SAE INTERNATIONAL

OVERVIEW OF RECOMMENDED PRACTICE - SAE J3061™

CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS

June 2016

Lisa Boran
Ford Motor Company
SAE J3061 Committee Chair

Barbara J. Czerny
ZF TRW
SAE J3061 Committee Member

David Ward, HORIBA MIRA
SAE J3061 Committee Member

AGENDA

- SAE Standardization Activities
- Motivation
- Main Content of J3061™
- Current Status
- Future Plans

SAE Portfolio. Reaching over 145,000 individuals in over 110 Countries.

PUBLICATIONS
100,000+ collection of technical publications

TECHNICAL STANDARDS
35,000+ aerospace and ground vehicle standards

MEDIA
Magazines, *e*Newsletters, custom publishing, Tech Briefs Media Group

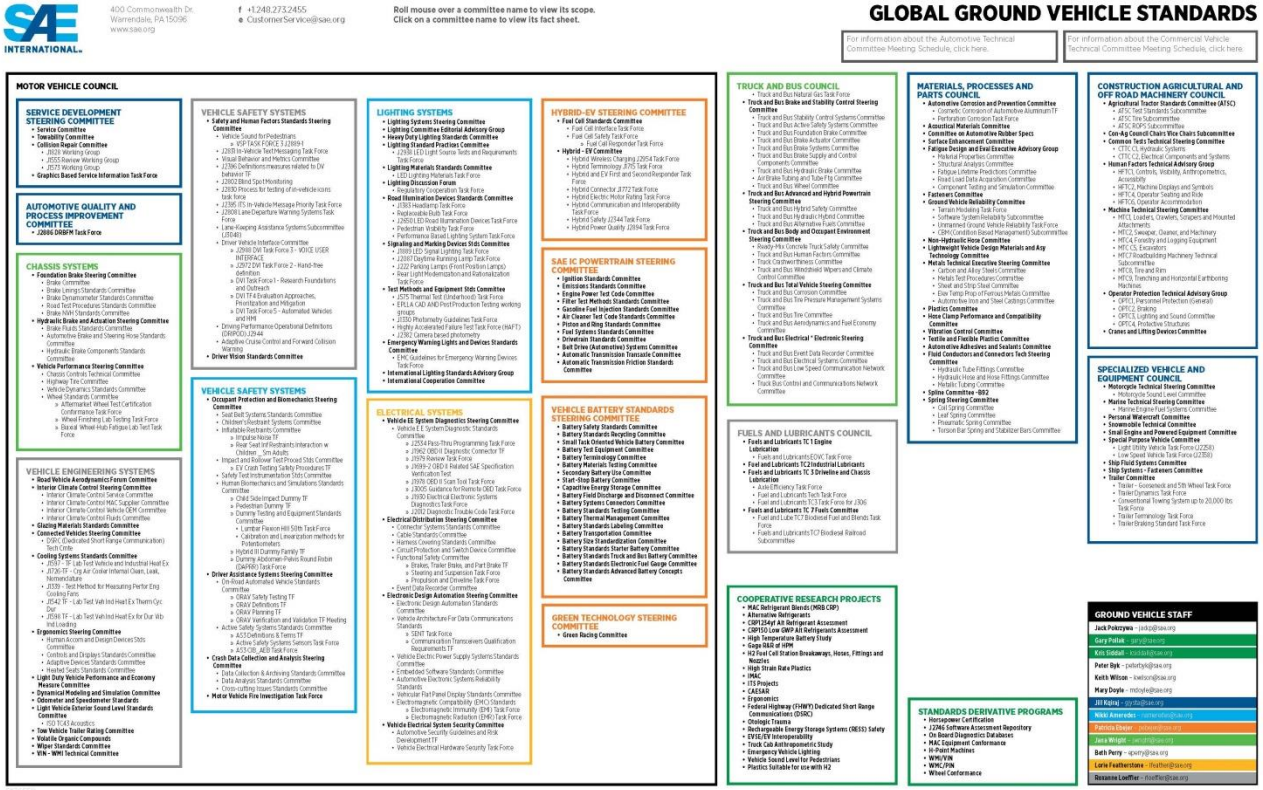
MEMBERSHIP
145,000 members worldwide, multiple-tiered/benefit model

