J3101 as a Security Controls Library for ISO/SAE 21434

Bill Mazzara

SAE Hardware Security for Ground Vehicles - Chair

Using J3101

Agenda

- Introduce ISO/SAE 21434
- What is a Cybersecurity Controls Library
- Origins of J3101
- J3101 Common Requirements
- Future Direction of J3101 with GlobalPlatform

Bill Mazzara, SWX Cybersecurity Principal Engineer

Bill Mazzara, sets strategy for Product Cybersecurity as a part of the design of the new Vehicles. He is the SAE Vehicle Electrical System Hardware Security Subcommittee Chair which has published SAE J3101 and also serves on the SAE/ISO Joint Working Group for Road Vehicles Cybersecurity Engineering which has published ISO/SAE 21434. Involvement in the SAE has also lead to contributions through GRVA(CS/OTA) to UN ECE WP29 R155.

Having begun his career as a test engineer during the infancy of the connected car, Mazzara has witnessed and been a driving force in the evolution of the field being granted 29 related patents in the process. As it became apparent that the lack of cybersecurity was an unfortunate oversight of the connected car, Bill became part of the solution. Mazzara served on the response team charged with addressing what is widely considered one of the automotive industry's first cybersecurity incidents against a passenger vehicle, the incident chronicled in 2010 study by researchers from the Universities of California San Diego and Washington.

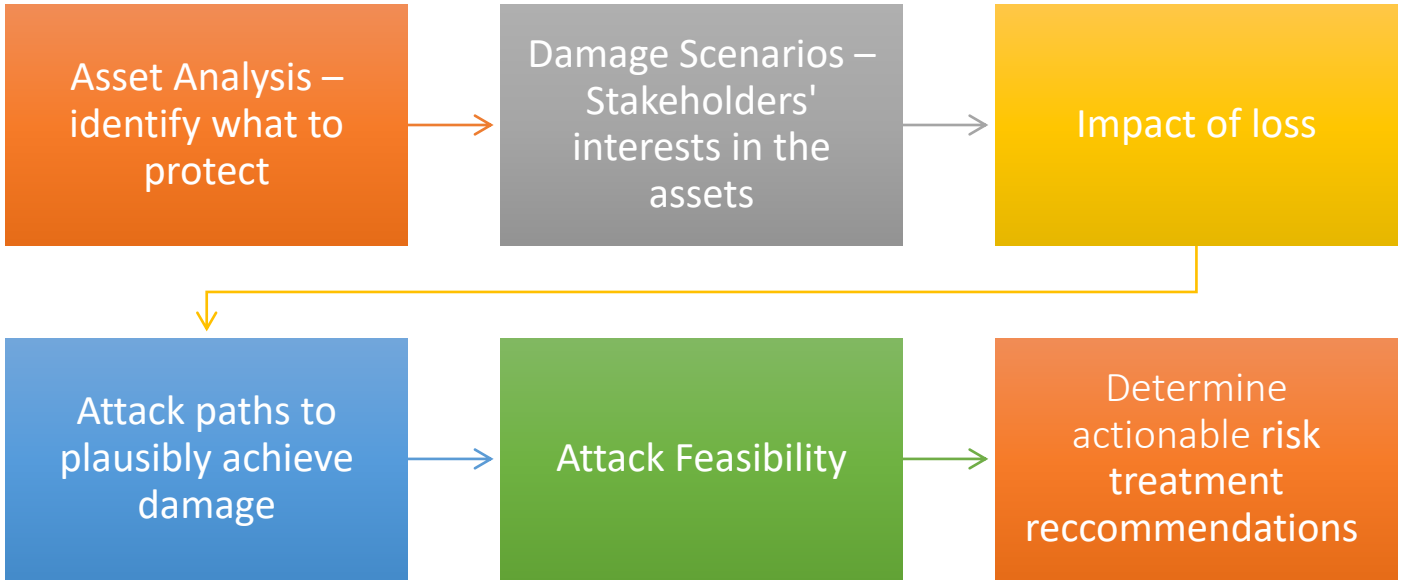
A Certified Information Systems Security Professional(CISSP), Mazzara holds a bachelor's degree in Electrical Engineering from the University of Notre Dame in addition to masters' degrees in wireless communications and business administration(MBA).

Formation of the Joint working Group

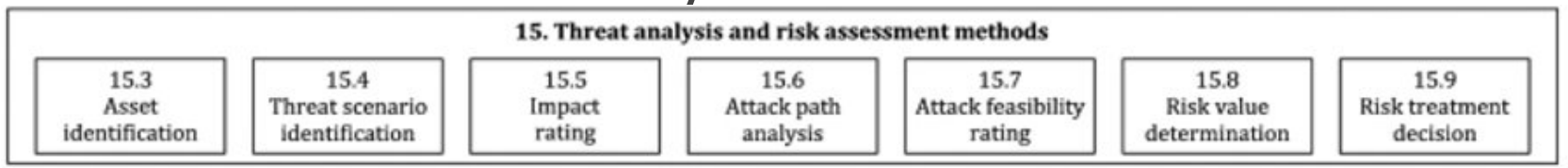
- In 2016 a Joint working group was formed to address the need
- ISO and SAE collaborated together on the creation of the standard
- The ISO/SAE 21434 Standard is a result of the efforts of a joint working group of more than 100 experts from 14 nations and 82 industry organizations across public, private, and government sectors
- Published Aug 31 2021
- This new standard expands on the same basic framework developed by SAE J3061™: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- Formulated to Align with ISO26262
- Leveraging principles found in the NIST Risk Management Framework

TARA based thinking

- The TARA, the last section (§15) of ISO/SAE 21434, describes a methodology and philosophy used as the foundation of the process of cybersecurity engineering throughout 21434.

