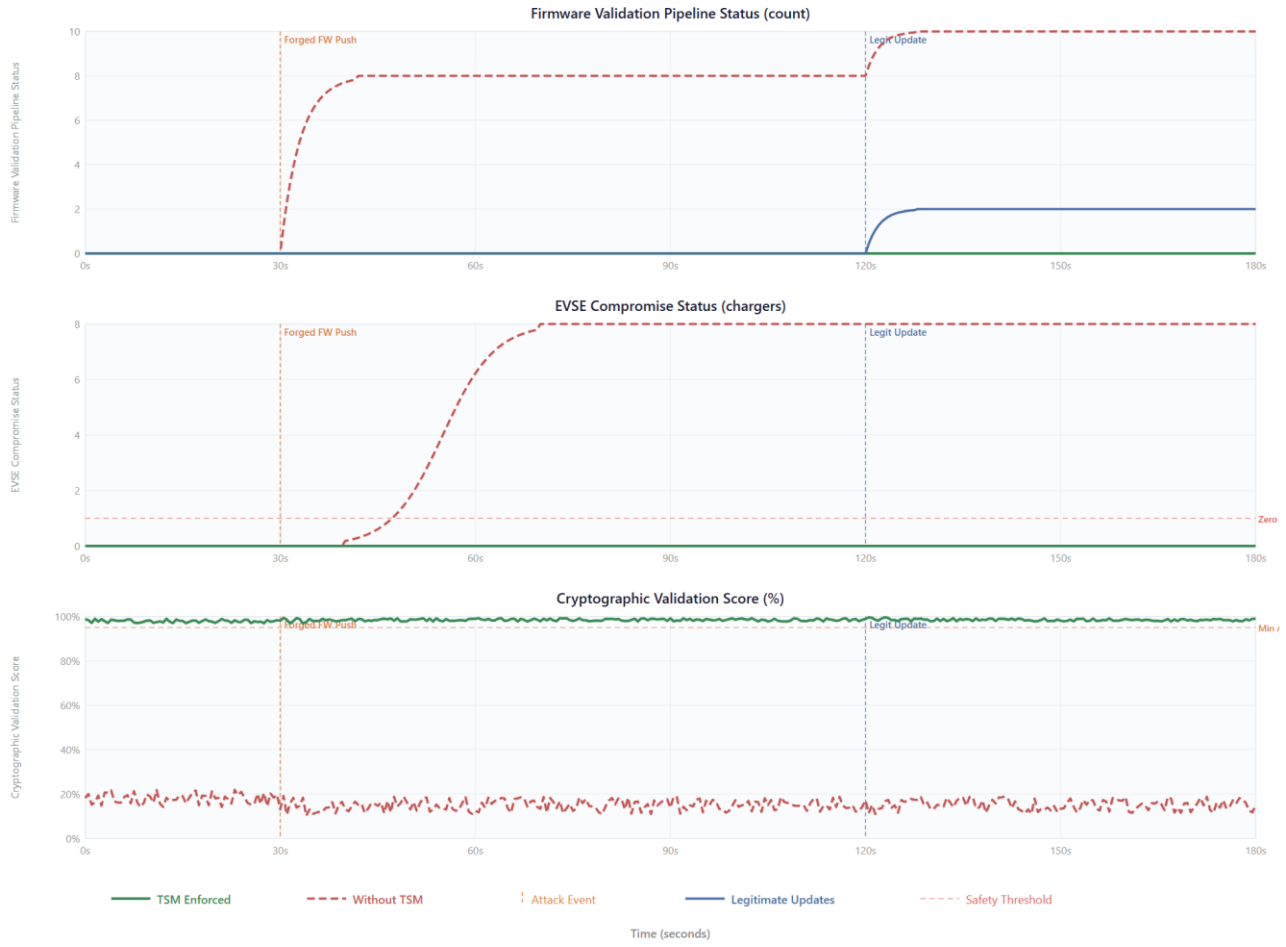


Figure 41: *TC1: Injection of invalid firmware image. The TSM enforcement uses a crypto engine to reject all firmware images with invalid keys using ECDSA signatures verification and validating the certificate chain in the trust chain.*

TC2 — Malicious but Validly Signed Firmware: Figure 42 illustrates a critical firmware update threat scenario in which cryptographic checks pass due to valid OEM signatures. The threat arises from an embedded malicious payload that overrides normal EVSE charger behavior, suppresses the safety contactor interlock, and enables unauthorized remote fleet charging. This type of threat is intercepted by the TSM at runtime through behavioral policy enforcement.

At (t = 40) sec, a malicious firmware update request is initiated on six EVSE chargers. The panels present the following observations:

- **Power draw:** In TSM bypass mode, power ramps from 70 kW to 160 kW. In TSM-enabled mode, each EVSE charger is clamped back to 80 kW within 50 ms, with a short transient peak at 92 kW.
- **Contactor safety score:** The safety interlock collapses to ~18/100 in TSM bypass mode, while in TSM-enabled mode it recovers within 2 sec due to enforcement.
- **Cumulative policy violations:** Without TSM, 52 policy violation events go undetected over 260 sec; with TSM, only 2 events occur and are mitigated.
- **Unsafe actuation duration:** 260 sec without TSM versus 0.05 sec with TSM, reflecting the rapid detection-to-clamping response.

Key results:

- Policy enforcement latency: < 50 ms
- Unsafe actuation duration reduced by > 99.98%

These results validate hypotheses H1 and H2, demonstrating that cryptographic authenticity alone is insufficient and that runtime behavioural enforcement is essential to mitigate TC2 firmware update threats effectively.

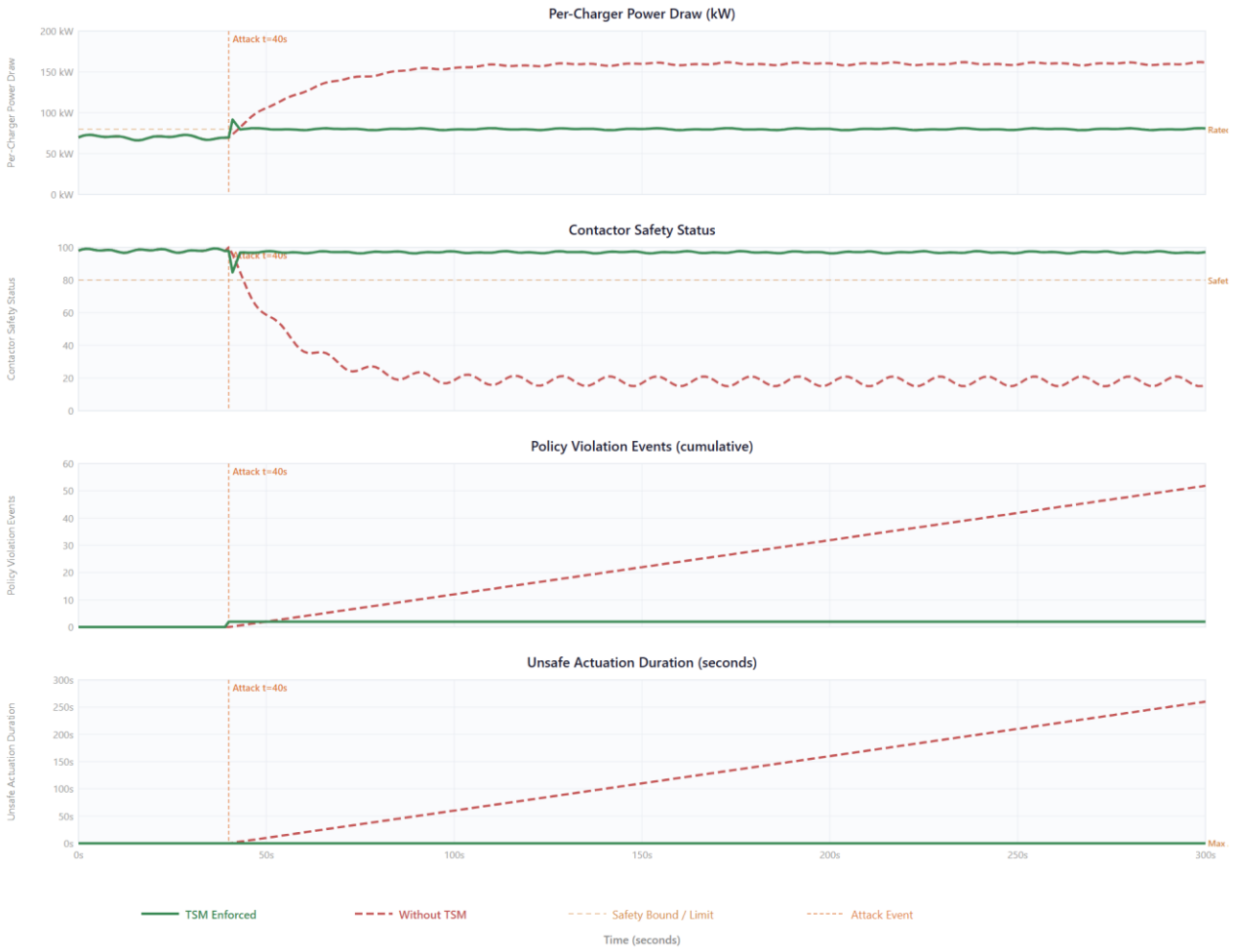


Figure 42: *TC2: Malicious but validly signed firmware. The TSM security pipeline is enforcing a runtime behavioural model for the EVSE charger behaviour within 50 ms, while the unsafe duration is 0.05 sec.*

TC3 — Firmware Rollback / Downgrade Attack

Figure 43 illustrates a firmware rollback or downgrade attack in which an attacker attempts to revert the firmware from version v3.2.1 to v2.8.0—an outdated version containing vulnerabilities such as telemetry spoofing and bypassed safety logic, which were patched in v3.1.2. The TSM trust chain deterministically blocks this attack using a monotonic counter in the HRoT: the counter value 321 exceeds the target downgrade value 280, and the firmware update is rejected according to anti-rollback policies.

