GP Cybersecurity Vehicle Forum
OTA Standards Update

4 June 2024

Ira McDonald (High North Inc)
blueroofmusic@gmail.com

GP CSVF June 2024
OTA Standards – Agenda

- **Agenda**
  - ISO and UNECE Specs – Cybersecurity & Software Update
  - ISO 24089:2023 – Road Vehicles: Software Update Engineering
  - ISO 24089 – Road Vehicles: Software Update – Extension Projects
  - ISO 25090 – Road Vehicles: Software Update – Vehicle Configuration Info
  - UNECE WP29 R156 (2021) – Road Vehicles: Software Update (certification)
  - Uptane Framework – OTA Software Updates
  - IETF SUIT – Software Updates for IoT
  - ITU-T X.1370 Series – Intelligent Transportation System Security

GP CSVF June 2024
OTA Standards – ISO & UNECE Specs

- **ISO Standards – Automotive Cybersecurity & Software Update**
  - ISO/SAE 21434:2021 (International Standard, August 2021)
    - Road vehicles — Cybersecurity Engineering
      – Vehicle only cybersecurity engineering requirements
    - https://www.iso.org/standard/70918.html
  - ISO 24089:2023 (International Standard, February 2023)
    - Road Vehicles – Software Update Engineering
      – Infrastructure (back office) and Vehicle software update requirements
    - https://www.iso.org/standard/77796.html
- **UNECE Regulations – Automotive Cybersecurity & Software Update**
  - UNECE WP29 R155 (March 2021) – Road Vehicles – Cybersecurity
    - https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
  - UNECE WP29 R156 (March 2021) – Road Vehicles – Software Update
    - https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

GP CSVF June 2024
OTA Standards – ISO 24089:2023 (1 of 3)

- **ISO TC22/SC32/WG12 – ISO 24089 – Software Update Engineering**
  - Introduction
    – vocabulary, objectives, requirements, and guidelines for software updates
  - Normative References
    – ISO/SAE 21434 and ISO 26262 Parts 6 and 8
  - Terms and Definitions
    – compatibility, **condition**, **dependency**, infrastructure, in-vehicle resource, **recipient**, **safe vehicle state**, **skilled person**, software update campaign, software update distribution method, **software update operation (receipt, installation, activation steps)**, software update package, software update project, **tailor**, **target (vehicle class)**, vehicle configuration info, vehicle system, vehicle user
  - Organizational Level Requirements
    – establishing organization-level processes for software update engineering
    – adopting quality, functional safety, and cybersecurity management
    – instituting and maintaining a continuous improvement process
    – establishing an information sharing policy
    – performing an organizational audit for process compliance

GP CSVF June 2024
OTA Standards – ISO 24089:2023 (2 of 3)

- **ISO TC22/SC32/WG12 – ISO 24089 – Software Update Engineering**
  - Project Level Requirements
    – planning a software update project, including roles and responsibilities
    – managing and storing of information regarding a software update project
    – providing justifications for any tailoring of a software update project
    – confirming interoperability of the infrastructure and the vehicle functions
    – preserving integrity of software, metadata, and software update packages
  - Infrastructure Level Requirements
    – management of cybersecurity risks for the infrastructure
    – functionality for collecting and managing vehicle configuration information
    – functionality for collecting and distributing information about software update campaigns
    – functionality for creating, managing, and distributing software update packages

GP CSVF June 2024
OTA Standards – ISO 24089:2023 (3 of 3)

- **ISO TC22/SC32/WG12 – ISO 24089 – Software Update Engineering**
  - Vehicle and Vehicle Systems Level Requirements
    – managing safety and cybersecurity risks for software update operations
    – managing vehicle configuration information
    – communicating software update campaign information
    – enabling software update operations, verifying software update packages, and managing failures during software update campaigns
  - Software Update Package Requirements
    – identifying the target(s) and contents of the software update package
    – assembling the software update package containing the necessary software and metadata for the target(s)
    – verifying and validating the software update package
    – approving release of the software update package
  - Software Update Campaign Requirements
    – preparing software update campaigns
    – executing software update campaigns
    – completing software update campaigns
  - Bibliography

