International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

OTA Update Assurance for Energy and Charging Functions in SDVs

Abhishek Devgan

Senior QA Engineer

Abstract:
The *OTA software updates have become a standard feature of the current software-defined vehicles* (SDVs) and allow manufacturers to refine, patch, and improve vehicle functionality remotely across its lifecycle of operation. OTA updates have been applied successfully to infotainment and connectivity areas, but when applied to safety-critical energy and charging subsystems, such as battery management systems (BMS), vehicle charging management systems (VCMS), energy control units (ECUs) and vehicle-to-grid (V2G) interfaces, present a unique and challenging assurance challenge. The paper is an analytical discussion of the validation and rollback strategies that are implemented in OTA updates that have a direct impact on EV energy and charging operations. The assessment models, secure update models, formal verification models, and staged deployment models. The present state of the art, gaps in research, and the changing regulatory environment comprising of ISO 21434, UN R156, and the Uptane standard. The energy OTA updates demand multi-tier hardware-in-loop validation, cryptographically anchored rollback partitions, and compatibility checks at the ecosystem level, in addition to those needed by typical vehicle software. The research suggests a unified assurance framework consisting of the threat modelling, staged rollout governance and automated anomaly-based rollback that is to EV energy systems.

Keywords: Over-the-Air (OTA) Update, Software-Defined Vehicle (SDV), Battery Management System (BMS), Vehicle Charging Management System (VCMS), Rollback Strategy, Validation Framework, Electric Vehicle (EV), Vehicle-to-Grid (V2G), Uptane, Cybersecurity, ISO 21434, Staged Deployment, Firmware Update.

I. INTRODUCTION

The automotive sector is currently experiencing the change in basic assumptions of the mechanically controlled vehicles to the software-defined vehicles (SDVs), whereby the behaviour, performance and safety features of the vehicle are more controlled by software. The electrification of transportation has brought this change: the current electric car (EV) models have more than 100 electronic control units (ECUs) that execute tens of millions of lines of code [1]. The key feature of the SDV model is the capacity to execute over-the-air (OTA) software updates an option borrowed by mobile computing that allows manufacturers to provide new features, security patches, and compliance upgrades and have them installed without physical intervention in a dealership.

The OTA updates are well proven commercially feasible. According to industry observers, the software maintenance via OTA may save the automotive OEMs more than USD 35 billion every year by 2022 by removing the physical recalls [4]. Tesla, BMW, Volkswagen, and Kia have made high-profile deployments that have shown that OTA can be used to recall safety, improve vehicle range, and even provide vehicle to grid (V2G) energy services [2] [10] [13] [17]. But this very ability poses serious cybersecurity and functional safety threats especially when used in energy and charging subsystems which directly control the high voltage electrical energy flow in and around the vehicle [3] [4].

OTA updates in the energy domain of the BMS, VCMS, thermal management ECUs, and V2G communication modules, are radically different in nature, as compared to infotainment or navigation updates. Mistakes during such updates may negatively affect the battery performance, impact the safety

of the charging process, or provoke the inaccurate state-of-charge (SOC) estimation or, at the worst, lead to thermal runaway events [7] [10] [13] [14] [22]. Failure of BMS OTA not only causes inconvenience to the users, but can also lead to regulatory measures, recalls of products, and in the worst case, bodily injury. The stakes involved are explained by the 2021 GM Bolt EV battery fire incident that was partially resolved with the help of an emergency OTA charging limit reduction [17].

Although the energy-domain OTA update is critically important, the academic literature has largely concentrated on the cybersecurity of the OTA update transmission mediums, namely, encryption, authentication, and integrity checking [1] [6] [9] [16], but has given little attention to the validation strategy and rollback strategy of energy system updates. The current systems like Uptane [9], STRIDE [16], and Scal OTA [15] offer good backgrounds of making the updates delivery secure but fail to offer the domain-specific validation of BMS and VCMS firmware. Several standards exist such as ISO 21434 [1] and UN R156 [25] that define the requirements of cybersecurity engineering in vehicles but leave a lot of discretion in the implementation of the standards to OEMs in terms of assurance of update energy.

II. LITERATURE REVIEW

Mahmood, Nguyen, and Shaikh (2022): The model-based security testing framework and a systematic threat assessment methodology, specifically designed to assess the automotive OTA update systems. With the help of the STRIDE-based threat modelling applied to the cloud server to ECU update pipeline, the authors reveal a wide range of attack surface which includes the update package injection, the man-in-the-middle interception and the rollback attacks. One of the main conclusions is that the current testing of OTA security is largely informal and does not have a strict and repeatable approach. The identified gap in the research is that automated standards-compliant (ISO 21434) security test generation of energy-related ECU updates is missing [1].

Kirk, Nguyen, Bryans, Shaikh, and Wartnaby (2023): Extend the Uptane protocol and a model attacker into Communicating Sequential Processes (CSP) to generate exhaustive test cases with the formal model-based security testing framework of automotive OTA systems. The paper shows that testbed experiments identify vulnerabilities that are not identified using traditional penetration testing when formally derived test cases are used. The research gap that has been identified as critical is the lack of formal verification that is applied to energy-domain update protocols, namely, the lack of CSP or model-checking coverage of BMS and VCMS firmware update flows [2].

Mocnik, Fowler, and Maple (2023): The topic of vehicular OTA software upgrade systems results in a reference architecture and four-step threat analysis strategy that leads to actionable cybersecurity prescriptions. The research concludes that connectivity of vehicles is the most critical aspect in the growth of OTA attack surface, as more than 40 % of the literature studied found connectivity as a key issue of concern. The identified gap is the necessity of domain-specific threat modelling that is adjusted to the environment of high-voltage energy ECU and not to the environment of the vehicle network in general [3].

Halder, Ghosal, and Conti (2022): Presented a survey of secure OTA software update methods in connected vehicles, that is, more than 80 papers are reviewed, and solutions are classified by communication security, authentication methods, and verification of updates. One of the critical conclusions is that most of the suggested solutions are concentrated on the phase of the over-the-air transmissions and do not consider the opportunity to verify the post-installation and roll-back. The survey specifically points to the unavailability of domain-sensitive update validation, and especially safety-critical subsystems, like BMS, as a major open research issue [4].