The panels highlight the following results:

- **Firmware version scale (top panel):** The current version is normalized to scale 100, while the targeted downgrade is at scale 60. In TSM bypass mode, EVSE chargers' firmware is downgraded from 100 to 60. With TSM enabled, the version remains at 100, with a brief 2 sec processing hold at 98 at (t = 25) sec.
- **Security feature coverage (middle panel):** In bypass mode, rollback reduces coverage from 95% to 45%, whereas TSM-enabled mode maintains 95% throughout the process.
- **Vulnerability exposure (bottom panel):** Without TSM, rollback reintroduces known vulnerabilities such as compromised safety limits, contactor logic issues, and missing patches. With TSM enforcement, the exposure count remains zero due to trust chain policies.

Key results: Rollback Prevention Rate (RPR) is covered 100% . Unlike TC1 and TC2, TC3 affects the maturity of security features rather than introducing malicious code. The HRoT monotonic counter effectively prevents rollback and downgrade attacks, validating hypothesis H1 for TC3 scenarios.

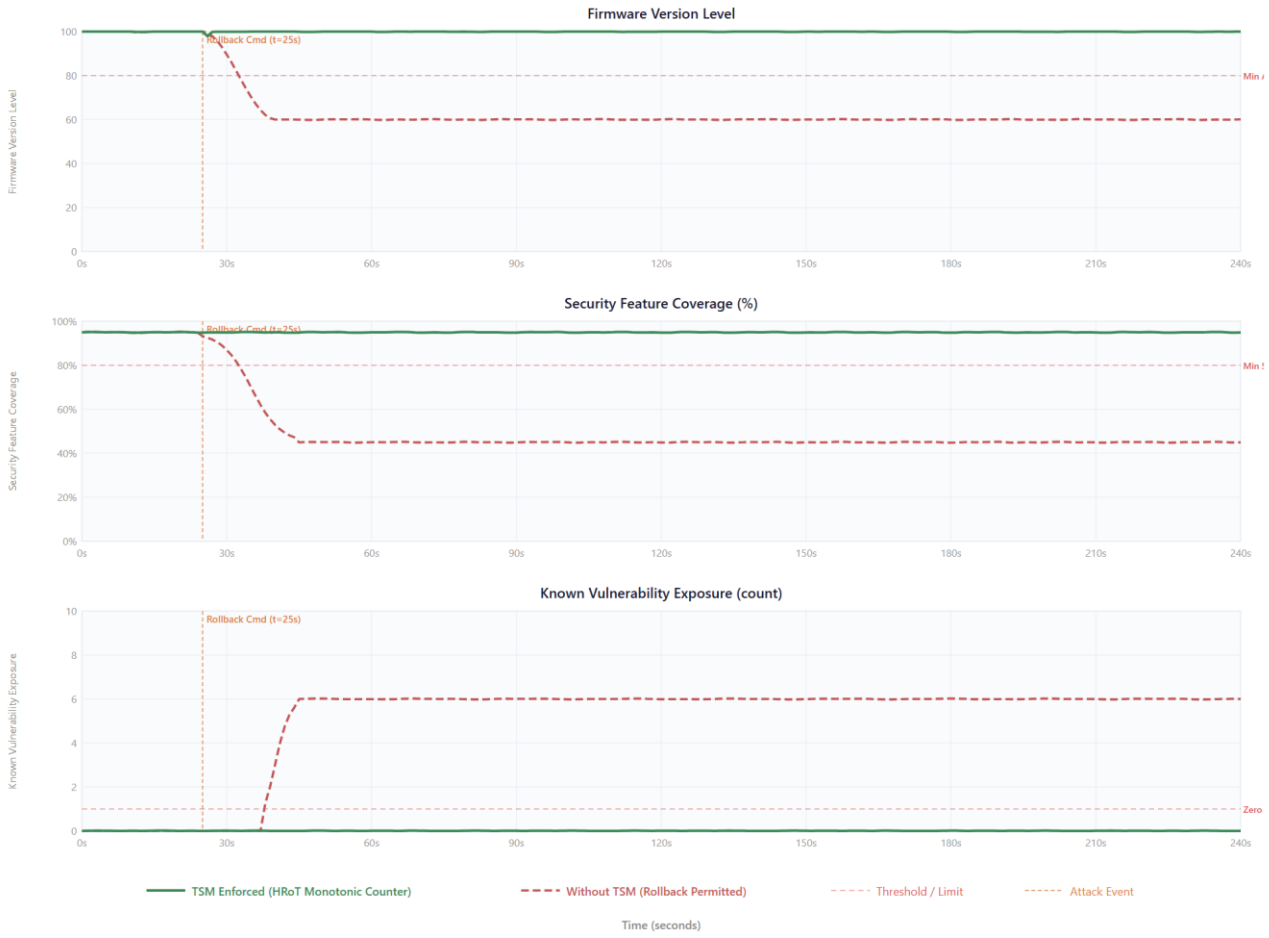


Figure 43*: TC3: Firmware rollback attack. TSM-enabled enforcement triggered HRoT monotonic counter to block the older version and maintained full security features with RPR=100%.*

TC4 — Trust Anchor Compromise: Figure 44 illustrates the most severe firmware attack scenario, in which an attacker compromises the HRoT of eight EVSE chargers by resetting

monotonic counters, modifying golden hashes, replacing secure boot keys, and injecting rogue root certificates. Once the trust anchor is compromised, all security and cryptographic mechanisms in the TSM trust chain are rendered ineffective, and a malicious firmware image could be treated as legitimate. To mitigate this, TSM enforces periodic remote attestation, allowing the CPO and other stakeholders to detect the compromise and associated vulnerabilities.

During the attack:

- At (t = 20) sec, four EVSE chargers are tampered with HRoT. The **first panel** shows trust anchor integrity dropping from 100% to 50% in TSM bypass mode, where no detection occurs. In TSM-enabled mode, the next attestation cycle at (t = 35) sec identifies the compromise, and the affected chargers are isolated at (t = 45) sec, maintaining fleet integrity at 100% for healthy chargers.
- The **second panel** tracks the secure boot chain, which drops from 8 to 4 in both modes. TSM reprovisions the compromised chargers at (t = 120) sec, restoring the full fleet count to 8.
- The **third panel** shows the attestation success rate: ~5% in TSM bypass mode, 50% in TSM-enabled mode during the detection phase, and 100% after full recovery.
- The **fourth panel** presents the fleet risk score (0 = safe, 100 = critical). In TSM bypass mode, the score peaks at 85 due to the attack. In TSM-enabled mode, it drops from 85 to 45 during detection and stabilizes at 5 after reprovisioning.

These results demonstrate that TSM remote attestation and runtime policy enforcement can detect, isolate, and recover from even the most severe trust anchor compromise attacks, preserving fleet integrity and minimizing operational risk.

Figure 44*: TC4: Trust anchor compromise. The TSM-enabled enforcement provides remote attestation capabilities to detect HRoT manipulation using attestation cycle and detection latency to isolate the promised EVSE chargers from the fleets and restore EVSE fleet.*

3.8.1 Fleet-level Impact and Risk Escalation

The individual threat classes TC1–TC4 are first evaluated at the device level. In real-world scenarios, combined attack vectors can be initiated at the fleet level to observe their impact on the distribution grid and to follow the escalation pathway from EVSE devices to the grid.

Coordinated Fleet Attack

Figure 45 illustrates a TC2 scenario where a malicious simultaneous firmware update is injected across a fleet of 20 EVSE chargers connected to a 2 MW distribution feeder. The compromised chargers override their power limits from 80 kW to 150 kW, producing an aggregated demand of 3.0 MW—150% of the feeder's rated capacity, thereby exceeding thermal limits.

Observations from the panels:

- **Aggregated fleet demand (top panel):** Without TSM enforcement, load surges from 1.2 MW to 3.0 MW, violating the feeder rating. With TSM enabled, runtime clamps limit each EVSE to 80 kW, resulting in a fleet demand peaking at 1.7 MW and stabilizing at 1.6 MW, maintaining safe operating margins.

- **Bus voltages (second panel):** In bypass mode, voltage drops to 0.85 p.u. With TSM enforcement, voltages are maintained at 0.97 p.u., within the GSE bounds of 0.95–1.05 p.u.
- **Transformer thermal rating (third panel):** TSM bypass mode causes the transformer temperature to rise to 115 °C, exceeding the 105 °C tripping limit. TSM-enabled mode maintains a peak temperature of 65 °C.
- **Composite grid stability score (bottom panel):** The score is 15/100 in bypass mode versus 93/100 with TSM enforcement.

