ISO 24089
(and a Little Bit of SAE/ISO 21434)

Suzanne Lightman, NIST

For UPTANE October 2022

24089 *Road vehicles – Software update engineering*

Very Important

- Print out clause 3 – definitions and keep it with you when reading this document
    - Uses precise terms for software update engineering
    - But these terms are unique to document

Over Arching Thoughts

- Does NOT prescribe any specific architecture or methodology for updates
- Covers hardware as well as software updates
- Does NOT cover the development of code and hardware
- This is the first standard that addresses organizations’ infrastructure as well as the vehicles

Organizational processes

- Requires conformance with
  - SAE/ISO 21434
  - ISO 26262-6 and ISO 26262-8
  - The combination of these normative standards should ensure that all code and hardware is developed with proper attention to safety and cybersecurity
    - The two parts of 26262 were selected to allow conformance by organizations who do not apply all parts of the standard series due to specialty work

Organizational Processes cont.

- Pretty standard requirements for organizational processes but specialized for software update engineering
  - Processes and rules
    - To conform with this document and normative references
    - Continuous improvement
    - Information sharing
    - Supporting processes
      - Document management
      - Configuration management
      - Requirements management
      - Quality management
    - Auditing

Software update project processes

- Software update project
    - First of the terminology
        - Defined by targets and can cover multiple updates
    - Requires:
        - A plan
        - Documentation
        - Assignment of roles and responsibilities
- Tailoring
- Interoperability
- Integrity

Tailoring Discussion

- There was extensive debate on the tailoring clause
  - Many organizations create updates but do not distribute them to vehicles on the road
  - Some sections of the industry have a different relationship to the vehicles (bodybuilders)
  - However, there are many parts of the document that affect the development of vehicles, vehicles systems and/or ECUs

Infrastructure and Vehicle & Vehicle System Functions: Overall Thoughts

- Covers the functions that must exist to conform with the requirements of this document and to be able to do software update engineering
  - Both in the organization’s infrastructure
    - only infrastructure which supports software update activities
  - And in the vehicle
  - To remain solution neutral –
    - many requirements include a note that they can be ‘either on the vehicle or in the infrastructure or both’
  - Tools considered part of the infrastructure

Infrastructure and Vehicle & Vehicle System Functions

- Sample functions
  - Management of vehicle configuration information
  - Identification of dependencies and compatibility
  - Communications
  - Resolving targets into recipients
  - Integrity
  - Processing software update packages
  - Support for software update distribution methods
  - Ensuring safe vehicle state

Software Update Package Assembly

- Creation of the software update packages
  - Contains code and associated metadata
- Software update packages determine many parts of the software update campaign
  - Software update distribution methods
  - Communications
  - Compatibility/dependencies and conditions
  - Necessary actions
- Packages must be verified and validated and then approved for release

Software Update Campaigns

- Three phases
  - Preparation
  - Execution
  - Completion
- Must have a plan
- Resolving targets into recipients
- Communications
- Results

21434 *Road vehicles – Cybersecurity Engineering*

Just a brief overview

SAE/ISO 21434 *Road Vehicles – Cybersecurity Engineering*

- Focuses on cybersecurity for
  - The vehicle
  - Lifecycle from concept through decommissioning
  - Supporting and management processes
  - First international standard for cybersecurity in the automotive industry

- Developed by
  - SAE and ISO joint working group
  - OEMs and suppliers
  - With awareness of regulation and UNECE work

Concept through Development

- Takes a risk-based approach
- Integrates cybersecurity throughout the design and development cycle
- Starts with item definition
  - Define cybersecurity goals
  - Create a cybersecurity concept
  - This leads to requirements on the actual item
  - These requirements can be verified and validated
- Items are on the vehicle
- Items contain assets with cybersecurity properties

Concept Through Development

- Discussion of different types of development
  - Distributed activities
    - Activities that are done by suppliers
    - Conform with the requirements of the document
- Out of context
  - Component developed for one situation and reused in another
  - Allows for efficiencies
- Off-the-shelf component
  - Not developed under distributed activities

Threat Analysis and Risk Assessment

- Different parts of TARA presented for use in developing items with appropriate cybersecurity requirements
- Asset identification
- Threat scenario identification
- Impact rating
- Attack path analysis
- Attack feasibility rating
- Risk value determination
- Risk treatment decision

Continual Cybersecurity Activities

- Activities that occur throughout the lifecycle of the item being produced
  - Cybersecurity monitoring
    - Sets up a process to keep the monitoring function apprised of relevant information
      - Called triage
      - Could be software/hardware
      - Could be specific organizations or types of attacks
  - Cybersecurity event evaluation
    - Use of triage to determine what cybersecurity information needs to be analyzed more deeply
    - Allows a lightweight activity to reduce burden
  - Vulnerability analysis
    - Uses the TARA elements
  - Vulnerability management

Post-Development Phases

- Production
  - Concentrates on preserving the cybersecurity requirements on the item from development
  - There is a requirement for a cybersecurity management system for production to support these activities
  - A production plan must be created and implemented, including
    - The necessary steps in sequence to apply cybersecurity requirements
    - Covering any tools and equipment
    - Controls to prevent unauthorized alternations
    - Ways to confirm that cybersecurity requirements are met

Post-development Phases

- Operations and Maintenance
  - Covers cybersecurity incident response
    - Follows from the event identification requirements during continual cybersecurity activities
  - Requires that all updates and ‘update-related capabilities’ be developed in accordance with 21434
- Decommissioning
  - End of cybersecurity support
  - Any requirements to enable secure decommissioning of items and components