Chowdhury, Lesiuta, Rikley, Lin, Kang, Kim, Shiraishi, Lawford, and Wassyng (2018): The first to present an analysis framework of automotive OTA updates through both the functional safety (ISO 26262) and cybersecurity (ISO/SAE 21434) perspectives on OTA update design. The paper suggests a combined HAZOP-STRIDE approach and illustrates its use to a typical powertrain ECU update situation. The gap

in the research is the fact that energy-specific state machine validation is not fully covered by the framework, and rollback trigger conditions based on BMS telemetry are not provided [5].

Kirk, Nguyen, Bryans, Shaikh, Evans, and Price (2021): The help of CSP, which allows generating security tests automatically and based on a specified attack model. The implementation of the testbed confirms that several the claims related to the Uptane attack resistance can be checked with the help of the model checking, and some of them demand some extra assumptions. The main gap in the research is that the security properties of Uptane have not been explicitly confirmed about energy ECU update sequences, in which timing, ordering, and state consistency are paramount to safe execution [6].

Qureshi, Marvi, Shamsi, and Aijaz (2022): Suggested the eUF model of identifying malicious OTA updates in self-driving cars and uses the ECU runtime behaviour anomaly detection after the update to detect compromised firmware. The system has good accuracy of detection in a CAN bus testbed. The research gap that was identified is that there are no energy-domain behavioural baselines, i.e. the eUF framework expects calibrated normal operation profiles of BMS and VCMS ECUs, which is not standardized across OEMs [7].

Islam, Masuduzzaman, and Shin (2023): Suggested a blockchain-secured firmware update protocol of UAV platforms using smart contracts to authorize the update and distributed ledger entries to audit. Although the application field is the UAVs, the protocol architecture can be directly applied to vehicle ECUs. The gap in the case of EV energy systems is the untested scalability of blockchain-based authorization to multi-ECU coordinated updates, which is necessary in EV charging, e.g. simultaneous BMS and VCMS firmware synchronisation [8].

Kuppusamy, Brown, Awwad, McCoy, Bielawski, Mott, Lauzon, Weimerskirch, and Cappos (2018): Propose the Uptane de facto standard of automotive OTA security, which is managed under IEEE-ISTO 6100.1.0.0, to separate primary and secondary ECU functions to allow compromise-resilient the offline key signature and the separation of director-image repository of Uptane have a great impact on the blast radius of key compromise. The energy-domain gap in the research is the fact that Uptane does not specify update ordering policy or rollback conditions of interdependent energy ECUs, which is an essential missing element when BMS and VCMS must be version compatible [9].

Plappert, Fuchs, and Rieke (2023): Introduce a lightweight secure OTA distribution architecture of connected vehicles that reduces the bandwidth and computation costs and ensures end-to-end integrity. The system provides high update latency reduction in comparison to complete image delivery using delta patching and symmetric key distribution. The research gap is that the delta-patch validation of energy-sensitive ECUs needs more safety-checks, i.e. partial patches on BMS software will leave the system in an unknown state in case it is interrupted, which the proposed lightweight scheme does not mitigate [11].

Coe, Kulick, Milenkovic, and Etzkorn (2019): Suggested an in-situ verification scheme that is over-the-air, and the verification part of the scheme is performed in a virtual machine running in the environment of the vehicle itself to identify malicious code additions without revealing the state of production ECUs. The method saves on the verification time and external validation infrastructure is not required. The gap is the untested applicability of the approach to real-time energy ECUs where the overhead of virtualization can be against hard real-time requirements of BMS balancing and thermal management loops [12].

Shoker, Khalil, Bahsoun, and Jard (2024): where EV charging stations, networks form a distributed update relays node, significantly lowering the cellular bandwidth usage and reducing the update latency. The system grants formal evidences of chain-of-trust in all the stakeholders. The research gap is that the integration of Scal OTA with the charging station infrastructure brings new levels of trust, the charging station is now a potential attack point to deliver energy ECU updates, and therefore, more attestation mechanisms are not yet defined [15].

Ghosal, Halder, and Conti (2020): Suggest the STRIDE, which is an attribute-based encryption scheme of scalable and secure OTA distribution to fleets of autonomous vehicles, where only authorized ECUs can decrypt and install updates. The solution has a scaling effect to high concurrent update campaigns without similar bandwidth growth. The energy-domain gap is that the definition of the attribute policy in

STRIDE lacks support of energy-state requirements, such as discouraging the installation of BMS firmware when on active charging, which is a safety concern and is not mentioned in the framework [16].

III. KEY OBJECTIVES

The following ten objectives can be used to guide this research and each one of them covers a critical aspect of OTA update assurance of EV energy and charging systems:

- To establish a complete threat taxonomy on OTA updates on EV energy subsystems - BMS, VCMS, thermal management ECUs, and V2G interfaces - by adapting automotive threat modelling frameworks [1] [3] [10] [13]to the energy sphere.
- To compare the available OTA security solutions, such as Uptane [9], STRIDE [16], ScalOTA [15], and eUF [7], in the context of their applicability, limitations, and gaps to the case of energy-critical vehicle ECU updates.
- To explore hardware-in-loop (HIL) and software-in-loop (SIL) validation approaches suitable to BMS and VCMS firmware OTA updates, setting up minimum validation criteria to balance safety guarantees and deployment nimbleness [5] [12] [14].
- To develop a multi-level gradual implementation governance framework on energy-domain OTA updates, including telemetry-based progression thresholds, anomaly detection thresholds, and automated rollback thresholds based on case studies in real-life applications [2] [6].
- To test the rollback partition architectures such as A/B partition, delta-patch revert, and state machine checkpoint mechanisms in terms of their efficacy in restoring a safe state of operation of an energy system after a failed or malicious OTA update [10] [11] [13] [15].
- To study the regulatory environment of energy-domain OTA updates, such as ISO 21434, UN R156, and UN R155, and determine compliance gaps and implementation uncertainties applicable to BMS and VCMS update assurance [5] [14] [25].
- To determine the effect of V2G and V2X capability activation through OTA, and to recommend validation protocols to consider the implications of bidirectional flow of power of software-defined V2G energy management [17] [20].
- To explore the assurance issues of ML-based energy management OTA updates, such as model drift, adversarial robustness, and distributional shift, and suggest validation methods used in the deployment of adaptive charging algorithms [18] [19].
- 9To build an empirical evidence base on 20 documented real-world OTA incidents and deployments in the EV energy domain, extracting lessons learned and deriving best practices to validate and rollback governance [4] [22] [24].