Key result:

Malicious firmware updates can trigger coordinated EVSE load attacks, potentially destabilizing the power distribution network. The TSM-enabled trust chain successfully mitigates this threat, preserving grid stability and validating hypotheses H2 and H3.

Figure 45*: A fleet-level coordinated load attack occurs under TC2 when a malicious firmware update is initiated simultaneously on 20 EVSE chargers. This causes the total load to surge to 3.0 MW, exceeding the distribution feeder's rated capacity by 150%. With TSM*

Risk Escalation: Device-to-Grid Cascade Approach: Figure 46 illustrates a four-level cascade of risk propagation during firmware attack scenarios, showing how a single compromised EVSE can escalate through the infrastructure:

Device level ((t = 30) sec): A malicious firmware request is injected into a single EVSE, overriding power limits and suppressing safety interlocks. The device-level risk score peaks at 90/100.

Site level ((t = 60) sec): The compromised firmware propagates across EVSE chargers within a station via shared OTA channels, affecting inverters, controllers, and transformers. The site-level risk score reaches 80/100.

Fleet level ((t = 120) sec): The firmware spreads to remote sites through OEM backend communication channels, with a fleet-level risk score of 70/100.

Grid level ((t = 240) sec): Aggregate fleet behaviour impacts the distribution system, causing feeder overloads, voltage deviations, and potential brownouts. The grid-level risk score is 85/100.

With TSM security pipeline enforcement, the attack is intercepted at the device level within 50 ms, reducing the device-level risk score to 10. Subsequently, site, fleet, and grid risk scores remain below 5 throughout the simulation. The shaded region in figure 46 illustrates this potential escalation wave that is mitigated by proactive TSM policies.

Key results:

Device-level TSM enforcement is the most effective layer, preventing attacks from propagating to critical infrastructure.

Proactive intervention at EVSE devices blocks threats before site, fleet, or grid-level impacts occur.

This approach validates hypotheses H1, H2, and H3, demonstrating that early, localized TSM enforcement ensures system-wide cybersecurity and operational stability.

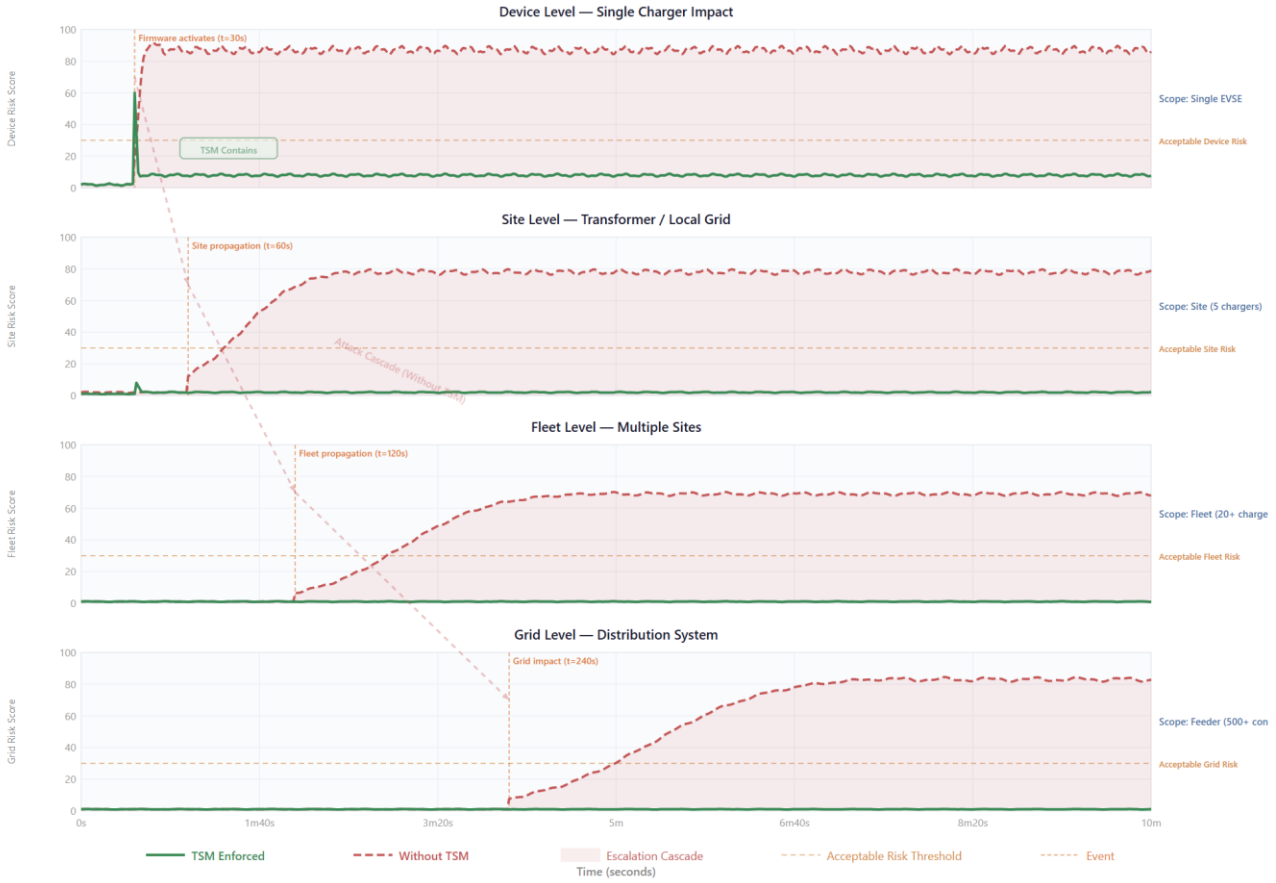


Figure 46: ***The risk escalation model follows a cascade from Devices → Sites → Fleets → Grids. In the absence of TSM, a single compromised EVSE can propagate the attack through all levels, reaching the grid within approximately 4 minutes. With TSM-enforcement.***

TSM Metrics and Performance Validation: Apart from single scenario analysis, the V&V approach evaluated the TSM overall security performance and operational behavior through a metrics framework. Figure 47 showing the performance metrics of all firmware update threat classes. The top section compares TSM-enabled and without TSM modes for key metrics. All malicious firmware update images are rejected, with a true positive rejection rate (TPR) of 1.00 and a false accept rate (FAR) of 0.00. All legitimate firmware updates are accepted without rejection, validated with a false reject rate (FRR) of 0.00. Rollback policies are fully enforced, achieving a rollback prevention rate (RPR) of 100%. Fail-safe reliability (FSR) is 1.00, and the audit trail provides 100% coverage for threat analysis. The middle section shows performance overhead: TSM-enabled decision latency is 7.6 ms, signature verification latency is 3.1 ms, and total pipeline latency is 8.9 ms, all within the 15 ms standard. The bottom section illustrates threat class coverage, showing TSM strategies effectively prevent attacks across all firmware update threat classes.

Figure 47: ***The summarized TSM-enabled security metrics are: True Positive Rejection Rate (TPR) = 1.00, False Accept Rate (FAR) = 0.00, False Reject Rate (FRR) = 0.00, and Fail-Safe Reliability (FSR) = 1.00. All firmware update-related threat classes are mitigated.***

Pipeline Performance Under Load: Figure 48 evaluated the TSM-enabled firmware validation pipeline was evaluated for three operations over a 60-minute window: validation decisions, signature verification, and overall pipeline throughput. Routine updates involve individual EVSE chargers updated within 10 minutes, achieving a pipeline throughput of approximately 5 updates per minute. Batch updates involve 20 EVSE chargers simultaneously updated within 25 minutes, with a throughput of approximately 20 updates per minute. At 40 minutes, an attack attempts to inject eight forged firmware images.

Decision Latencies: The top panel tracks latency percentiles. The mean baseline latency is 7.6 ms, rising to 10.2 ms during batch updates. The 95th percentile is 11.4 ms at baseline and surges to 14.1 ms under batch load. The maximum observed latency reaches 17.8 ms.

Cryptographic Operations: The middle panel shows signature verification and cryptographic operation times. ECDSA-P256 verification averages 3.1 ms, certificate chain validation averages 2.2 ms, and CRL lookup averages 1.8 ms. Minor jitter is observed around 30 minutes during batch updates.

Pipeline Throughput: The bottom panel illustrates throughput, with a maximum of 22 validations per minute during batch updates. Malicious or invalid firmware images are processed faster than legitimate images because they fail at initial pipeline stages, while legitimate images traverse the full TSM security pipeline.

These results demonstrate that TSM policies can operate effectively under routine, batch, and attack conditions while maintaining acceptable latency, validating the feasibility claim H4.

Figure 48*: The aggregate performance of the TSM firmware update security pipeline for the 60-minute simulation window. The mean latency is 7.6 ms indicate the operational feasibility and latency acceptance of TSM enforcement policies for the firmware update.*

3.9 TSM Future Implementation

The results in previous sections demonstrate the technical capabilities of TSM for threat detections, grid stability constraints, and numerous attack scenarios from a unified co-simulation environment to field-deployed EVSE infrastructure considering a distinct set of practical constraints. The technical challenges for charging operators, EVSE manufacturers, and standardization bodies should be addressed before its practical implementation on scale. In addition, the technology maturity, software applications, and cybersecurity technologies would accelerate the real-world deployment of TSM implementation.