GP CSVF June 2024
OTA Standards – ISO 24089 Extensions

- **ISO TC22/SC32/WG12 – ISO 24089 – Extension Projects**
  - ISO Amendment to ISO 24089 – *completed and ISO TC22/SC32 approved*
    – correct one error in section 5.3.4.1 (misplaced commas, dangling clause)
    – add one definition for “Tool” (device or module for software update)
  - ISO PAS 25090 Software Update – Vehicle Config Info – *active project*
    – define common vehicle configuration abstract elements (*without format*)
    – allow partial vehicle configuration metadata (only *relevant* ECUs)
    – allow fine-grained access control (e.g., OEM vs Tier-1 Supplier)
    – allow decomposition of vehicle configuration metadata elements
  - ISO TR 24935 Software Update – Using Mobile Comms – *active project*
    – report of Korean government sponsored prototype in 2021
    – collaboration between OEMs, telecom providers, software vendors

GP CSVF June 2024
OTA Standards – ISO PAS 25090 (1 of 2)

- **ISO TC22/SC32/WG12 – ISO PAS 25090 – Vehicle Config Info**
  - Introduction
    – vocabulary, objectives, and requirements for Vehicle Config Info
  - Normative References
    – ISO/SAE 21434 and ISO 24089
  - Terms and Definitions
    – define common vehicle configuration abstract elements (*without format*)
  - Organizational Level Responsibilities
    – extends ISO 24089:2023 to focus on *relevant* Vehicle Config Info
    – facilitates communications about software update engineering activities that involve vehicle configuration information throughout the supply chain
  - Elements of Vehicle Configuration Info
    – describes common types of elements of Vehicle Configuration Info
    – Vehicle Identifier, ECU Identifier (immutable), ECU Version (unique)
    – Vehicle System Identifier (immutable), Vehicle System Version (unique)
    – Hardware Identifier (immutable), Hardware Version (unique)
    – Software Identifier (immutable), Software Version (unique)

GP CSVF June 2024
OTA Standards – ISO PAS 25090 (2 of 2)

- **ISO TC22/SC32/WG12 – ISO PAS 25090 – Vehicle Config Info**
  - Relationships between Elements of Vehicle Configuration Info
    – identifies relationships between elements of Vehicle Configuration Info
    – describes communication of these relationships in the supply chain
  - Selection of Relevant Vehicle Configuration Info
    – provides requirements and recommendations for selecting relevant Vehicle Configuration Info
    – software update project, package, and campaign level requirements
  - Annex A – Examples of Selection of Relevant Vehicle Configuration Info
    – Steering System and Automated Lane Keeping System (ALKS)
  - Bibliography

GP CSVF June 2024
OTA Standards – UNECE WP29 R156 (1 of 2)

- **UNECE WP29 R156 – Road Vehicles: Software Update (certification)**
  - Introduction
    – Defines “Type Certification” for various road vehicle and system types
  - Terminology
    – **Vehicle Type**, **RX Software Identification Number** (RXSWIN), Software Update, **Execution** (installing and activating), Software Update Management System (**SUMS**), Vehicle User, **Safe State**, Over-the-Air (**OTA**) Update, **System** (set of components), Integrity Validation Data (checksums, hashes)
  - Application for Approval
    – Application for approval of a vehicle type for software update processes shall be submitted by vehicle manufacturer or duly accredited representative
  - Marking
    – International approval mark shall be affixed to every conforming vehicle, conspicuously and in a readily accessible place
  - Approval
    – Approval Authorities shall grant, as appropriate, type approval with regard to software update procedures and processes, only to such vehicle types that satisfy all of the requirements of this Regulation

GP CSVF June 2024
OTA Standards – UNECE WP29 R156 (2 of 2)

- **UNECE WP29 R156 – Road Vehicles: Software Update (certification)**
  - Certificate of Compliance for Software Update Management System (SUMS)
    – Contracting Parties shall appoint an Approval Authority to carry out the assessment of the manufacturer and to issue a Certificate of Compliance for the Software Update Management System
  - General Specifications
    – Requirements for Software Update Management System of manufacturer
    – Processes to be verified at initial assessment
    – Vehicle manufacturer shall record and store, the information for each update applied to a given vehicle type
    – Vehicle manufacturer shall demonstrate security processes
    – Additional process requirements for software updates over the air
  - Modification and Extension of the Vehicle Type
    – Every modification of the vehicle type which affects its technical performance and/or documentation required in this Regulation shall be notified to the Approval Authority which granted the approval
  - Conformity of Production Procedures – per UNECE 1958 agreement
  - Production Definitively Discontinued – end of vehicle type manufacturing

GP CSVF June 2024
OTA Standards – Uptane Framework (1 of 5)