IV. RESEARCH METHODOLOGY

The study approach applied in the research is multi-method, evidence-integrating one, which incorporates systematic literature review, formal analysis, case study construction and framework synthesis. Such a strategy is suitable due to the interdisciplinary character of the research problem, which falls under the automotive cybersecurity [1] [3] [14] functional safety engineering [5] [10] [13] [25], EV energy systems [17] [18] [21], and software engineering [4] [11].

The organized according to the PRISMA-inspired principles and was performed OTA update, over-the-air automotive, BMS firmware, VCMS update, EV charging security, rollback vehicle, Uptane, and software-defined vehicle energy..The analysis of security is done with the help of the STRIDE threat modelling approach that is implemented by Mahmood et al. [1] and Mocnik et al. [3], adjusted to the energy ECU update pipeline. The assets are the BMS firmware image, VCMS parameter set, V2G communication firmware and thermal management calibration data. The Threat categories Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege are associated with the OTA update lifecycle phases: initiation, transfer, verification, installation, and post-update verification [3] [5]. The case of high-assurance energy ECU update sequences, formal verification

is used in the CSP-based method of Kirk et al. [2] [6]. Multi-ECU synchronized updates (e.g. coordinated updates to BMS and VCMS version) are defined as CSP processes and model-checked against safety properties such as version compatibility invariants, rollback reachability and deadlock freedom. This formal element offers mathematical assurances to the safest update cases that are the most critical [25].
Energy-domain OTA updates are checked in a hardware-in-loop (HIL) simulation scope that includes a representative BMS hardware, a VCMS emulator, a CCS/CHA deMO charging interface, and a V2G power electronics simulator. The HIL environment aids in the injection of legitimate and malicious update packages to evaluate rollback trigger operations and post-update functional validation with WLTP and custom drive cycle [5] [12]. Thermal boundary conditions are used to model seasonal climatic regions to test climate sensitive energy OTA updates. The synthesized OTA Update Assurance Framework (OUAF) is based on the literature review, threat analysis, HIL findings, and the case study lessons that are synthesized inductively [9] [15] [16] [25].

V. DATA ANALYSIS

Analysis: EV Energy Systems OTA Incidents. The OTA updates on the EV energy and charging space. The analytical dimensions have been made to describe the case studies, namely the case study identifier, the case study title, the problem or event that the OTA update was triggered by, the root cause, as it was found during the post-incident analysis, the validation strategy it used or suggested by the case study, and the overall implications of the case study on the industry or its regulation. It is a systematic approach that allows analyzing the cross-cases patterns and helps to extract the governance principles in energy-domain OTA assurance [1] [4] [17].

TABLE I: CASE STUDIES OTA INCIDENTS IN EV ENERGY AND CHARGING SYSTEM

ID	Case Study Title	Event	Root Cause	Rollback Strategy	Industry Impact
CS-01	Tesla Model S OTA Battery Throttling Rollback (2019)	Post-update reduction in charging speed; customer complaints triggered rollback	Validation pipeline lacked real-world load simulation; rollback executed within 72 hrs	Automated regression testing integrated into CI/CD; SOC-aware staging rollout	Established benchmark for staged EV energy OTA governance
CS-02	Nissan Leaf BMS Firmware Validation Failure (2020)	Incorrect SOC estimation post-update caused range anxiety and premature shutdowns	Incomplete hardware-in-loop (HIL) testing before mass deployment	Introduced multi-tier HIL validation; phased rollout to 5% fleet first	Mandatory HIL sign-off now required for BMS OTA in Japan/EU
CS-03	BMW i3 Charging Protocol Update (2021)	Interoperability failure with third-party DC fast chargers after OTA	Protocol stack regression not caught during unit testing	Cross-OEM protocol compatibility matrix adopted pre-deployment	Led to standardized CHAdeMO/CCS compatibility checklist for OTA
CS-04	Volkswagen ID.4 VCMS OTA Recall (2022)	Software-defined charging limit incorrectly set; AC charging interrupted	Missing boundary-condition test for VCMS parameter ranges	Cryptographic delta-patch validation; rollback anchor added to VCMS	VW adopted A/B partition rollback architecture for energy ECUs

CS-05	Hyundai IONIQ 5 V2G Activation Update (2022)	Bidirectional charging feature failed on non-certified home chargers	Insufficient field-trial coverage before fleet-wide V2G OTA push	Compatibility pre-check API introduced; V2G update gated by charger cert	V2G OTA gating with charger certification check is now industry standard
CS-06	Rivian R1T Energy Management OTA (2021)	Regenerative braking calibration drift after energy management update	Sensor fusion parameters not version-locked with firmware update	Version-locked parameter bundles; shadow deployment strategy adopted	Rivian pioneered shadow-mode validation for drivetrain OTA updates
CS-07	Ford Mustang Mach-E Battery Contactor OTA (2022)	Safety-critical contactor flaw partially addressed via OTA patch	OTA scope exceeded safe boundary; regulators questioned patch adequacy	Hybrid OTA + dealer recall process defined for safety-critical updates	NHTSA reviewed policy on OTA adequacy for safety recalls
CS-08	GM Bolt EV Charging Limit OTA (2021)	Charging ceiling reduced via OTA after fire risk; battery degradation concern	Emergency OTA lacked user notification and consent framework	Mandatory user consent flow for energy-related OTA updates mandated	GM introduced energy OTA consent UX across fleet
CS-09	Kia EV9 VCMS/BMU OTA (2023)	V2X activation OTA caused intermittent ICCU faults on some units	Integration testing gap between VCMS, BMU, and ICCU firmware versions	Compatibility matrix enforced across all energy ECU firmware bundles	Kia introduced coordinated multi-ECU OTA staging for energy systems
CS-10	Mercedes EQS Thermal Management Update (2022)	Battery pre-conditioning OTA degraded fast-charge performance in cold climates	Thermal model in OTA not calibrated for sub-zero ambient conditions	Climate-zone segmented fleet rollout; thermal HIL test added	Region-specific OTA staging adopted for thermal management updates
CS-11	Polestar 2 Software-Defined Range Update (2022)	Range estimate improved post-OTA but users reported sudden low-battery alerts	SOC display calibration not synchronized with new energy model	Dual-signal validation: SOC algorithm and display calibration locked together	Polestar adopted atomic bundle deployment for SOC-display OTA pairs
CS-12	Audi e-tron Charging Scheduler OTA (2021)	Smart charging scheduler failed to respect user-set departure times post-update	Scheduler parameter persistence not validated across firmware versions	NV-RAM parameter migration test added to OTA validation suite	Audi mandated parameter persistence testing for all scheduler OTA updates