3.9.1 Practical Limitation and Challenges

There some potential practical challenges in the implementation of TSM at full-scale EVSE infrastructure. The summarized details are a follow:

- **HRoT Availability**: The proposed TSM-enforced framework is secured hardware-based rooted identity for all types of EVSE chargers which is not considered in the design. The possible solution would be modifying main controllers or introducing bump-in-the-wire cyber control gateways to intercept OCPP traffic for attestation and EVSE hardware identification.
- **Firmware Signing Supply Chain**: Dual signing verification and attestation required dual trust model to delegate trust from OEMs to national signing authorities in the current supply chain which does not exist in current trust enforcement models. For the update supply chain models, operating procedures, critical processes, dispute resolution mechanism, and OEM dual attestation support policies should be established.
- **Protocols and Standards**: Current EVSE and grid protocols OCPP 2.0.1, ISO 15118-20, and OpenADR 2.0b provides message-level control information and did not support mediation layer between EVSE and CSMS. To support this, the standard working groups should adopt TSM hooks for mediation layer profiles so that each OEM have support to implement TSM integration for mediation actions, trust states, and threat levels.
- **Large-scale PKI lifecycle**: The deployment of TSM-enabled EVSE on large-scale requires X.509 certificate chains having revoking, rotating, and issuing certificate chains to meet CRL distribution is significantly challenging to meet certificate transparency and operational requirements. Existing ISO 15118 did not support device-level attestation certificates which requires larger PKI infrastructure or PKI as a services availability to support TSM-enforced PKI lifecycle certifications.
- **Processing Overhead Constraints**: The TSM-enforced end-to-end latency is mean 4.20 ms and 99th percentile is 11.28 ms which is acceptable in 30 seconds OCPP pipeline. However, every EVSE estimated policy enforcement at 0.51 ms, trust score at 0.89 ms, and firmware attestation at 2.80 ms will require more resources on EVSE controllers. To cope this, TSM kernel on EVSE nodes or cloud-based third-party verification will be required to mitigate real-time processing overhead.
- **Cross-border Interoperability:** OCPI assumes the EVSE real-time sessions are authorized and trusted when roaming between eMSP and CPO networks. For TSM-enforced trust anchors, it will be managed through trust anchors federations or requires mutual recognition between trusted authorities which do not exist in the current enforcement models and required polic-level implementation before technical endorsement.

3.9.2 TSM Supported Technologies

Considering practical limitations and technical challenges, the feasibility for TSM supported technologies is depends on proactive standardization, deployment of cross-border domains, and maturity of individual EVSE technologies to support TSM-enforced trust models.

- **HRoT Integration**: Current TPM 2.0 TCG TPM 2.0 library possesses embedded secure elements such as Infineon OPTIGA, ATECC608 Microchip, and NXP SE050/SE051 with reasonable price of 1-5 USD for mass production which could meet TSM-enforced HRoT criteria such as ECDSA signatures, monotonic counters, and hardware-rooted identities [45]. It would potentially accelerate the TSM integration and trust enforcement by adopting these technologies in the new EVSE designs.
- **Firmware Attestation Pipeline**: The current firmware attestation framework templates such as Arm PSA, UEFI Secure Boot, and NIST SP 800-193 provides runtime and boot time firmware attestation that could be adopted for the EVSE trust-enforced firmware attestation with modifying hash management and profile registration procedures [46]-[48].
- **Protocol Support**: Current OCPP 2.0.1 provides TLS 1.2+ support, security event reporting, security hooks, signed firmware messages, and customized configuration while ISO 15118 will need certificate provisioning , certificate contracts, and mutual TSL. OpenADR 2.0b protocol supports EVSE, grid, and dynamic load relevant communication that are sufficient for the end-to-end control messaging of TSM-enforced interactions without further protocol extensions and mediations.
- **PKI Lifecycle at Scale**: There are numerous PKI providers to provide open-source PKI stacks such as HashiCorp Vault PKI [49], Step-Ca [50], and EJBCA [51] to support PKI certificate chain for EVSE at larger-scale. It adopted on pilot scale in the USA by EV Roaming Foundations [52] and Hubject Plug&Charge [53] that provides certificates transparency and CRL distribution, root certificate handling, and incident response in the operational templates.
- **Operational Feasibility**: The adjacent sectors V2X, SCADA, and DERMS in smart grid deployed federated trust modelling while projects such as CharIN's Plug&Charge [54] and CyberSEAS programme [55] has been validated cross-federated trust models, policy mediation, and PKI certification. It provides a concrete foundation for the deployment of TSM-enforced policy mediation and trust enforcement if governance framework is implemented.

The best approach for the TSM adaptation is ***incremental*** deployment pathways for the full-scale TSM-enforced EVSE framework. EVSE operators should incrementally deploy TSM-enforced trust mediation through trust scores on server sides and on end user sides to capture complete cyber-physical command capture and develop concrete steps for next stage implementation. In addition, mature HRoT, open-source ***PKI***, customized ***EVSE protocol stacks***, and proactive regulatory frameworks would accelerate TSM implementation operationally and technically within 3-5 years. The major constraints are not technical, they are standardization, governance, and stakeholder engagement to push trust modelling research on existing EVSE infrastructure resources.

To further assess TSM deployment feasibility, Table 19 maps the identified implementation challenges to available enabling technologies. The analysis indicate that most technical barriers can be addressed using existing security technologies and industry practices. Technologies such as hardware roots of trust, firmware attestation, and PKI lifecycle management are already mature and deployed in adjacent domains, including ***V2X, DERMS***, and ***Plug&Charge*** ecosystems. Consequently, the primary challenges are not technological but relate to standardization, governance, regulatory alignment, and stakeholder coordination across EV charging infrastructures.

Table 19: Challenges and Enabling Technologies for TSM Deployment

Challenge	Impact on TSM Deployment	Enabling Technology / Mitigation Approach
HRoT Availability	Existing EVSE controllers may not provide hardware-rooted identities or secure attestation capabilities.	TPM 2.0, Infineon OPTIGA, Microchip ATECC608, NXP SE050/SE051 secure elements, or bump-in-the-wire security gateways.
Firmware Signing Supply Chain	Current firmware update processes do not support delegated trust between OEMs and trusted authorities.	Dual-signing frameworks, secure boot architectures, firmware attestation pipelines, and trusted firmware repositories.
Protocols and Standards	Existing OCPP, ISO 15118, and OpenADR standards lack native trust mediation interfaces.	Standardized TSM mediation hooks, security event reporting, policy enforcement profiles, and trust-state extensions.
Large-Scale PKI Lifecycle Management	Managing certificate issuance, revocation, rotation, and transparency at scale introduces significant operational complexity.	HashiCorp Vault PKI, Step-CA, EJBCA, certificate transparency logs, automated certificate lifecycle management.
Processing Overhead Constraints	Additional trust scoring, attestation, and policy validation may increase computational requirements.	Edge-based TSM kernels, cloud-assisted verification services, hardware acceleration, and optimized attestation workflows.
Cross-Border Interoperability	Trust enforcement across roaming eMSP and CPO ecosystems requires shared trust frameworks.	Federated trust models, OCPI trust federation, mutual recognition agreements, and cross-domain certificate authorities.

3.10 Summary

This section presents the implementation and experimentation results of the TSM within the EVSE–grid co-simulation environment. It describes the deployment architecture, runtime integration, and structured validation framework used to evaluate TSM enforcement behaviour. The architecture follows a layered, event-driven, and fail-secure-by-default design, ensuring deterministic execution and reproducibility. TSM mediates firmware updates, grid commands, and actuator operations through a sequential verification pipeline that includes hashing, signature validation, certificate chain checks, revocation verification, anti-rollback protection, bounded writing, and secure boot re-validation. Observability is achieved through telemetry streams, protocol traces, and audit logs, enabling evaluation across cybersecurity enforcement, EVSE operational behaviour, and grid-level stability impacts.

4 Insights

This project provides strategic insights into the cybersecurity resilience of Australia's rapidly expanding Electric Vehicle Supply Equipment (EVSE) and Distributed Energy Resource (DER) ecosystem. The findings demonstrate that EVSE security must be treated as a matter of national energy stability rather than isolated device protection. Through threat modelling, architectural design, and cyber–physical co-simulation, the project identifies systemic risks that could affect grid reliability under high DER penetration. The insights presented here outline practical, sovereign-aligned mechanisms for strengthening device-level assurance, regulatory oversight, and long-term grid stability in Australia's electricity transition.

4.1 Security Threats to EVSE Infrastructure

The threat modelling phase revealed that electric vehicle charging infrastructure introduces systemic cyber–physical risks that extend beyond individual devices and directly affect grid stability. When deployed at scale, charging stations operate as high-power, controllable distributed energy resources connected to distribution feeders and coordinated through backend platforms. Under high penetration scenarios, weaknesses in device architecture, firmware control, and communication trust can amplify into stability and reliability concerns for the broader electricity system. The key threat insights identified include:

- Firmware update pathways as fleet-scale compromise vectors
- Lack of enforced separation between communication logic and physical power control
- Weak certificate validation and backend impersonation risks
- Supply chain and commissioning vulnerabilities
- Aggregation effects that transform device compromise into grid-level disruption

Firmware Integrity as a Systemic Risk

One of the most critical findings was the exposure of firmware update mechanisms. Remote update channels, if not cryptographically enforced and independently verified, create high-impact attack surfaces. A compromised backend or malicious firmware image can propagate across an entire fleet of charging stations. At scale, coordinated manipulation of charging loads could trigger abrupt demand shifts, feeder overload conditions, or destabilising frequency excursions. Firmware integrity must therefore be viewed as a grid-stability control rather than an isolated software safeguard.