- **Uptane Framework – OTA Software Updates**
  - Uptane Project – OTA Software Update Community (Linux Foundation)
    – https://uptane.org/
  - Uptane Standard – OTA Software Update Framework
    – https://uptane.org/docs/2.1.0/standard/uptane-standard
  - Uptane Deployment Best Practices – OTA Software Update Guidance
    – https://uptane.org/docs/2.1.0/deployment/best-practices
  - Timeline
    – Uptane grants from US DHS for NYU, Univ of Michigan, SWRI – Fall 2015
    – Uptane first workshop – February 2016
    – Uptane Alliance organized under IEEE-ISTO – 2018
    – Uptane Standard v1.0.0 – IEEE-ISTO 6100 – July 2019
    – Uptane joined Linux Foundation / Joint Development Fund – Fall 2019
    – Uptane Standard v1.0.1 – March 2020
    – Uptane Standard v1.1.0 – January 2021
    – Uptane Standard v1.2.0 – August 2021
    – Uptane Standard v2.0.0 – March 2022
    – Uptane Standard v2.1.0 – June 2023

GP CSVF June 2024
OTA Standards – Uptane Framework (2 of 5)

- **Uptane Framework – Uptane Standard v2.1.0 – Overview**
  - Introduction
    – Architecture neutral secure software update framework for ground vehicles
  - Terminology
    – Conformance, Uptane, Acronyms and Abbreviations
  - Rationale
    – Essential components for the secure design, implementation, and deployment of Uptane by OEMs and suppliers – attack resilience
  - Design Requirement Principles
    – Mandate design and implementation steps that are security critical and followed as is, while offering flexibility in implementation of non-critical steps
    – Ensure that the security practices mandated or recommended do not interfere with the functionality of vehicles, vehicle systems, or ECUs
    – Ensure that, when any part of the OTA mechanism in a vehicle is attacked, an attacker has to compromise two or more modules to break OTA solution
  - Threat Model and Attack Strategies
    – Classes of Threats, Types of Attackers, Mitigations and Defenses

GP CSVF June 2024
OTA Standards – Uptane Framework (3 of 5)

- **Uptane Framework – Uptane Standard v2.1.0 – Requirements**
  - Image Repository containing binary images to install and signed metadata
  - Director Repository connected to Inventory Database that signs metadata
  - Repository tools for generating Uptane-specific metadata about Images
  - Vehicle *always* sends complete Image version manifest for all vehicle ECUs to Director *before* Director sends candidate update information to Vehicle
  - Role-based separation for compromise resilience
    – Root role – signs public keys used to verify metadata produced by Timestamp, Snapshot, and Targets roles
    – Targets role – produces and signs metadata for Images and Delegations
    – Snapshot role – produces and signs metadata about all Targets metadata that the Repository releases
    – Delegations – Targets role on the Image repository can delegate the responsibility of signing metadata (e.g., to a supplier organization)

GP CSVF June 2024
OTA Standards – Uptane Framework (4 of 5)

- **Uptane Framework – Uptane Standard v2.1.0 – Requirements**
  - Metadata – no mandate for any particular format or encoding for metadata
    – Root metadata – distributes public keys of top-level Root, Targets, and Snapshot roles
    – Targets metadata – information about Images to be installed on ECUs
    – Snapshot metadata – filenames and versions of all Targets metadata
  - In-vehicle Implementation Requirements
    – Uptane-conformant ECU – able to receive and verify Image metadata and Image binaries (before installation and activation)
    – Primary ECU – performs download, verification, and distribution of latest time, metadata, and Image binaries (for installation and activation)
    – Secondary ECU – performs either full or partial verification of latest time, metadata, and Image binaries (before local installation and activation)

GP CSVF June 2024
OTA Standards – Uptane Framework (5 of 5)

- **Uptane Framework – Uptane Standard v2.2 & v3.0 – Future**
  - Uptane Framework – Best Practices for Secure Identifiers
    – Strong Hardware Identifiers – IEEE 802.1AR – DevID and Local DevID
    – Strong Software Identifiers – IETF RFC 9393 – CoSWID (Concise Software Identification) Tags – compact alternative to ISO/IEC 19770-2:2015 SWID
  - Uptane Framework – Adoption and Transition
    – Multiple Image Repository support (e.g., for legacy and Uptane solutions)
    – Multiple Director Repository support (e.g., for segmented vehicle OTA)
    – Multiple PKI Infrastructure support (e.g., for OEM and Public CAs)
  - Uptane Framework – Aftermarket Updates
    – Image Repository Delegation support (e.g., for OEM end-of-life)
    – Director Repository Delegation support (e.g., for certain ECUs in models)
  - Uptane Framework – New Markets
    – Robotics (e.g., Airbotics projects in Ireland)
    – Autonomous Vehicles (e.g., SwRI projects in Texas)
    – Racing Vehicles (e.g., Aston Martin projects in England)
    – Aeronautics (e.g., ultralights, helicopters, flying cars)