MEDIA
Magazines, *e*Newsletters, custom publishing, Tech Briefs Media Group

FOUNDATION
Charitable arm of SAE International, supporting STEM for over 30 years

PROFESSIONAL DEVELOPMENT
400 courses portfolio, webinars; in-house, corporate and self-paced learning

SAE Standards Development



609 committees

8,865 members

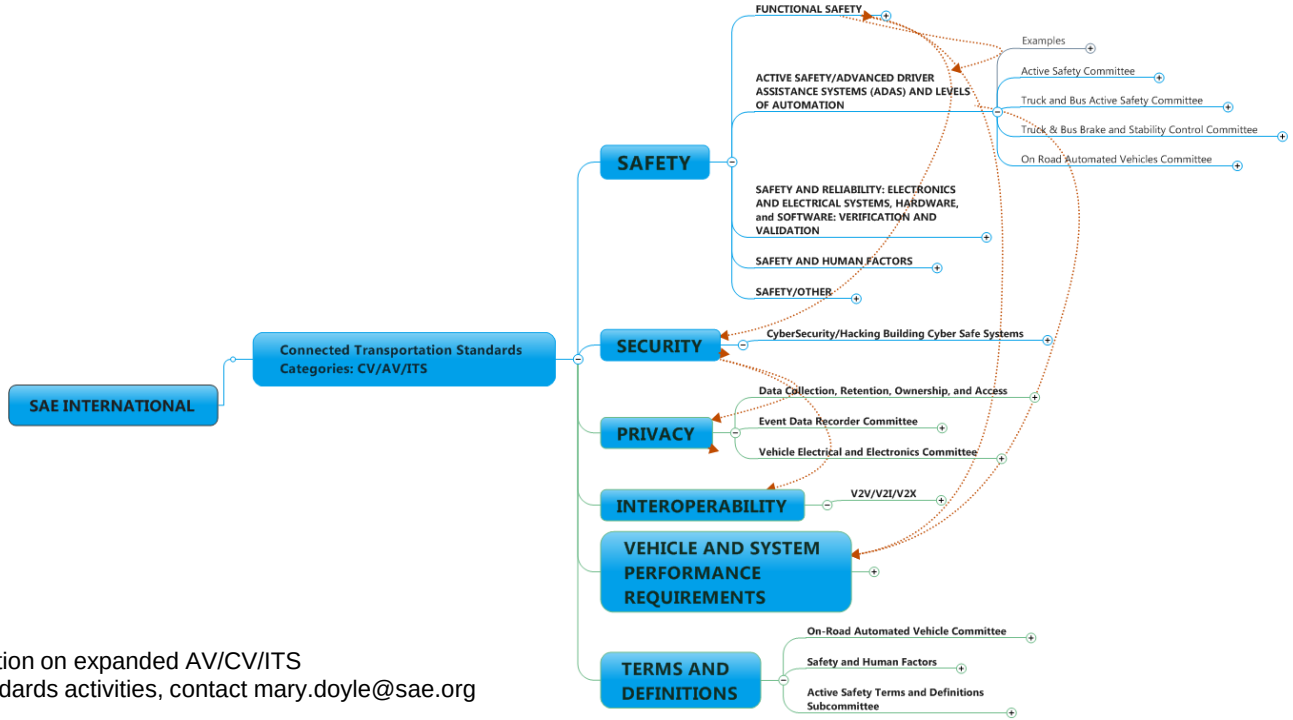
2,898 companies

1,423 meetings

Committee meetings are **open** to all interested parties, but **only committee members vote** on draft documents.

Individuals participate on committees as technical experts and **not** as representatives of their organizations

SAE'S Ground Vehicle Map of Standards for Connected, Automated and Cooperative Intelligent Transportation Systems



For information on expanded AV/CV/ITS
Map of standards activities, contact mary.doyle@sae.org

Why standards are needed: Safety Considerations

J2980™ – Considerations for ISO 26262 ASIL hazard classification

ISO 26262 contains requirements but a certain amount of "prior knowledge" is assumed

Guidance (including NOTES, EXAMPLES, most Annexes, and Part 10) are informative and are not comprehensive

Example: Part 3 (concept phase)

Original objectives

Develop a global harmonized approach to determining ISO 26262 ASIL classifications for vehicle level hazards