Architectural Flatness

The analysis identified structural weaknesses in conventional designs where communication stacks, application logic, and physical contactor controls reside within the same trust boundary. This architectural flatness enables escalation from network-layer compromise to physical-layer manipulation. An attacker exploiting a communication vulnerability can directly influence charging profiles or power dispatch behaviour. Across a fleet, such manipulation could generate oscillatory load patterns or disrupt demand-response coordination.

Backend Trust and Command Validation Weaknesses

Improper certificate validation, authentication bypass conditions, and insufficient command verification create risks in distributed orchestration environments. Weak validation of dispatch instructions allows impersonation of trusted backend systems or injection of manipulated control signals. In a networked distributed energy ecosystem, this creates the potential for coordinated load perturbation and grid instability.

Supply Chain Challenges in the EVSE ecosystem

Electric vehicle charging infrastructure relies heavily on globally sourced hardware and firmware, introducing inherent security uncertainty at the device level. Common weaknesses include hard-coded credentials, unsecured management interfaces, unsigned firmware, and exposed peripheral ports. These issues increase the likelihood of compromise both during deployment and throughout operational life. Given the high proportion of imported charging hardware, sovereign visibility into device integrity remains limited. Trust established at commissioning does not guarantee ongoing compliance or authenticity. As deployment scales, the absence of continuous device-level verification becomes a systemic governance and stability concern rather than a local technical issue.

4.2 Aggregation Effect: From Device Risk to Grid Risk

Large-scale deployment of electric vehicle charging as part of the DER ecosystem fundamentally alters the risk profile of charging infrastructure. As EVSE assets increasingly operate alongside rooftop solar, battery systems, and demand response programs, they become active participants in grid dynamics rather than passive loads. While a single compromised charger may have a limited operational impact, coordinated manipulation of thousands of devices can generate demand shifts comparable to large industrial loads or distributed generation assets. The analysis demonstrated that under high DER penetration conditions, charging fleets effectively behave as distributed, controllable grid resources. Malicious synchronised behaviour can introduce feeder stress, voltage instability, and balancing challenges across the distribution network. Device-level compromise can therefore escalate into systemic grid exposure. Charging infrastructure must consequently be treated as critical grid-connected DER assets requiring enforceable device-level trust guarantees rather than conventional consumer-grade security controls.

Key implications for the Australian Electricity Sector:

- EVSE fleets must be recognised as Grid-interactive DERs rather than passive consumer systems.
- Device-level cybersecurity assurance directly influences distribution network stability under high penetration scenarios.
- Grid planning and DER integration frameworks should incorporate adversarial load-manipulation modelling.
- Firmware integrity and command validation must be treated as grid-reliability controls.
- Sovereign verification mechanisms are required to ensure the ongoing integrity of imported charging hardware.

- Regulatory standards should mandate enforceable trust boundaries within grid-connected charging devices.

4.3 Sovereign Assurance Requirements

The risk patterns identified during the threat modelling exercise highlighted firmware integrity and trust as key challenges originating form EVSE supply chain and a lack of secure by design practices. This demonstrates that the conventional cybersecurity practices with less focus on DERs grid connectivity and EVSE design and governance principles need to be enhanced, considering the cyber-physical complexity of these systems. A core lesson from this project is that device-level trust (EV charging station) must be enforceable, non-bypassable, and should be independently verifiable. Security controls implemented solely within application software and communication stacks cannot guarantee containment once a compromise occurs. Structural separation between communication logic and physical power control is required to prevent escalation from network-layer compromise to Grid-impacting behaviour. The architectural response explored in this project demonstrates that enforceable security controls at the architectural level can operate as grid-reliability safeguards rather than optional cybersecurity features. By embedding independent verification layers within charging devices, escalation pathways can be structurally constrained even under adversarial conditions.

From an Australian Electricity transition perspective, this signals a shift towards sovereign-aligned assurance mechanisms. As DERs penetration accelerates, regulatory and planning frameworks must incorporate:

- Enforce device-level integrity, applying security by design principles.
- Integrity verification and validation at each layer of the local device, from firmware to operational control.
- Enforce attestation capabilities for remote compliance verification.
- Design level containment of escalation pathways instead of only focusing on runtime monitoring.

The project demonstrates that these requirements are technically feasible and operationally compatible with distributed coordination platforms. More importantly, they are necessary to ensure that the rapid electrification of transport does not introduce unmanaged systemic exposure into the national grid.

5 Future work

AR-PST Topic 9 (DER and Stability) has made significant progress in advancing dynamic modelling, inverter behaviour analysis, and weak-grid performance assessment, thereby strengthening the physical stability foundations of Australia's high-DER transition. However, as DER ecosystems become increasingly digitalised, cybersecurity must be recognised not simply as an IT issue, but as a material driver of dynamic system stability. Thus, future research under Topic 9 should systematically integrate advanced threat modelling, cyber-physical security analysis, and resilience within stability assessment and planning frameworks, discussed in the following subsections.

5.1 AR-PST Topic 9 (DER and Stability)

While AR-PST Topic 9 (DER and Stability) prioritises enhanced DER dynamic modelling and inverter behaviour analysis under weak-grid conditions to maintain system security [16, 17], the rapid digitalisation of DER ecosystems introduces an additional and increasingly material dimension of risk: cybersecurity-driven instability. Modern DER fleets depend on ICT-enabled control architectures, aggregation platforms, cloud-based coordination, and remote fleet management systems. This evolving cyber layer fundamentally alters the stability landscape, creating new pathways through which cyber can propagate into physical system disturbances.

Stage 4 and Stage 5 reporting documents substantial progress in DER interaction studies, hardware testing, and modelling improvements that strengthen the physical stability evidence base [16, 17]. However, from a cyber-physical systems perspective, several structural gaps remain that warrant targeted research attention:

A. **Limited cyber-physical threat modelling within Topic 9.**
   Current Topic 9 reporting is not structured around explicit attacker models, compromise pathways, or cyber-physical causality frameworks that systematically map cyber incidents to stability outcomes. The absence of adversarial scenario modelling limits the ability to assess cybersecurity-driven stability risks alongside conventional disturbance analysis [16, 17].
B. **Governance, incident response, and recovery for DER ecosystems.**
   Existing AR-PST stability work does not yet articulate research directions for coordinated response and recovery operating models for DER operators and aggregators during cyber-induced stability events and incidents. This is despite the presence of broader sector governance frameworks, such as the AESCSF, that provide high-level cyber guidance but are not yet operationalised within DER stability contexts [18, 5, 44].
C. **Standards and assurance mechanisms at the DER edge.**
   As DER ecosystems decentralise, the need for cybersecurity standards, certification pathways, and security-by-design integration at the device and inverter level becomes increasingly critical. Australian grid cybersecurity road-mapping emphasises coordinated standards uplift, and international guidance (including NIST-aligned practices) provides relevant security patterns. However, the integration of these mechanisms into stability-aware DER frameworks remains underdeveloped [19].

Addressing these gaps will require a coordinated cyber-physical research agenda that integrates stability analysis, threat modelling, governance design, and standards development to ensure DER-driven decarbonisation proceeds without introducing systemic cyber-induced instability risks.

5.2 Future Research Work Opportunities

A key opportunity is the progression of the 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 also be directly linked to national policy developments through collaboration with the Department of Home Affairs and the 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 also examine how future national infrastructures, such as the emerging DER registry and the national PKI ecosystem, can incorporate device-level attestation and trust signals to improve whole-of-system visibility, assurance, and operational coordination. This would support addressing control and visibility constraints around the “hidden market participants” that are responsive to pricing incentives.

Topic 9 research should also explore how future national infrastructures, such as the emerging DER registry and the national PKI ecosystem, can incorporate device-level attestation and trust signals to strengthen whole-of-system visibility.

Finally, as Australia approaches 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.

These research directions establish a cyber-physical stability framework for high-DER grids, treating cybersecurity not only as a confidentiality, integrity, and availability (CIA) issue, but as a driver of dynamic system instability. The following topics address both near-term translation and long-term national resilience needs.

1. Cyber-Physical Threat Propagation Through DER, Aggregator, DERMS, and VPP Architectures

While a single DER compromise may have minimal impact, coordinated attacks on a substantial proportion of DERs — effectively forming a DER botnet — pose significant risks to area power system reliability. DER ecosystems are increasingly coordinated through aggregators, DERMS, and VPP platforms that rely on hierarchical communication architectures. These architectures create systemic coupling between thousands of distributed devices. A compromise at one node, or at the aggregator control layer, may propagate across fleets, enabling synchronised setpoints, coordinated disconnections, manipulation of inverter parameters, firmware updates, ride-through and trip thresholds, or induced oscillatory behaviour.

Current cyber risk assessments often focus on device-level vulnerabilities or perimeter security, but insufficiently address how architectural design, communication topology, and aggregator security posture influence attack propagation pathways and system-level impact. Current DER stability research similarly does not yet model attacker-induced propagation pathways within these architectures in a way that links compromise to stability outcomes.