GP CSVF June 2024
OTA Standards – IETF SUIT (1 of 2)

- **IETF SUIT – Software Update for Internet of Things**
  - IETF Manifest Info Model for Firmware Updates in IoT Devices (January 2022) – https://datatracker.ietf.org/doc/rfc9124/
  - IETF Firmware Update Architecture for Internet of Things (April 2021) – https://datatracker.ietf.org/doc/rfc9019/
  - IETF Strong Assertions of IoT Network Access Requirements (March 2024) – https://datatracker.ietf.org/doc/draft-ietf-suit-mud/
  - IETF Secure Reporting of Update Status (March 2024) – https://datatracker.ietf.org/doc/draft-ietf-suit-report/
  - IETF SUIT Manifest Extensions for Multiple Trust Domains (March 2024) – https://datatracker.ietf.org/doc/draft-ietf-suit-trust-domains/
  - IETF Update Management Extensions for SUIT Manifests (March 2024) – https://datatracker.ietf.org/doc/draft-ietf-suit-update-management/
  - IETF Encrypted Payloads in SUIT Manifests (March 2024) – https://datatracker.ietf.org/doc/draft-ietf-suit-firmware-encryption/

GP CSVF June 2024
OTA Standards – IETF SUIT (2 of 2)

- **IETF SUIT – Software Update for Internet of Things**
  - IETF Mandatory-to-Implement Algorithms for Authors and Recipients of SUIT Manifests (February 2024)
    – https://datatracker.ietf.org/doc/draft-ietf-suit-mti/
  - IETF CBOR-based Serialization Format for the (SUIT) Manifest (February 2024)
    – https://datatracker.ietf.org/doc/draft-ietf-suit-manifest/

GP CSVF June 2024
OTA Standards – ITU-T X.1370 (1 of 2)

- **ITU-T X.1370 Series – Intelligent Transportation System Security**
  - ITU-T X.1371 Security Threats to Connected Vehicles (May 2020)
    – https://www.itu.int/rec/T-REC-X.1371/en
  - ITU-T X.1372 Security Guidelines for V2X (March 2020)
    – https://www.itu.int/rec/T-REC-X.1372/en
  - ITU-T X.1373 Secure Software Update Capability for ITS Communication Devices (March 2017)
    – https://www.itu.int/rec/T-REC-X.1373/en
  - ITU-T X.1374 Security Requirements for External Interfaces and Devices with Vehicle Access Capability (October 2020)
    – https://www.itu.int/rec/T-REC-X.1374/en
  - ITU-T X.1375 Guidelines for an Intrusion Detection System for In-Vehicle Networks (October 2020)
    – https://www.itu.int/rec/T-REC-X.1375/en
  - ITU-T X.1376 Security-Related Misbehaviour Detection Mechanism using Big Data for Connected Vehicles (January 2021)
    – https://www.itu.int/rec/T-REC-X.1376/en

GP CSVF June 2024
OTA Standards – ITU-T X.1370 (2 of 2)

- **ITU-T X.1370 Series – Intelligent Transportation System Security**
  - ITU-T X.1377 Guidelines for an Intrusion Prevention System for Connected Vehicles (October 2022)
    – https://www.itu.int/rec/T-REC-X.1377/en
  - ITU-T X.1379 Security Requirements for Roadside Units in ITS (July 2022)
    – https://www.itu.int/rec/T-REC-X.1379/en
  - ITU-T X.1380 Security Guidelines for Cloud-based Event Data Recorders in Automotive Environments (March 2023)
    – https://www.itu.int/rec/T-REC-X.1380/en
  - ITU-T X.1381 Security Guidelines for Ethernet-based In-Vehicle Networks (March 2023)
    – https://www.itu.int/rec/T-REC-X.1381/en
  - ITU-T X.1382 Guidelines for Sharing Security Threat Info on Connected Vehicles (March 2023)
    – https://www.itu.int/rec/T-REC-X.1382/en
  - ITU-T X.1383 Security Requirements for Categorized Data in V2X Comms (March 2023)
    – https://www.itu.int/rec/T-REC-X.1383/en