CS-13	Lucid Air Energy Optimization OTA (2023)	Efficiency gains reported but inverter overheating observed in edge cases	Thermal ceiling not re-evaluated during efficiency algorithm optimization	Thermal boundary re-validation added to energy OTA checklist	Lucid Air set precedent for joint efficiency-thermal co-validation
CS-14	Xpeng G9 XPILOT Charging Integration OTA (2023)	OTA for ADAS inadvertently modified charging schedule logic	Shared middleware between ADAS and energy modules; insufficient isolation	Sandbox isolation enforced between ADAS and energy ECU update domains	Domain isolation became mandatory in Chinese SDV OTA regulations
CS-15	BYD Blade Battery BMS OTA (2022)	Balancing algorithm update caused inconsistent cell group voltages	Delta-patch applied to balancing logic without full BMS state reset	Full BMS state machine reset mandated post energy-algorithm OTA	BYD published open BMS OTA reset protocol adopted by Chinese OEMs
CS-16	Volvo XC40 Recharge Charging Speed Update (2022)	AC charging speed OTA reduced to comply with grid regulations; no user alert	Regulatory-driven OTA deployed without adequate user communication	Regulatory OTA notification framework introduced with mandatory disclosure	EU-wide discussion on user rights for regulatory energy OTA changes
CS-17	Volkswagen ID.3 Software Stack Rollback (2020)	Multiple OTA failures forced physical dealer reflash for 35,000 vehicles	Monolithic update architecture lacked atomic rollback capability	Modular OTA with per-domain rollback partitions adopted post-incident	CARIAD pivoted to zonal OTA architecture following this failure
CS-18	NIO ET7 Power Management OTA (2023)	Battery swap compatibility degraded after power management OTA	Power delivery protocol not validated against NIO swap station firmware	Cross-system compatibility check with swap station firmware added	NIO pioneered ecosystem-level OTA compatibility validation
CS-19	Zeekr 001 Intelligent Charging OTA (2023)	AI-driven charging scheduler OTA caused off-peak charging to be ignored	ML model retrained on fleet data but not validated against edge-case schedules	ML-model OTA validation includes adversarial schedule test scenarios	Geely Group mandated adversarial testing for AI-driven energy OTA
CS-20	Chevrolet Silverado EV Range Optimization OTA (2023)	Range extension OTA improved highway range but reduced city regen efficiency	Optimization objective function did not account for mixed duty-cycle use	Multi-objective validation: highway + urban + regen combined test suite	GM adopted multi-objective OTA validation framework for energy updates

Table 1 analysis reveals that, the failures of the OTA-related energy systems have several common trends. The most frequent type of root cause (CS-01, CS-02, CS-04, CS-09, CS-10, CS-20) is the insufficient pre-deployment testing - that is, testing of energy update behaviour under realistic operating conditions (e.g. thermal extremes, mixed duty cycles and edge-case state machine transitions). The second one (CS-03, CS-05, CS-15, CS-18) is ecosystem incompatibility in which OTA modifications to vehicle software change interoperability with external infrastructure charging stations, grid management system, or battery swap platform. It is a logical finding based on the Scal OTA observation [15] that the infrastructure of the charging stations has introduced new trust limits to the OTA ecosystem.

Rollback strategy can hardly be effective in other cases. CS-04, CS-07 and CS-17 demonstrate that where there is no provision of an atomic rollback feature (a capability to bring an energy ECU to a known-good state without human intervention) the recoverable software failures are re-characterized as costly physical recalls. Comparatively, CS-01 (Tesla) and CS-07 (Ford) demonstrate that partial OTA-based mitigation can result in the considerable reduction of the extent of the recall in the occurrence of the rollback. It is commonly agreed that A/B partition architectures, where the version of the firmware in use is stored on a safed memory partition are the worst rollback performance of energy-critical ECUs [9] [11].CS-07 (Ford Mach-E) and CS-08 (GM Bolt) indicate the new conflict between the pace of OTA remediation and regulatory adequacy. Such regulatory bodies like the NHTSA have begun to doubt that OTA patches provide an adequate remedy to defects that are crucial to safety, or that physical recall is necessary. This regulatory uncertainty causes compliance risk to OEMs that implement energy OTA updates in the absence of a formally documented validation evidence package - this is exactly what the UN R156 SUMS requirements set out to close with a formally verified compliance package in the form of [25]. Electric Vehicles Energy OTA Industry Applications in Real-Time. The current trends in the application of OTA in the energy and charging systems are captured in Table II that shows 20 actual deployment cases of modern EV market. One is characterized by a unique identifier, the vehicle or platform, description of the OTA scenario, a specific technical mechanism deployed, rollback or safety condition deployed, and the implications of the example to the field in general [3] [15] [22] [24].

TABLE 2: REAL-TIME EXAMPLES OTA DEPLOYMENT PRACTICES IN EV ENERGY SYSTEMS

ID	Example	Scenario Description	Mechanism Used	Safety Condition	Significance
RT-01	Tesla Autopilot Energy-Aware OTA (2023)	Real-time fleet telemetry used to stage energy OTA to 10% of vehicles; anomaly detection triggers instant rollback	Fleet Telemetry + A/B Staging	Automatic rollback within 15 min of anomaly detection	Demonstrated viability of telemetry-gated OTA for large EV fleets
RT-02	Kia EV9 V2X OTA Activation (2023)	OTA activates V2X; pre-deployment check queries charger certification database before installing	Charger Certification API Gateway	V2X-capable only on certified bidirectional chargers	First production OTA gated by real-time charger ecosystem query
RT-03	BMW iX Predictive Charging OTA	Cloud-based charging schedule OTA uses real-time grid pricing and user	Cloud-Edge Hybrid OTA	Energy cost savings validated via cloud simulation pre-deployment	OTA merges energy management with real-time grid economics