Why It Matters for Stability

Coordinated malicious DER behaviour can directly degrade:

- Frequency stability
- Voltage margins in weak grids
- Small-signal oscillatory damping
- Protection coordination during disturbances
- Area reliability through cascading outages or power quality effects

Key research questions

- How does grid architecture and DER aggregator security posture influence the likelihood, propagation, and system-level impact of cyber intrusions originating at compromised DER assets?
- How can attacker-induced propagation pathways be modelled across hierarchical device–aggregator–grid architectures?
- What resilient design strategies (e.g., trust zones, segmentation, redundancy, distributed enforcement) can constrain systemic instability?

Research Directions

Develop hierarchical device–aggregator–grid cyber-physical threat models; apply graph-theoretic propagation analysis and stability sensitivity assessment; integrate cyber-induced behavioural changes into dynamic simulations; and develop an architecture-based cyber risk assessment framework that models attack propagation from compromised DER devices through aggregators and into upstream grid control systems, while proposing resilient design strategies that limit systemic impact.

2. Cyber-Resilient Grid-Forming Inverter Control and Stability Limits in High Inverter-Based Resource Penetration Power Systems

As inverter-based resources (IBRs), grid-forming inverters (GFMIs), and inverter-based loads (IBLs) increasingly replace synchronous machines, system strength, fault response, frequency stability, and voltage control are becoming software-defined. This digitalisation exposes the power system

to new cyber-physical vulnerabilities. GFMIs rely on firmware-based control (droop, virtual oscillator, VSG, predictive control). Cyber manipulation of frequency droop coefficients, virtual inertia constants, fault current limits, protection settings could destabilise the system.

Why It Matters for Stability

- Power system stability is now software-defined.
- Grid-forming inverters replace synchronous machines, making frequency and voltage control digitally controlled—and therefore cyber-exposed.
- High IBR penetration reduces physical inertia, meaning small malicious perturbations can cause disproportionate system-wide instability.
- Weak-grid regions are more vulnerable, where control errors or manipulated parameters can rapidly escalate into cascading failures.
- Existing stability studies ignore adversarial conditions, potentially overestimating secure IBR penetration limits.

Key research questions

- How can grid-forming and inverter-based resources be designed, modelled, and standardised to ensure cyber-resilient operation under weak-grid and high-penetration conditions, particularly against false data injection (FDI), denial-of-service (DoS), parameter tampering, and coordinated wide-area cyber-attacks?
- What is the impact of coordinated FDI attacks on grid-forming droop control in weak-grid conditions?
- How do DoS attacks on wide-area measurement systems affect transient instability? Can AI-driven predictive control remain stable under adversarial input perturbations?
- What are the cyber-induced limits to IBR penetration in the NEM?

Research Directions

Develop a cyber-physical stability framework for inverter-dominated power systems by embedding cybersecurity directly into grid-forming inverter (GFMI) modelling, control, and planning. Construct integrated models that incorporate communication layers, firmware-level control logic, and adversarial attack vectors (e.g., false data injection, denial-of-service, and parameter tampering) within transmission-level networks. Develop resilient control and detection strategies to define cyber-aware IBR limits and inform secure grid-forming standards.

3. Stability-Aware Incident Response, Recovery, and Resilience Engineering for DER Operators

DER operators and aggregators lack stability-aware cyber incident response models. While sector frameworks (e.g., AESCSF) provide maturity benchmarks, they do not specify how cyber incidents affecting DER fleets should be detected, isolated, and recovered at an operational level while preserving dynamic system security.

Why It Matters for Stability

Delayed detection or poorly coordinated response may:

- Prolong frequency deviations
- Delay voltage restoration
- Trigger cascading disconnections
- Disrupt protection logic under abnormal flows

Key research questions

- How can DER cyber incidents be detected and classified in ways that are meaningful for fleet operations and power system stability?
- What response and recovery strategies enable containment of compromised DER fleets while maintaining dynamic system security?
- How can restoration approaches (e.g., staged reconnection) be designed to support secure recovery without inducing further instability?

Research Directions

Define DER-specific incident taxonomies (e.g., coordinated ramp events, ride-through manipulation, fleet-level disconnections); develop stability-aware detection linked to frequency and voltage signals; model-controlled recovery strategies such as staggered reconnection; and quantify performance using restoration time, voltage recovery, and damping metrics.

4. Secure, Coordinated, and Grid-Aware Firmware Updating and Lifecycle Governance for DER Fleets

Current DER standards (e.g., CSIP-AUS) lack scalable, grid-aware secure update frameworks tailored for aggregated fleets. DER fleets require firmware updates for performance and compliance, but the mass rollout of updates can unintentionally modify aggregated dynamic characteristics. Compromised update channels can also introduce malicious logic at scale. A poorly coordinated mass update could disrupt aggregated power output, affect voltage or frequency stability, violate market obligations, or introduce systemic cyber vulnerabilities.

Why It Matters for Stability

Firmware changes can alter:

- Ramp rates
- Reactive power support
- Ride-through thresholds

- Frequency response behaviour

Key research questions

- How can DER aggregators securely, reliably, and economically deploy large-scale software/firmware updates across heterogeneous, multi-owner DER fleets participating in wholesale markets—without compromising grid stability or creating new cyber vulnerabilities?
- How can aggregators validate firmware integrity independently of vendors, and what options are available through certification schemes arising from IoT labelling standards and certification regimes?
- How should update sequencing and rollout strategies be constrained to preserve stability and market obligations?
- How does partial DER compromise affect wholesale market clearing, ancillary services, and price stability during remediation and lifecycle operations?

Research Directions

Develop a cyber-resilient, grid-aware framework for secure mass firmware updates in DER/CER aggregator fleets, noting that some aggregators already control DER updates from certain providers; model firmware-induced behavioural changes in inverter dynamics; develop stability-constrained rollout strategies (phased, state-aware updates); formalise cryptographic assurance with independent integrity validation; simulate aggregate behavioural impacts on frequency and voltage; and establish governance principles linking lifecycle control to stability thresholds. This should be complemented by a dynamic, system-aware cyber risk assessment framework that quantifies operational and economic impacts of partial DER compromise, including standardized risk metrics, probabilistic risk assessment integrated with power system stability analysis, and cyber-physical digital twin models for scenario testing.

5. Aggregator and Energy Market Interface Security, Including False Data Injection and DOE Misuse

The operation of modern energy markets relies on the real-time exchange of data packets across communication networks for pricing, dispatch, and settlement. Aggregators interact with energy and ancillary service markets, and compromise of dispatch optimisation algorithms or measurement integrity can distort balancing signals and degrade reserve provision. These data flows and interfaces are vulnerable to cyberattacks, particularly false data injection (FDI), telemetry manipulation, and optimisation compromise. As markets integrate high levels of DER and automated controls such as Dynamic Operating Envelopes (DOEs), attackers may manipulate or spoof market information to influence economic incentives, disrupt operations, or subvert DOE-based control and market mechanisms.

This study should sit alongside work on DOE in Topic 8 and identify threats and suitable controls that protect the emerging use of DOEs across Australia, including both supply-side and emerging consumption-side DOEs.

Why It Matters

Compromised market participation and communications may result in:

- Incorrect market clearing and settlement
- Financial losses and distorted incentives
- Under-delivery of frequency containment and ancillary services
- Voltage violations due to incorrect dispatch
- Reduced balancing capability during disturbances

Key research questions

- How can energy market communication systems and aggregator market interfaces be secured against false data injection attacks to ensure accurate, reliable, and resilient market operation under high DER penetration and automated grid control?
- How can Dynamic Operating Envelopes be mis-used to distort the market, considering both supply and emerging consumption DOEs?
- How does partial DER compromise affect wholesale market clearing, ancillary services, and price stability?
- How can secure optimisation and dispatch integrity be maintained while preserving stability outcomes?

Research Directions

Develop a cyber-resilient framework for energy market communications and aggregator interfaces capable of detecting, mitigating, and preventing false data injection attacks while ensuring stable, reliable market and grid operations; model the market-dispatch-to-dynamic-response chain; introduce adversarial manipulation into optimisation algorithms; quantify impacts on FCAS performance and frequency containment; develop secure optimisation frameworks with authenticated dispatch and stability-constrained bidding; and link market integrity metrics directly to physical stability outcomes.

6. Cybersecurity Risks in Microgrid Control Systems (AC and DC)

Microgrids are small-scale power systems capable of operating in both grid-connected and islanded modes. They are increasingly deployed to integrate renewable energy resources. Their operation depends heavily on communication between system components and controllers, making them vulnerable to cyberattacks. In AC microgrids, Remote Terminal Units (RTUs) transmit operational data to controllers, which could be falsified by attackers. In DC microgrids, voltage and current measurements sent to controllers or used by current differential relays can also be manipulated. Such falsified data may destabilize the microgrid, interfere with protection schemes, or disrupt power sharing between resources.

Why It Matters for Stability

Manipulated measurement data in AC and DC microgrids can lead to:

- Voltage, frequency, and power-sharing instability, compromising operational reliability.
- Protection maloperation or failure-to-trip events, increasing risk of equipment damage and cascading faults.
- Severe impact on inverter-dominated systems, which rely heavily on accurate real-time measurements.