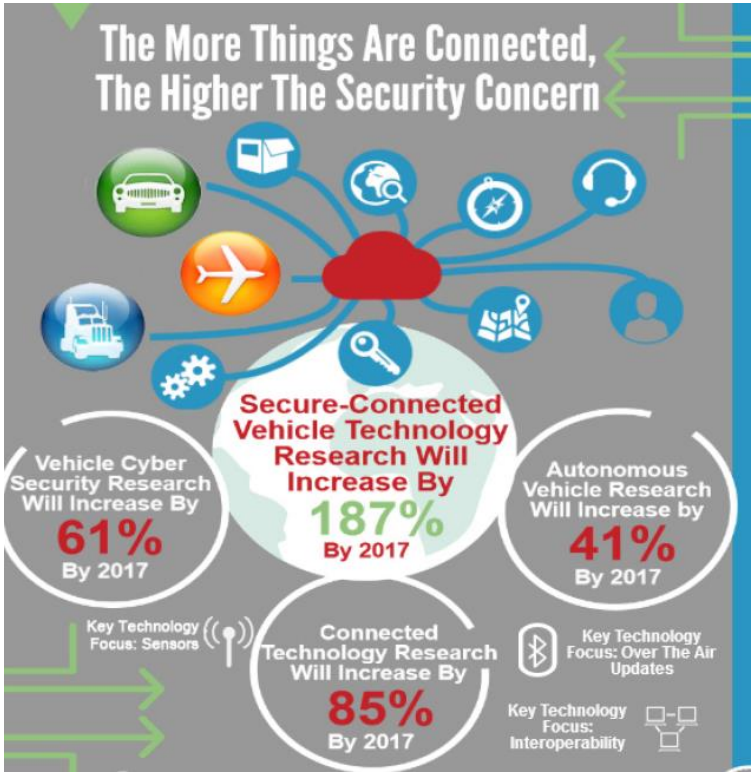
Develop global harmonized ASIL classifications for vehicle level hazards

Develop global standard hazard metrics for harmonized ASIL classified hazards

Now mostly concerned with guidance on a consistent process

Found very quickly it was not possible to agree on "global harmonized ASIL classifications"

Why standards are needed: Security Considerations



Infographic by Ashleigh N. Faith 2015

The connected world poses threats to:

- **Product Safety and Performance**
- **Data Integrity and Access**
- **Privacy**
- **Interoperability**

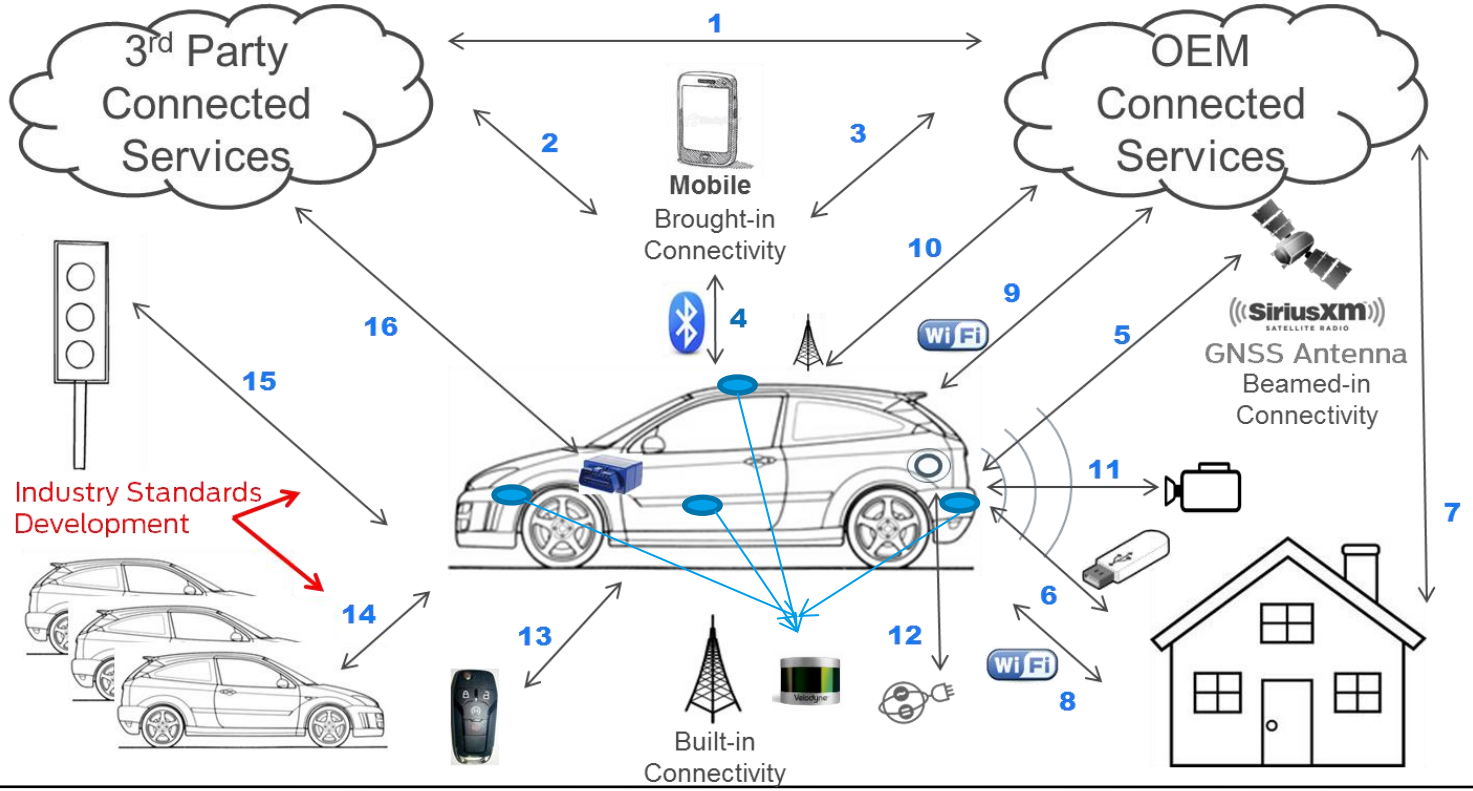
J3061™ Establishes needed guidance and recommendations for designing cybersecurity into the system including product design, validation, deployment and communication tasks