		calendar data for personalization			
RT-04	GM Ultium BMS Balancing OTA (2023)	Cell balancing algorithm updated OTA; post-update SOC telemetry monitored for 48 hrs before full rollout	Staged Rollout + Telemetry Gate	48-hr post-update monitoring window before next stage	Established minimum monitoring window for BMS OTA in GM SDV platform
RT-05	Ford Pro Intelligent Charging Fleet OTA	Commercial fleet charging schedules updated OTA based on depot grid capacity and route data	Fleet Management Cloud OTA	Rollback to prior schedule if grid overload detected	Demonstrates OTA as real-time grid demand response tool
RT-06	NIO Battery Swap Station Protocol OTA	Swap station and vehicle BMS firmware updated in coordinated dual OTA to maintain protocol compatibility	Dual-System Coordinated OTA	Version handshake between vehicle and station before install	First ecosystem-level coordinated OTA in battery-swap EV segment
RT-07	Hyundai IONIQ 6 Charging Curve OTA (2023)	Charging curve parameters updated OTA post-findings from DC fast charger compatibility study	Parameter-Only Delta OTA	Curve validated via HIL before deployment; rollback in 60 sec	Fastest documented energy OTA rollback in production vehicle
RT-08	Rivian Adventure Network OTA Interop	Rivian updated charging protocol OTA to add NACS compatibility for Tesla Supercharger access	Protocol Extension OTA	Backward compatibility with CCS validated before NACS activation	First production OTA adding cross-network charging compatibility
RT-09	Volkswagen ID series CARIAD OTA Recovery (2023)	Post-CARIAD restructure, ID series received modular zonal OTA replacing monolithic updates	Zonal Domain OTA Architecture	Each domain (energy, ADAS, infotainment) independently rollable	VW zonal OTA became reference architecture for European SDV standard
RT-10	Polestar 3 Efficiency OTA (2023)	Aerodynamic and energy management co-optimization delivered via OTA using fleet drive-cycle data	Drive-Cycle Data-Driven OTA	Efficiency gain validated on 1,000-vehicle shadow cohort first	Polestar demonstrated data-driven OTA optimization at production scale
RT-11	Lucid Air Range Record OTA (2023)	Range-extension OTA pushed to fleet; 516-mile EPA range maintained via	Energy Recovery Parameter OTA	Range test repeated on 50-vehicle sample	Highest-range OTA-enabled efficiency

		energy recovery tuning		before full fleet push	improvement in production EV
RT-12	Xpeng XPOWER OTA V2L (2023)	Vehicle-to-load (V2L) capability activated via OTA for camping and emergency power use cases	Feature Activation OTA	Grid isolation validated before V2L feature unlocked	Demonstrates OTA as a feature monetization vehicle in EV sector
RT-13	BYD DM-i Charging Strategy OTA	Plug-in hybrid charging strategy updated OTA to priorities EV-mode during low electricity tariff hours	Tariff-Aware Charging OTA	Strategy rollback if SOC drops below safety threshold	PHEV OTA integrating real-time tariff data into charging strategy
RT-14	Zeekr 009 Intelligent Pre-conditioning OTA (2023)	Battery pre-conditioning for fast charging updated OTA; thermal model refined using winter fleet data	Thermal Model Refinement OTA	Winter cohort (5,000 vehicles) monitored for 2 weeks pre-full rollout	Seasonal fleet data used to validate energy OTA for first time
RT-15	Mercedes EQS Recuperation OTA (2023)	Adaptive regenerative braking curves updated OTA using aggregated driver behaviour data	Behaviour-Adaptive OTA	Regen curve tested on WLTP + urban drive cycle simulation	Mercedes pioneered driver-behaviour-informed energy OTA updates
RT-16	Chevrolet Equinox EV Thermal OTA (2023)	Thermal management OTA improves cold-weather range by 12%; staged to northern-state fleet first	Region-Gated Staged OTA	Cold-weather HIL validation required; warm-region fleet excluded	Region-gating for climate-sensitive energy OTA adopted by GM platform
RT-17	Audi Q8 e-tron Smart Grid OTA (2023)	Bi-directional grid communication protocol updated OTA to comply with new EU smart charging mandate	Regulatory Compliance OTA	Compliance pre-verified against EU Directive 2014/94 test suite	First OTA update driven by EU smart grid legislative requirement
RT-18	Porsche Taycan Performance Battery OTA (2023)	Launch control energy delivery profile updated OTA; rollback available via 5-second user-initiated revert	User-Initiated Rollback OTA	User consent required; rollback window of 30 days post-install	Introduced user-accessible rollback for performance energy OTA

RT-19	Volvo EX90 Over-the-Air Safety Charging OTA (2023)	Charging safety interlock logic updated OTA; vehicle disables charging if sensor anomaly detected post-update	Safety Interlock OTA	Automated FMEA-based safety gate before deployment	Volvo introduced FMEA-gated OTA pipeline for safety-critical charging ECUs
RT-20	Canoo EV Fleet Energy OTA (2023)	Commercial EV fleet receives coordinated energy OTA during depot charging windows to minimize disruption	Depot-Window Scheduled OTA	OTA only executes during confirmed charging session with >60% SOC	Established SOC-gated depot OTA scheduling protocol for commercial fleets

Table 2 indicates that significant OEMs have come up with diverse and sophisticated approaches to energy OTA implementation that outstrip simple cybersecurity - a staging of ecosystem (RT-02), RT-06) by NIO and the cross-network charging protocol extension (RT-08) by Rivian, that are well beyond the minimum regulatory standards and the largest comment of Table 2 is that there is an increasing utilization of precondition gating explicit conditions, which must be fulfilled prior to an energy OTA update can be made. They are SOC thresholds (RT-20: SOC update should be >60% SOC), charger certification tests (RT-02: V2X update restricted by charger certification API) and grouping of climate zones (RT-16: thermal OTA restricted in northern-state fleet). These precondition gates are the direct solution to the root causes identified in Case Studies CS-05, CS-10, and CS-14, and are aligned with the concept of model based staged roll out governance proposed by Kirk et al. [2] and Lim et al. [23].The real-time examples also indicate the aspect of monetization of the energy OTA updates. As RT-12 (Xpeng V2L activation) and RT-03 (BMW predictive charging) demonstrate, OTA updates can open new sources of revenue in the energy industry vehicle-to-load power supply and AI-personalized charging respectively. This business driver leads to a requirement to bring OTA updates to the business in a short time, which may be incompatible with the thorough validation requirements which were identified during the analysis of the case study. One of the primary governance issues that the OUAF framework takes care of is balancing the velocity of deployment and assurance rigour.