Key research questions

- How can microgrid control and protection systems be secured against falsified measurement data to prevent cyber-induced instability in both AC and DC microgrids?
- Develop a cyber-resilient framework for AC and DC microgrids, securing communication and measurement data, and ensuring stable operation under both normal and adversarial conditions.

7. Cybersecurity Risks and Resilience of Power System Control Algorithms and Platforms (Control Centres and Cloud-Based Control)

Control centre operations are critical to power system monitoring, analysis, and decision-making, relying heavily on data received from sensors, SCADA systems, and forecasting inputs. These algorithms include state estimation, power flow, load forecasting, and EMS computations, and are vulnerable to cyberattacks where attackers falsify measurements or input data to manipulate system behaviour without immediate detection.

As modern power systems evolve, an increasing portion of control, monitoring, and analytics functions is migrating to cloud-based platforms. Cloud integration offers benefits such as scalability, real-time data processing, remote management, and advanced optimization for DERs, microgrids, and energy markets. However, this shift introduces additional cybersecurity risks because critical

grid operations depend on externally hosted infrastructure, increasing exposure to unauthorized access, data integrity compromise, service disruption, and supply chain vulnerabilities.

Why it Matters

- Incorrect state estimation, masking instability conditions
- Inappropriate dispatch and remedial actions, exacerbating voltage deviations
- Delayed contingency detection, reducing damping and response effectiveness
- Distorted DER coordination, leading to unstable aggregate behaviour
- Loss of secure fallback capability, impairing and disrupting control continuity

Key research questions

- How can control centre algorithms, including state estimation, power flow, load forecasting, and EMS computations, be secured against falsified data to ensure accurate monitoring and reliable decision-making in the power system?
- How can cloud-based power system control platforms be designed and secured to ensure resilient, real-time operation of critical grid functions, while mitigating cyber threats, unauthorized access, and data integrity compromises?
- How can control continuity and secure fallback be maintained when cloud services are degraded or unavailable?

Research Directions

Develop a cyber-resilient framework for control centre algorithms and cloud-based power system control that detects, mitigates, and withstands falsified data attacks; ensures accurate state estimation, power flow analysis, load forecasting, and EMS operations; and supports secure, reliable, and real-time operation of grid functions while addressing threats from data manipulation, unauthorized access, service disruption, and supply chain vulnerabilities.

8. Cybersecurity Vulnerabilities in Power System Communication Networks

Communication networks are critical to modern power system operations, enabling data exchange between devices, controllers, and control centres using standard protocols. However, these networks are vulnerable to cyberattacks, including false data injection (FDI), denial-of-service (DoS), and GPS spoofing, which can compromise the accuracy, timing, and integrity of transmitted data. Data packets transmitted over protocols such as IEC 61850, TCP/IP, and GOOSE can be falsified or intercepted. GPS signals used for precise timing can be spoofed, affecting synchronization-dependent operations.

This has been identified by Office of National Security (ONS) and the European Union [7] as a research priority for existing energy networks, and the increased distributed generation through DER is likely to further exacerbate this reliance and it is not clear how the developing Australian market is exposed to these threats.

Why it matters

Cyber vulnerabilities in power system communication networks can lead to:

- Loss of data integrity and timing accuracy, resulting in incorrect control and protection actions.

- Widespread operational disruption from FDI, DoS, or GPS spoofing attacks affecting multiple grid devices simultaneously.
- Compromised synchronization-dependent functions, such as wide-area monitoring and differential protection.
- Uncertain vulnerability of the evolving Australian electricity market stability, requiring targeted assessment and mitigation strategies

Key research questions

- How can power system communication networks be secured against FDI, DoS, and GPS spoofing attacks while maintaining reliable, accurate, and timely data exchange across grid devices and control systems?
- Develop a cyber-resilient framework for power system communication networks that ensures secure, accurate, and timely data exchange, mitigates FDI, DoS, and GPS spoofing attacks, and protects connected control and protection devices from compromise.

9. EV Charging and V2G Cybersecurity and Stability

EVSE and V2G systems introduce bidirectional power flows with rapid, aggregated response characteristics. Manipulated charging schedules or dispatch instructions can create synchronised load spikes or injection surges. These systems are increasingly network-connected and remotely managed.

Why It Matters for Stability

Coordinated EV charging manipulation can cause:

- Rapid frequency dips
- Feeder overvoltage
- Oscillatory instability in weak grids
- Transformer overload and protection tripping

Key research questions

- How can EVSE and V2G systems be secured against manipulation of charging schedules, dispatch instructions, and coordinated fleet behaviour?
- What are the worst-case stability impacts of synchronised charging or injection across aggregated EV fleets?
- What stability-aware control constraints and enforcement mechanisms can reduce cyber-induced instability?

Research Directions

Develop EVSE/V2G-specific attack models (charging manipulation, dispatch compromise); integrate fleet dynamics into grid simulations; quantify worst-case synchronised load impacts; design stability-aware control constraints (rate limiting, enforced dispatch); and evaluate mitigation through dynamic simulation and hardware-in-the-loop validation.

10. Cybersecurity Standards, Certification, and Architectural Guidelines for Stability-Critical DER

Current DER standards (e.g., IEEE 1547) emphasise physical interconnection performance but do not fully embed cybersecurity requirements tied to stability. Australian grid cybersecurity roadmaps emphasise coordination and governance, but stability-specific security criteria remain fragmented.

Why It Matters for Stability

Non-uniform security practices can enable:

- Coordinated exploitation of homogeneous firmware
- Weak authentication across fleet control
- Increased probability of large-scale disconnections

Key research questions

- What stability-relevant cybersecurity requirements are missing or insufficiently defined in current DER and aggregator standards?
- What minimum security baselines and architectural guidance should apply to stability-critical DER fleets and aggregator platforms?
- How can certification and assurance approaches incorporate stability-relevant cyber-physical criteria?

Appendix-A

Report Name	Description	Link (Available through CSIRO)
Technical Report 1	EVSE Threat Modelling Report	Phase 1 - TR1 - EVSE Threat Analysis Report_V1.5_Final.pdf
Technical Report 2	TSM Reference Architecture	Phase 1 - TR2 - TSM Reference Architecture_V1.5_Final.pdf
Project Report (Phase 2)	Co-Simulation Platform Development	Phase 2 - PR1 - EVSE Cosimulation Platform Development V1.51_Final.pdf
Technical Report 3	POC for TSM- Implementation and Experimentation	

References

[1] Australian Energy Market Operator (AEMO), Integrated System Plan (ISP) – 2026 Draft, Melbourne, Australia, Dec. 2025. [Online]. Available: https://www.aemo.com.au/energy-systems/major-publications/integrated-system-plan-isp

[2] AEMO, EV Technical Standards for Grid Operation – Insights for the NEM, Melbourne, VIC, Australia, Dec. 2023. [Online]. Available: https://www.aemo.com.au/-/media/files/initiatives/engineering-framework/2023/enx---ev-technical-standards-for-grid-operation---insights-for-the-nem.pdf. [Accessed: Feb. 2026].

[3] Australian Energy Market Operator (AEMO), EV Technical Standards for Grid Operation – Insights for the NEM, Melbourne, VIC, Australia, Dec. 2023. [Online]. Available: https://www.aemo.com.au/-/media/files/initiatives/engineering-framework/2023/enx---ev-technical-standards-for-grid-operation---insights-for-the-nem.pdf . [Accessed: Sep. 2025].

[4] S. Abedi, A. Arvani, and R. Jamalzadeh, “Cyber security of plug-in electric vehicles in smart grids: Application of intrusion detection methods,” in Smart Grid Security: An End-to-End View of Security in the New Electrical Grid, Cham, Switzerland: Springer, 2015, ch. 5, doi: 10.1007/978-981-287-299-9_5.

[5] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis and C. Douligeris, "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)," in IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1504-1533, thirdquarter 2022, doi: 10.1109/COMST.2022.3184448.

[6] J. Johnson, J. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt, T. Carroll, L. Ross O’Neil, B. Dindlebeck, P. Maloney, J. O’Brien, D. Gotthold, R. Varriale, T. Bohn, and K. Hardy, “Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses,” Energies, vol. 15, no. 11, p. 3931, 2022, doi: 10.3390/en15113931.

[7] P. Kumar, H. K. Channi, R. Kumar, A. Rajiv, B. Kumari, G. Singh, S. Singh, I. F. Dyab, and J. Lozanović, “A comprehensive review of vehicle-to-grid integration in electric vehicles: Powering the future,” Energy Conversion and Management: X, vol. 25, 100864, 2024, doi: 10.1016/j.ecmx.2024.100864.

[8] A. Sanghvi, Cybersecurity for Electric Vehicle Fast-Charging Infrastructure, NREL/TP-6A40-75236, National Renewable Energy Laboratory (NREL), Golden, CO, USA, 2021. [Online]. Available: https://docs.nrel.gov/docs/fy21osti/75236.pdf . [Accessed: Oct. 2025].

[9] S. B. Mitikiri, K. V. S. M. Babu, D. Dwivedi, V. L. Srinivas, P. Chakraborty, P. K. Yemula, and M. Pal, “Cyber–physical security in EV charging infrastructure: Components, vulnerabilities, and defense strategies,” Sustainable Energy Technologies and Assessments, vol. 81, p. 104435, 2025.