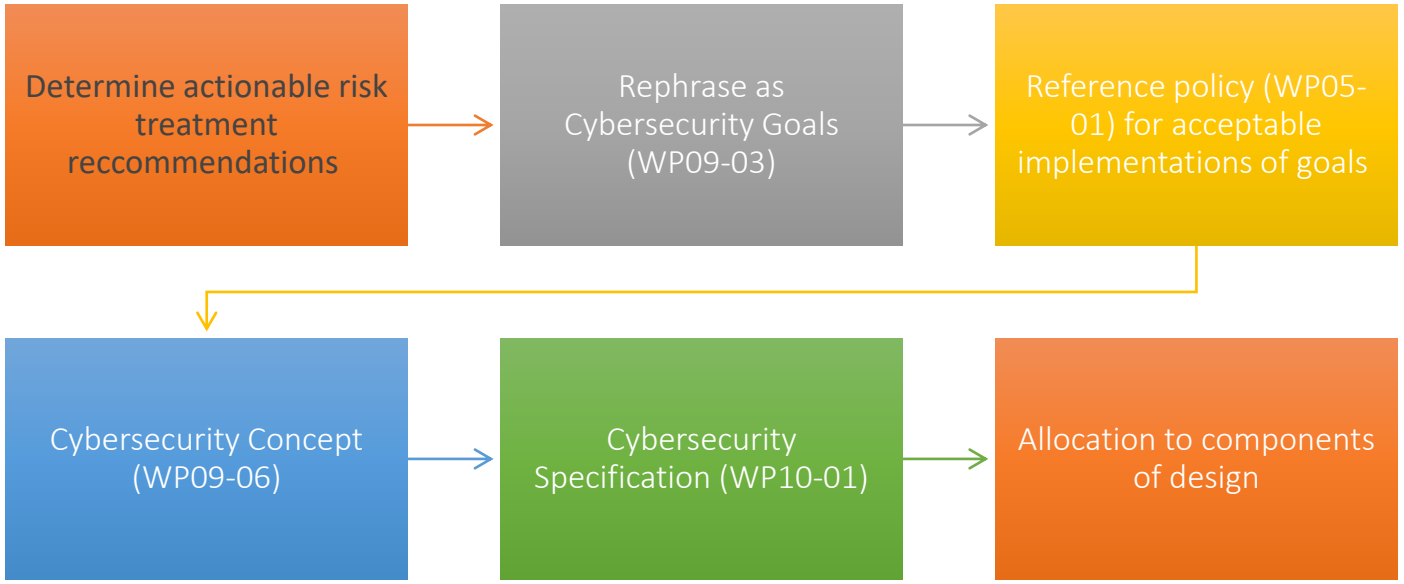


- Constrains risk into quantifiable terms
- Not needless anxiety



Risk Treatment Recommendations according to Policy

- **Policy :** Statements, rules or assertions that specify the correct or expected behavior of an entity. NIST 800-95
- Establishes the Risk Tolerances of an organization
- WP 05-01 : Policies Rules and Processes
  - Not just a mission statement



- Policies are characteristic standards of acceptable cybersecurity control to meet the common needs of an organization
- So where do Policies come from?

Cybersecurity Controls Library

- Descriptions of acceptable characteristics of Cybersecurity Mechanisms that offer designed to help meet compliance to policy
- A concept of the NIST Cybersecurity Framework (NIST 800-53) - Identify, Protect, …
- Cybersecuirty Mechanisms are a part of technologies adopted for solutions
- Internet Protocols = Transport Layer Security
- Wifi = Wifi Protected Access (WPA)
- Build your Policies rules and procedure leveraging the Cybersecurity Mechanisms of the technologies adopted
- What about automotive technologies?