Motivation for Creating SAE J3061™

- Past Vehicle Design Emphasis was on Engine Design, Comfort and Chassis
  - Vehicle was self contained

Motivation for Creating SAE J3061™

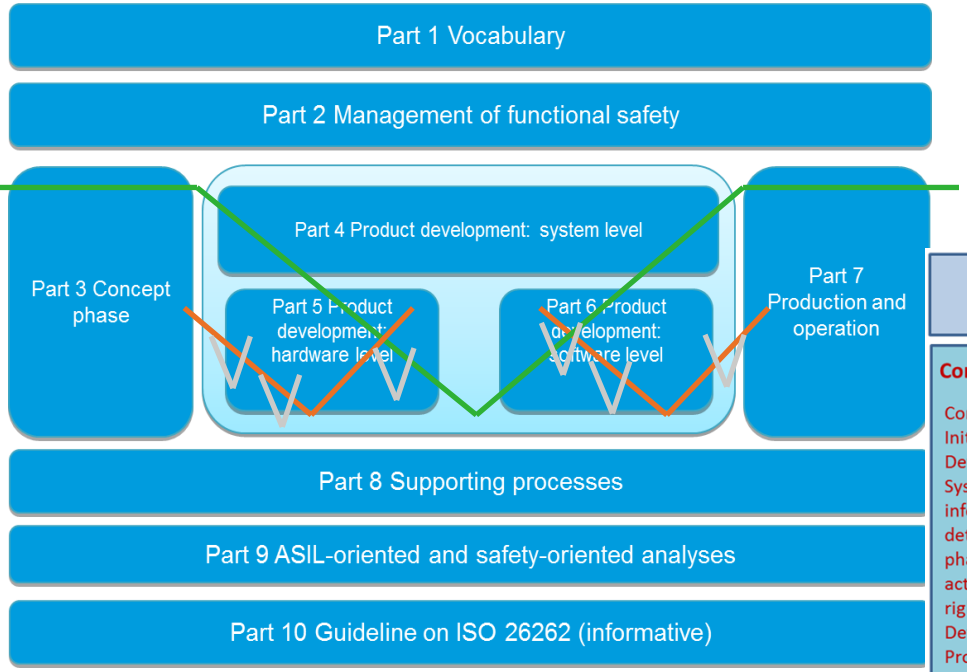
- Interconnectivity of today's and future vehicles makes them potential targets for attack