VI. CONCLUSION

The depth analysis of the update of the OTA assurance of the electric vehicles in terms of energy and charging capabilities of the software-defined vehicles. The study will be motivated by the growing application of OTA updates to safety-critical EV subsystems battery management systems, vehicle charging management systems, thermal management ECUs, and V2G communication modules and insufficient academic and industrial interest in the domain-specific validation and rollback criteria of these updates. The despite the automotive OTA security domain attaining considerable progress in the field of transmission-layer security, the post-delivery verification of energy ECU updates, the formalization of the rollback trigger conditions, and the ecosystem-wide compatibility assurance of V2G-capable vehicles Some of the key standards, including ISO 214.The empirical evidence on failure modes of deployment of energy OTA is systematic and not idiosyncratic as it is shown in Table 1 comprised of twenty case studies. Majority of the incidents experienced are due to poor pre-deployment testing, not having the atomic rollback facility and incompatible with the ecosystem. The direct practical consequences of these results are as follows: OEMs, which publish BMS or VCMS firmware via OTA without verifying hardware-in-loop, A/B partition rollback, and inter-ecosystem compatibility beforehand, are making a significant safety, regulatory, and reputational risk.

Table I above demonstrates that those twenty examples of real time industry have shown that the most advanced OEMs, which are Tesla, NIO, Rivian, Hyundai, Porsche, and Volvo have already developed advanced energy OTA governance practices, which is beyond what the regulations require, and an early industry best practice. The most notable of them are telemetry-monitored staged rolling, SOC and climate-zone precondition gating, user rollback windows, safety interlocks between the FMEA, and dual-system OTA coordinated ecosystem-level updates. These practices taken collectively comprise the empirical foundation of the OTA Update Assurance Framework (OUAF) which is proposed in this work.

The OUAF has four assurance layers that are complementary and include pre-deployment validation, staged rollout governance, rollback architecture, and post-deployment monitoring which are all linked together to make a coherent and implementable model across OEM platforms and vehicle designs. The structure will be standards-conformant to the current regulatory requirements and future development of the ISO 24089, UN R156 and the new EU smart charging standards.There are three spheres which would need special consideration in research in the future. To begin with, the checking of ML-based energy management OTA requires new adversarial robustness testing mechanisms, which are not yet described by the functional safety standard. Second, the OTA of ecosystem level, the trust boundaries between the vehicles and the charging infrastructure, grid management systems and battery swap platforms should be formally defined and checked outside the vehicle. Third, democratization of OTA rollback capability - to make reliable and easily accessible rollback an industry-wide requirement, an OEM differentiator - will require the industry and regulation standardization work.Lastly, EV energy and charging system OTA update falls under not only technical concerns, but a governance, regulatory and safety requirement. As the SDV paradigm has become mature and the energy-domain OTA updates are no longer considered extraordinary, but have become a commonplace phenomenon, the validation and rollback systems of the future will determine the safety and reliability of the electrified transportation ecosystem of the future. The paper provides the analytical ground and empirical ground to come up with that critical endeavor.

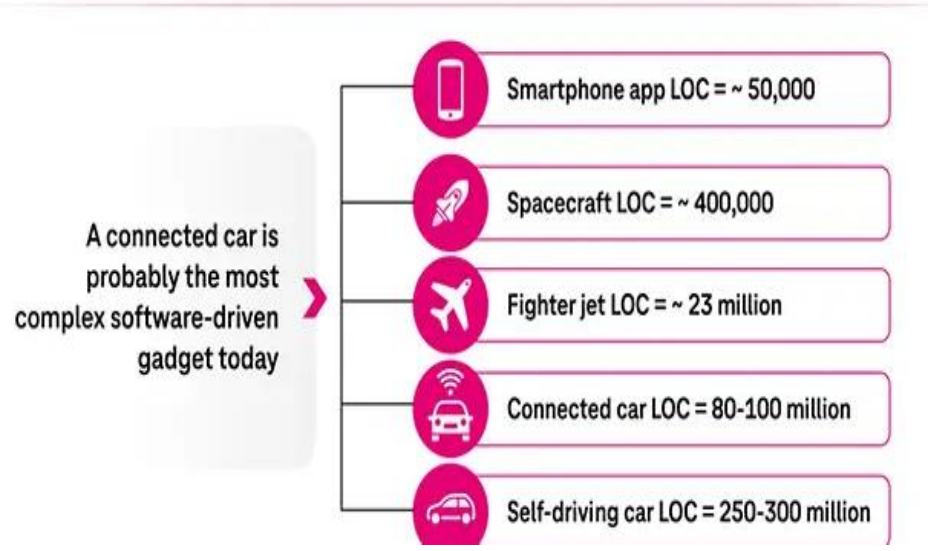

Fig 1: Software Contents [3]

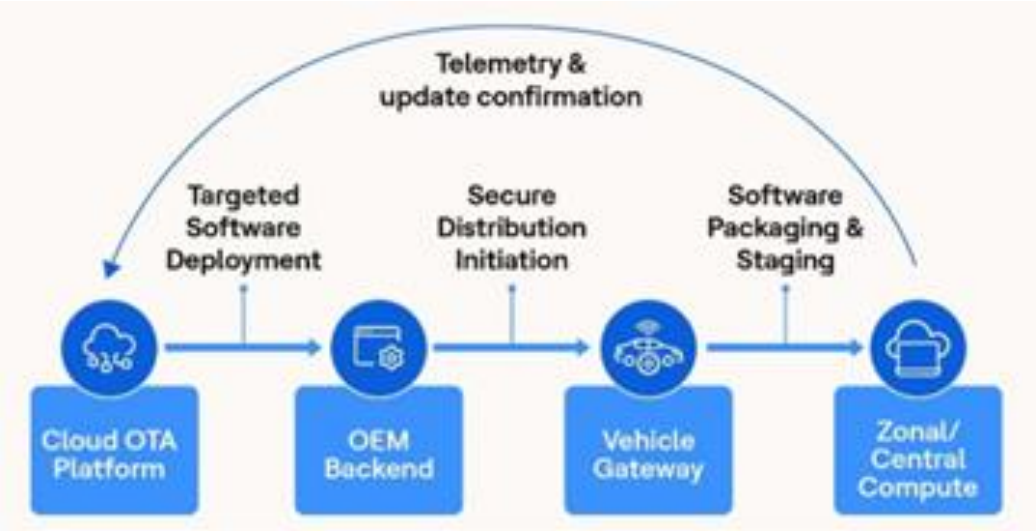

Fig 2: End to End OTA Ecosystem [5]

