ISO/SAE 21434™ Cybersecurity Engineering Draft Standard

Tim Weisenberger

Senior Project Manager, Emerging Technologies

Stacey Stevens

Senior Product Manager, Professional Development

SAE International

Agenda

- SAE Partnership with ISO
- Cybersecurity in the Mobility Sector
- Looking under the Hood
  - Benefits of the 21434 Standard
  - In-scope and Out of Scope
  - Consensus Areas
  - Status
- Planned SAE Support and Development
- 21434 Training Overview- “Managing Cybersecurity Risks Using ISO/SAE 21434”

The Journey From SAE J3061™ To ISO/SAE 21434

- SAE J3061 Standard released January 2016 and set the foundation
  - Cybersecurity engineering framework
  - Consistent with ISO 26262 functional safety
- ISO and SAE joined forces in 2016 to pursue ISO/SAE 21434 Draft Standard
  - Progressive work based off SAE J3061 Standard
- Other non-cybersecurity standards are also in development or planned (e.g. vehicle automation and EV)

History of Cybersecurity in Mobility

- No real industry cyber visibility until 2010
  - Univ. Washington/UC San Diego vulnerability research
  - Vehicle becomes the “sexy” hack from 2010-2015
- SAE creates the Vehicle Electrical System Cybersecurity Committee in 2011
  - Drives automotive engineers up the cyber learning curve
  - SAE J3061 Standard Published in 2016
  - J3016 espouses a risk-based, process-driven approach to implementing cybersecurity throughout the product development lifecycle
- Beginning in 2011, the SAE CyberAuto Challenge™ pairs professional engineers and students in a hands-on cybersecurity learning environment

State of Cybersecurity in Mobility

- Cybersecurity in vehicle is *very unique*
  - Vehicles are *cyber-physical systems* that require different security controls from IT networks, LANs, etc.
  - Functional Safety and Security are intertwined; a vehicle cannot be safe if it is not secure
  - Vehicles are mobile systems-of-systems that are wirelessly connected
- Thus, typical security best practices (e.g. software security patches, password updates, etc.) are much more difficult to use.

State of Cybersecurity in Mobility

- Industry cybersecurity discipline has matured quickly
- Industry experts understand the risk-based, process-driven approach
- However…
  - Cybersecurity professionals are *very expensive* and do not fit well within established industry engineering pay bands
  - The cybersecurity professional pipeline is very narrow; cybersecurity is a relatively new field of study at universities
- Thus, professional development and more advanced standards are vital

Benefits Of The Standard

- Common terminology for the supply chain
- Industry consensus
- Sets minimum criteria for vehicle cybersecurity engineering
- Creates a key reference
- Builds trust

The Standard is a Baseline for Industry

Targeted to Vehicle Product Development

Cybersecurity Organization and Governance

Cybersecurity Engineering Throughout Lifecycle

Built To be Used as a Baseline for Vehicle Manufacturers and Suppliers

Lessons Learned, Training and Communication

Includes Post-production Processes

What Is In-Scope And Out-of-Scope?

In Scope

- **Specifies requirements for cybersecurity risk management** for E/E systems engineering thru concept development to decommissioning
- Provides a **cybersecurity process framework**
- **Provides a common language** to help communicate cybersecurity risk
- Applies to all vehicle E/E systems and their components and interfaces

Out of Scope

- specific cybersecurity **technology or solutions**
- requirements around **remediation methods**
- requirements for **telecommunications systems**
- requirements for **connected back-office**
- requirements for **electric vehicle chargers**
- requirements for **autonomous vehicles**

Represents Broad Industry Consensus

Areas of Consensus

- Definition and contributing dimensions of risk
- Impact must be assessed minimally for Safety, Privacy, Operations, and Finance
  - Safety must be drawn from an ASIL assessment
- Impact is assessed from the point of view of road users
- Ratings are all described as lower is better for the road user.
- Risk rated on a scale of 1 to 5

Where Consensus can be Achieved

Topics where Consensus Not Reached

- Method of Threat Scenario Identification
- Method of Attack Feasibility analysis
  - ISO18045: elapsed time, expertise, equipment, knowledge of the item or component, window of opportunity.
  - CVSS (Common Vulnerability Scoring System for computer systems)
  - “Attack vector-based approach”
- Method of Risk to Tolerance mapping

Standard Status

Balloting

- **On May 6, 21434 passed** the ISO Draft International Standard (DIS) ballot and the SAE Committee Ballot
  - Many comments collected
- **Draft Standard is published** and will be superseded by the final standard

Technical Development

- The Joint Working Group will meet throughout 2020 to resolve comments and **continue developing and strengthening** the standard
- Final Draft International Standard (FDIS) **ballot by Q1 2021**

2020 Outreach and Promotions

21434 Introduction Webinars

Regional Roll-out

- North America- February
- China and Asia-Pacific- May
- Europe- TBD

Webinar Archived Here

Media Promotions

- SAE Trade magazines

Presentations at early 2020 international events

(Suspended due to COVID-19)

Future Support and Promotions

21434 Implementation Guide

- Instruct developers in how to implement cybersecurity throughout product development

Introductory Training

- 21434 Training **to be released in Q3**

Future Advanced Training Modules

- Implementation
- Risk Management
- Product Development

Presentations at 2021 international events

(TBD: COVID-19)

Media Promotions

- SAE trade magazines
- Mainstream media outlets

In-depth 21434 Webinars (in global regions)

SAE Training: Managing Cybersecurity Risks Using ISO/SAE 21434

Stacey Stevens

Senior Product Manager, Professional Development

SAE International

Course Overview

- *Modality:* On Demand Course – Online
- *Length of course:* 5 hours
- *SMEs:* David Ward & Bill Mazzarra
- *Continuing Education Credits:* .5 CEUs
- *Course Launch:* End of August 2020

Course Objectives

By successfully completing this course, you'll be able to:

- Identify the cybersecurity processes and activities introduced in ISO/SAE 21434 and highlight the aligned work products
- Recite the activities in the development lifecycle aligned to ISO/SAE 21434 including how they differ from other development lifecycles
- Summarize the taxonomy of the work products introduced in the standard including the relationships of each
- Describe activities and work products that need to be applied post start-of-production to maintain the cybersecurity of the item or component
- Describe how the requirements in ISO/SAE 21434 are applied in daily operations to create organizational cybersecurity plans and processes

Course Outline

The 21434 course will cover the following modules:

- Module 1: Risk Assessment
- Module 2: Product Development
- Module 3: Ongoing Operations
- Module 4: Management System

Questions?

Stacey Stevens

Senior Product Manager, Professional Development

SAE International

stacey.stevens@sae.org

Tim Weisenberger

Senior Project Manager, Emerging Technologies

SAE International

tim.weisenberger@sae.org