[10] S. Hamdare, S. P. Pawar, and S. S. Sambare, “Cybersecurity risk analysis of EV charging systems,” Sensors, vol. 23, no. 14, p. 6345, 2023, doi: 10.3390/s23146345.

[11] Open Charge Alliance, Open Charge Point Protocol (OCPP) Overview, Arnhem, The Netherlands, 2020. [Online]. Available: https://openchargealliance.org/protocols/open-charge-point-protocol/ . [Accessed: Sep. 2025]

[12] International Organization for Standardization (ISO), ISO 15118 – Road Vehicles – Vehicle to Grid Communication Interface, Geneva, Switzerland, 2019.

[13] International Electrotechnical Commission (IEC), IEC 62196 – Conductive Charging of Electric Vehicles, Geneva, Switzerland, 2016.

[14] European Union Agency for Cybersecurity (ENISA), Threat Landscape for Supply Chain Attacks, Athens, Greece, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks . [Accessed: Feb. 2026]..

[15] Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australian Research in Power Systems Transition (AR-PST). [Online]. Available: https://www.csiro.au/en/research/technology-space/energy/electricity-transition/ar-pst . [Accessed: Oct. 2025].

[16] Commonwealth Scientific and Industrial Research Organisation (CSIRO), Topic 9 – DER and Stability: Stage 4 Interim Report, Canberra, ACT, Australia, 2024. [Online]. Available: https://www.csiro.au/-/media/EF/Files/GPST-Roadmap/Topic-9-DER-and-Stability-Final-Report-with-alt-text-2.pdf . [Accessed: Aug. 2025].

[17] CSIRO, AR-PST Stage 4 Topic 9 Final Report, Canberra, Australia, 2024.

[18] Australian Government, Department of Climate Change, Energy, the Environment and Water (DCCEEW), Australian Energy Sector Cyber Security Framework (AESCSF), Canberra, Australia.

[19] Energy Networks Australia and CSIRO, Grid Cyber Security Roadmap, Canberra, Australia, 2018.

[20] A. Shostack, Threat Modeling: Designing for Security. Indianapolis, IN, USA: Wiley, 2014.

[21] MITRE Corporation, “MITRE ATT&CK® for Industrial Control Systems (ICS),” 2024.

[22] P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable, graph-based network vulnerability analysis,” in Proc. 9th ACM CCS, Washington, DC, USA, 2002, pp. 217–224.

[23] National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, NIST SP 800-30 Rev. 1, Gaithersburg, MD, USA, 2012.

[24] Microsoft, “Microsoft Threat Modeling Tool overview,” 2025. [Online]. Available: https://learn.microsoft.com

[25] NIST, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, SP 800-160 Vol. 1 Rev. 1, 2022.

[26] Y. Mo et al., “Cyber–physical security of a smart grid infrastructure,” Proc. IEEE, vol. 100, no. 1, pp. 195–209, 2012.

[27] P. Palensky et al., “Cosimulation of intelligent power systems,” IEEE Ind. Electron. Mag., vol. 11, no. 1, pp. 34–50, 2017.

[28] T. D. Hardy et al., “HELICS: A co-simulation framework for scalable multi-domain modeling and analysis,” IEEE Access, vol. 12, pp. 24325–24347, 2024.

[29] CSIRO, AR-PST Guidance Document for Stage 5 RFQ, Canberra, Australia, 2024.

[30] Australian Energy Market Operator, EV Technical Standards for Grid Operation: Insights for the NEM, 2023.

[31] Department of Climate Change, Energy, the Environment and Water (DCCEEW), Minimum Operating Standards for Government-Supported Public EV Charging Infrastructure, 2024.

[32] Electric Vehicle Council, EV Charging at Home Guide, 2023.

[33] Fleet EV News, “Australia’s charging network expands rapidly: Exclusive data reveals 8.5% growth in Q2 2025,” 2025. [Online]. Available: https://fleetevnews.com.au/australias-charging-network-expands-rapidly-exclusive-data-reveals-8-5-growth-in-q2-2025/ . [Accessed: Feb. 2026].

[34] A. R. Singh et al., “Electric vehicle charging technologies, infrastructure expansion, grid integration strategies, and their role in promoting sustainable e-mobility,” Alexandria Engineering Journal, vol. 105, pp. 300–330, 2024, doi: 10.1016/j.aej.2024.07.026..

[35] M. Boucetta et al., “The architecture design of electrical vehicle infrastructure using viable system model approach,” Systems, vol. 9, no. 1, p. 19, 2021, doi: 10.3390/systems9010019..

[36] I. Skarga-Bandurova et al., "Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 3099-3106, doi: 10.1109/BigData55660.2022.10020644.

[37] A. Kaur et al., “Cybersecurity challenges in the EV charging ecosystem,” ACM Computing Surveys, vol. 58, no. 1, Art. no. 14, pp. 1–32, Jan. 2026, doi: 10.1145/3735662..

[38] Australian Energy Market Operator (AEMO), Integrated System Plan (ISP), Melbourne, VIC, Australia, 2022. [Online]. Available: https://www.aemo.com.au/-/media/files/major-publications/isp/2022/2022-documents/2022-integrated-system-plan-isp.pdf .

[39] J. Menyhart, “Electric vehicles and energy communities: Vehicle-to-grid opportunities and a sustainable future,” Energies, vol. 18, no. 4, p. 854, 2025, doi: 10.3390/en18040854.

[40] R. Metere, Z. Pourmirza, S. Walker, and M. Neaimeh, “An overview of cyber security and privacy on the electric vehicle charging infrastructure,” arXiv preprint, arXiv:2209.07842, 2022. [Online]. Available: https://arxiv.org/abs/2209.07842

[41] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, “Cybersecurity of smart electric vehicle charging: A power grid perspective,” IEEE Access, vol. 8, pp. 214434–214453, 2020, doi: 10.1109/ACCESS.2020.3038811.

[42]. Electric Power Research Institute (EPRI), “OpenDSS – Open Distribution System Simulator,” EPRI, Palo Alto, CA, USA. [Online]. Available: https://www.epri.com/pages/sa/opendss . [Accessed: Feb. 2026].

[43]. T. Aljohani and A. Almutairi, “A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods,” Defence Technology, vol. 42, pp. 31–58, Dec. 2024, doi: 10.1016/j.dt.2024.06.009

[44] Australian Energy Market Operator (AEMO), AESCSF Framework and Resources. Melbourne, VIC, Australia. [Online]. Available: https://www.aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources. [Accessed: Jan. 2026].

[45] Trusted Computing Group, “TPM Library Specification,” *Trusted Computing Group*, [Online]. Available: . [Accessed: 28-Apr-2026].

[46] Arm, “Platform Security,” *Arm Developer*, [Online]. Available: . [Accessed: 28-Apr-2026].

[47] National Security Agency (NSA) Cybersecurity, “Hardware and Firmware Security Guidance – Secure Boot,” *GitHub*, [Online]. Available: . [Accessed: 28-Apr-2026].

[48] National Institute of Standards and Technology (NIST), “Special Publication 800-193: Platform Firmware Resiliency Guidelines,” *NIST Computer Security Resource Center (CSRC)*, May 2018. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/193/final. [Accessed: 28-Apr-2026].

[49] HashiCorp, "PKI secrets engine (API)," HashiCorp Developer. [Online]. Available: . [Accessed: 28-Apr-2026].

[50] Smallstep Labs, “step-ca Certificate Authority Overview,” *Smallstep Documentation*, [Online]. Available: . [Accessed: 28-Apr-2026].

[51] Keyfactor, “Download EJBCA – Get the Open-Source CA,” *EJBCA*, [Online]. Available: https://www.ejbca.org/download/. [Accessed: 28-Apr-2026].

[52] EVRoaming Foundation, “EVRoaming Foundation – Realising cross-border charging,” *EVRoaming*, [Online]. Available: . [Accessed: 28-Apr-2026].

[53] Hubject, “Plug&Charge | Seamless and secure charging,” *Hubject*, [Online]. Available: . [Accessed: 28-Apr-2026].

[54] CharIN, “Plug & Charge – Standardized and interoperable Plug & Charge services for secure EV charging,” *CharIN*, [Online]. Available: . [Accessed: 28-Apr-2026].

[55] CyberSEAS Consortium, “CyberSEAS – Cyber Securing Energy dAta Services,” *CyberSEAS*, [Online]. Available: . [Accessed: 28-Apr-2026].

As Australia's national science agency, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Creating a better future for everyone.

Contact us

1300 363 400
+61 3 9545 2176
csiro.au/contact
csiro.au

For further information (position for single contact only, delete if more and use below only)

Insert Research/Enterprise Unit name
Insert contact name
+61 0 0000 0000
first.last@csiro.au
csiro.au/xxx

For further information (position for up to four contacts, delete all if single contact and use above only)

Insert Research/Enterprise Unit name
Insert contact name
+61 0 0000 0000
first.last@csiro.au
csiro.au/xxx

Insert Research/Enterprise Unit name
Insert contact name
+61 0 0000 0000
first.last@csiro.au
csiro.au/xxx

Insert Research/Enterprise Unit name
Insert contact name
+61 0 0000 0000
first.last@csiro.au
csiro.au/xxx

Insert Research/Enterprise Unit name
Insert contact name
+61 0 0000 0000
first.last@csiro.au
csiro.au/xxx