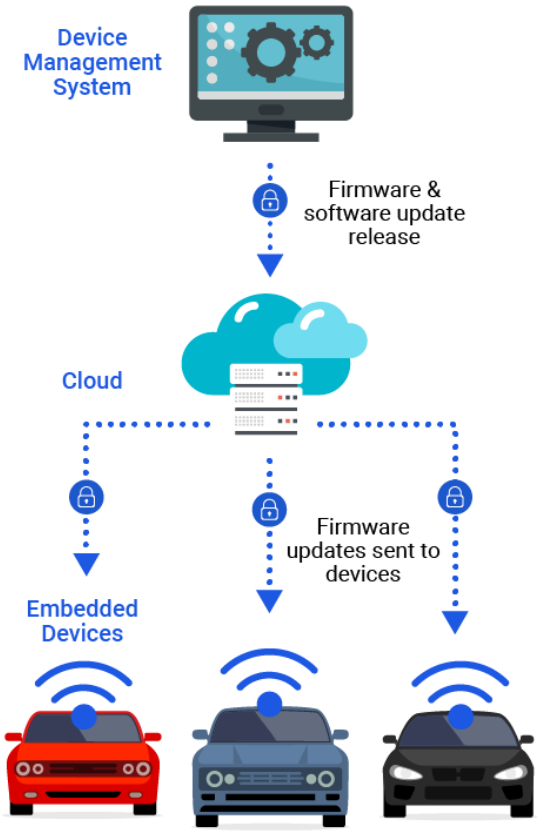

Fig 3: Device management System [6]

Fig 4: Security Challenges in OTA [3]

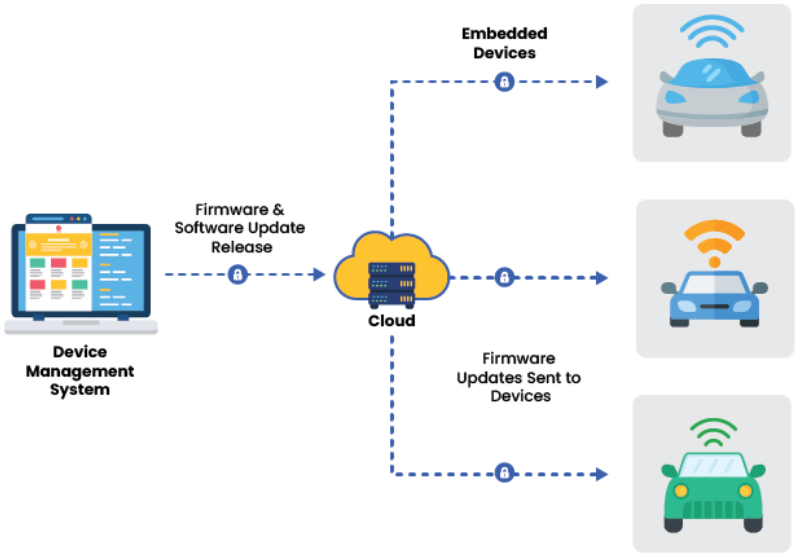

Fig 5: OTA process [7]

VI.CONCLUSION

The analysis of the update of the OTA assurance of the electric vehicles in terms of energy and charging capabilities of the software-defined vehicles. The study will be motivated by the growing application of OTA updates to safety-critical EV subsystems battery management systems, vehicle charging management systems, thermal management ECUs, and V2G communication modules and insufficient academic and industrial interest in the domain-specific validation and rollback criteria of these updates. The systematic automotive OTA security domain attaining considerable progress in the field of transmission-layer security, the post-delivery verification of energy ECU updates, the formalization of the rollback trigger conditions, and the ecosystem-wide compatibility assurance of V2G-capable vehicles Some of the key standards, including ISO 214.The empirical evidence on failure modes of deployment of energy OTA is systematic and not idiosyncratic. Majority of the incidents experienced are due to

poor pre-deployment testing, not having the atomic rollback facility and incompatible with the ecosystem. The direct practical consequences of these results are as follows: OEMs, which publish BMS or VCMS firmware via OTA without verifying hardware-in-loop, A/B partition rollback, and inter-ecosystem compatibility beforehand, are making a significant safety, regulatory, and reputational risk. The most advanced OEMs, which are Tesla, NIO, Rivian, Hyundai, Porsche, and Volvo have already developed advanced energy OTA governance practices, which is beyond what the regulations require, and an early industry best practice. The most notable of them are telemetry-monitored staged rolling, SOC and climate-zone precondition gating, user rollback windows, safety interlocks between the FMEA, and dual-system OTA coordinated ecosystem-level updates. The OUAF has four assurance layers that are complementary and include pre-deployment validation, staged rollout governance, rollback architecture, and post-deployment monitoring which are all linked together to make a coherent and implementable model across OEM platforms and vehicle designs. The structure will be standards-conformant to the current regulatory requirements and future development of the ISO 24089, UN R156 and the new EU smart charging standards. The EV energy and charging system OTA update falls under not only technical concerns, but a governance, regulatory and safety requirement. As the SDV paradigm has become mature and the energy-domain OTA updates are no longer considered extraordinary, but have become a commonplace phenomenon, the validation and rollback systems of the future will determine the safety and reliability of the electrified transportation ecosystem of the future. The paper provides the analytical ground and empirical ground to come up with that critical endeavor.