J3101 : Hardware Protected Security for ground vehicles

- SAE J3101 – Published Feb 2020
- A collection of Common Cybersecurity Requirements
- Derived from common automotive use cases
  - Embedded Controller Boot
  - Embedded Controller Update
  - Secure In Vehicle Messaging
  - Access mechanisms
  - Data storage within embedded devices
  - Intellectual Property Protection
  - Diagnosis of an ECU
  - Data Logging
- New use cases in development (look for these publications from the SAE soon)
  - J3101-2 : **HPSE Trusted Application Isolation Security Models**
  - J3101-3 : **HPSE Management of Confidential Data**
  - J3101-4 : **Side Channel Attack Resistanace**
  - **The SAE will continue to document ways the HPSE can serve to secure automotive applications**

Common Requirements

- The following common requirements have been derived from the use cases detailed, and represent categories of hardware protected security environment functionality.
  - 1. Cryptographic key protection
  - 2. Crypto algorithm
  - 3. Random number generator
  - 4. Secure nonvolatile data
  - 5. Algorithm agility
  - 6. Interface control
  - 7. Secure execution environment
  - 8. Self-tests
- SAE J3101

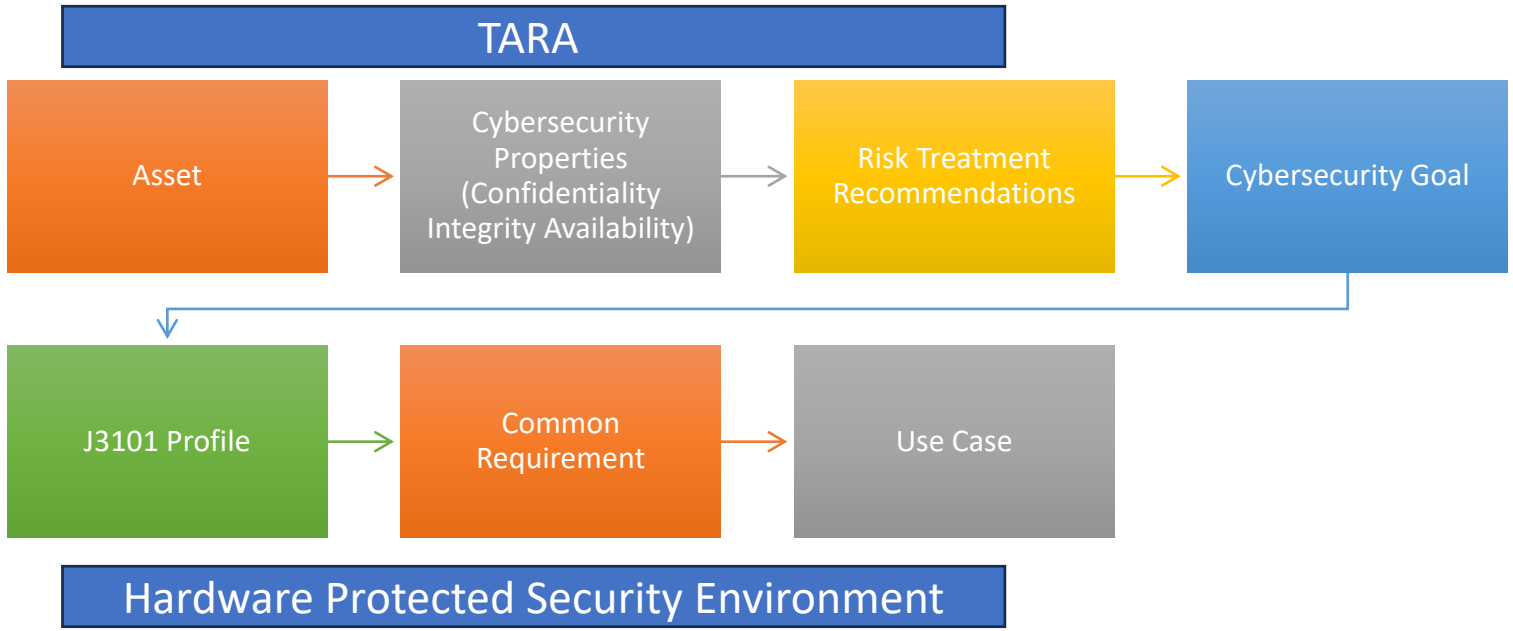
Hardware Profiles

- J3101 defines profiles forming groupings of the common requirements
- Each profile consists of a set of security features chosen based on the use cases that are typical for automotive systems.
- each profile is not a strict subset of another
- The profiles of hardware protected security environments are as follows:
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
  - Access control

Note the correlation to the Cybersecurity Properties required in the TARA according to ISO/SAE 21434

J3101 as a Security Controls Library for ISO/SAE 21434

- Based on the Cybersecurity Goals established for Risk treatment Recommendations to protect the Cybersecurity Properties of an Asset a J3101 Profile can be selected to provide a platform for common requirements useful in achieving automotive use cases



Implementation of J3101

ISO/SAE 21434 : [RQ-10-02] The defined cybersecurity requirements shall be allocated to components of the architectural design.

- J3101 is a description of common requirements not an implementation spec - challenging to allocate to a design
- J3010-1 Application Programming Interface Analysis - AutOSAr Classic Crypto API - Information Report
- Software Application Programming Interface (API) landscape for SAE J3101 devices,
- The purpose of this analysis was to identify how well the existing APIs cover the J3101
- By examining these APIs, the Task Force aimed to gain insights into the current state of API support for J3101 devices and identify any gaps in coverage that need to be addressed.
- Next : GlobalPlatform
- Can a GlobalPlatform Profile for J3101 be created?
- Can a GlobalPlatform Profile facilitate a SESIP Certification of J3101 Implementations?