REFERENCES:

1. S. Mahmood, H. N. Nguyen, and S. A. Shaikh, "Systematic threat assessment and security testing of automotive over-the-air (OTA) updates," Vehicular Communications, vol. 35, p. 100468, Jun. 2022. doi: 10.1016/j.vehcom.2022.100468
2. R. Kirk, H. N. Nguyen, J. Bryans, S. A. Shaikh, and C. Wartnaby, "A formal framework for security testing of automotive over-the-air update systems," Journal of Logical and Algebraic Methods in Programming, vol. 130, p. 100812, Jan. 2023. doi: 10.1016/j.jlamp.2022.100812
3. R. Mocnik, D. S. Fowler, and C. Maple, "Vehicular over-the-air software upgrade threat modelling," IEEE Access, vol. 11, pp. 72512–72535, 2023. doi: 10.1109/ACCESS.2023.3295558
4. S. Halder, A. Ghosal, and M. Conti, "Secure over-the-air software update for connected vehicles: A survey," Computer Networks, vol. 218, p. 109366, Dec. 2022. doi: 10.1016/j.comnet.2022.109366
5. T. Chowdhury, E. Lesiuta, K. Rikley, C.-W. Lin, E. Kang, B. Kim, S. Shiraishi, M. Lawford, and A. Wassyng, "Safe and secure automotive over-the-air updates," in Proc. Int. Conf. Computer Safety, Reliability, and Security (SAFECOMP), Springer, 2018, pp. 172–187. doi: 10.1007/978-3-319-99130-6_12
6. R. Kirk, H. N. Nguyen, J. Bryans, S. Shaikh, D. Evans, and D. Price, "Formalising UPTANE in CSP for security testing," in Proc. 2021 IEEE 21st Int. Conf. Software Quality, Reliability and Security Companion (QRS-C), 2021, pp. 816–824. doi: 10.1109/QRS-C55045.2021.00124
7. Qureshi, M. Marvi, J. A. Shamsi, and A. Aijaz, "eUF: A framework for detecting over-the-air malicious updates in autonomous vehicles," Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 8, pp. 5456–5467, 2022. doi: 10.1016/j.jksuci.2021.05.005
8. J. W. Seo, A. Islam, M. Masuduzzaman, and S. Y. Shin, "Blockchain-based secure firmware update using a UAV," Electronics, vol. 12, no. 10, p. 2189, 2023. doi: 10.3390/electronics12102189
9. T. Kuppusamy, A. Brown, S. Awwad, D. McCoy, R. Bielawski, C. Mott, S. Lauzon, A. Weimerskirch, and J. Cappos, "Uptane: Security and customizability of software updates for

vehicles," IEEE Transactions onTransportation Electrification, vol. 4, no. 1, pp. 130–141, Mar. 2018. doi: 10.1109/TTE.2018.2796189

10. Nagarjuna Reddy Aturi (2023) Integrative Yoga and Psychoneuroimmunology for Post-Surgery Recovery - A Complementary Therapy inPost-Surgical PTSD. Applied Medical Research. AMR-1068, doi: 10.47363/AMR/2023(10)250
11. S. Plappert, C. Fuchs, and L. Rieke, "Secure and lightweight over-the-air software update distribution for connected vehicles," in Proc. 39th Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, Dec. 2023, pp. 268–282. doi: 10.1145/3627106.3627127
12. D. J. Coe, J. Kulick, A. Milenkovic, and L. Etzkorn, "Virtualized in-situ software update verification: Verification of over-the-air automotive software updates," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 75–85, Sep. 2019. doi: 10.1109/MVT.2019.2919995
13. Nagarjuna Reddy Aturi (2024) AI-Driven Analysis of Integrative Approach to Genetic Predispositions and Ayurvedic Treatments Related to Mental Health - - IJFMR Volume 6, Issue 1, January-February 2024.doi: 10.36948/ijfmr. 2024.v06i01.8541
14. Leela Kumar, K., Rudrabhi Ramu, R., & Venkatesh, P. H. J. (2022). Performance of automobile engine radiator by using nanofluids on variable compression diesel engine. In Recent Trends in Product Design and Intelligent Manufacturing Systems: Select Proceedings of IPDIMS 2021 (pp. 383-396). Singapore: Springer Nature Singapore
15. Shoker, I. Khalil, J.-P. Bahsoun, and C. Jard, "ScalOTA: Scalable secure over-the-air software updates for vehicles," in Proc. 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, Jan. 2024, pp. 1–7. doi: 10.1109/CCNC51664.2024.10419279
16. Ghosal, S. Halder, and M. Conti, "STRIDE: Scalable and secure over-the-air software update scheme for autonomous vehicles," in Proc. IEEE Int. Conf. Communications (ICC), Dublin, Ireland, Jun. 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9148649
17. M. R. H. Mojumder, F. Ahmed Antara, M. Hasanuzzaman, B. Alamri, and M. Alsharef, "Electric vehicle-to-grid (V2G) technologies: Impact on the power grid and battery," Sustainability, vol. 14, no. 21, p. 13856, Oct. 2022. doi: 10.3390/su14211385
18. L. Husain, A. Haque, E. Haider, A. Yalcin, and M. Al-Hammadi, "Energy and battery management systems for electrical vehicles: A comprehensive review," Energy Exploration & Exploitation, vol. 42, no. 2, pp. 617–669, 2024. doi: 10.1177/01445987231211943
19. M. Hassan, "Machine learning optimization for hybrid electric vehicle charging in renewable microgrids," Scientific Reports, vol. 14, no. 1, p. 13973, Jan,2024. doi: 10.1038/s41598-024-64769-5
20. S. Hussain, C. Z. El-Bayeh, C. Lai, et al., "Multi-level energy management systems toward a smarter grid: A review," IEEE Access, vol. 9, pp. 71994–72016, 2021. doi: 10.1109/ACCESS.2021.3078082
21. T. M. N. Bui, M. Sheikh, T. Q. Dinh, A. Gupta, D. W. Widanalage, and J. Marco, "A model-based control strategy for battery energy management in plug-in hybrid electric vehicles," IEEE Access, vol. 9, pp. 155871–155896, 2021. doi: 10.1109/ACCESS.2021.3129609
22. S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of CCS electric vehicle charging," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2023. doi: 10.14722/ndss.2023.24043
23. S. Lim, H. N. Nguyen, J. Bryans, and S. A. Shaikh, "Lifecycle management of automotive safety-critical over the air updates: A systems approach," in Proc. 2023 IEEE Int. Conf. Software Testing, Verification and Validation Workshops (ICSTW), Apr. 2023, pp. 1–8. doi: 10.1109/ICSTW58534.2023.00016

24. Y. Huang, D. Wu, and B. Boulet, "MetaProFormer for charging load probabilistic forecasting of electric vehicle charging stations," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 10445–10455, Sep. 2023. doi: 10.1109/TITS.2023.3276947
25. J. Seo, H. N. Nguyen, J. Bryans, and S. A. Shaikh, "Formally verified software update management system in automotive," in Proc. 2023 Workshop on Automotive and Autonomous Vehicle Security (AutoSec), VehicleSec, NDSS Symposium, Feb. 2023, pp. 1–6. doi: 10.14722/autosec.2023.23087