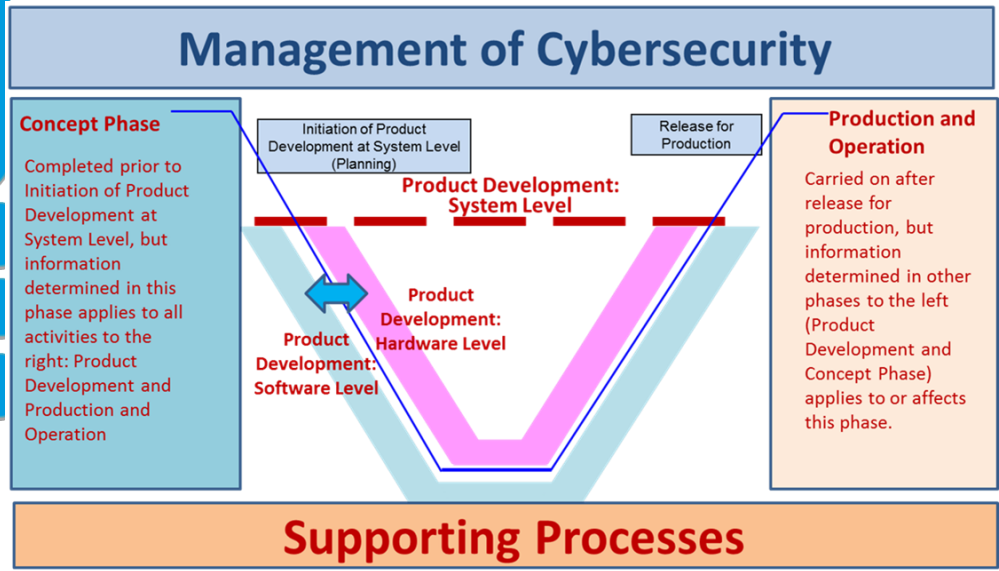
Motivation for Creating SAE J3061™

- Cybersecurity was relatively new to automotive, and most existing information did not address unique aspects of embedded controllers
- Cybersecurity principles, process and terminology are needed that can be commonly understood between OEMs, Tier 1 suppliers & key stakeholders
- A defined and structured process helps ensure that cybersecurity is built into the design throughout product development
  - Based on ISO 26262 Functional Safety process framework
  - No system can be guaranteed 100% secure
    - Following a structured process helps reduce the likelihood of a successful attack, thus reducing the likelihood of losses
    - A structured process also provides a clear means to react to a continually changing threat landscape

ISO 26262 Process Framework vs. Cybersecurity Process Framework



ISO 26262



SAE J3061™

Source: J3061™
Copyright SAE International

1. Scope

Describes the application and purpose of J3061™ and provides application guidance.

- Provides guidance on vehicle cybersecurity
  - Intended to be flexible, pragmatic, and adaptable in its application to the vehicle industry as well as to other cyber-physical vehicle systems
    - e.g., commercial and military vehicles, trucks, busses
- Defines a complete lifecycle process framework
- Provides information on existing tools and methods used when designing, verifying, and validating cyber-physical vehicle systems
- Provides high-level guiding principles on cybersecurity for CPVS
- Provides the foundation for further standards development activities in vehicle cybersecurity
- Provides guidance on when to apply a cybersecurity process

3. Definitions

Throughout the document, the initial use of a word contained in the definition section is bold italics.

Key Definitions

- Cyber-physical system – a system of collaborating computational elements controlling physical entities
- Cybersecurity – an attribute of a cyber-physical system that relates to avoiding unreasonable risk due to an attack
- Attack – exploitation of vulnerabilities to obtain unauthorized access to or control of assets with the intent to cause harm
- Threat – a circumstance or event with potential to cause harm
  - NOTE: Harm may be related to financial, operational performance, safety, reputation, privacy and/or sensitive data

Key Definitions
Vulnerability vs. Threat vs. Risk

Vulnerability

Risk = likelihood of attack|success

Threat

Source: AutoImmune

4. Relationship Between System Safety and System Cybersecurity

Provides an overview of system safety and system cybersecurity and how the two domains are related and different.

- Scope of cybersecurity is broader
  - All safety-critical systems are cybersecurity-critical systems, but not all cybersecurity-critical systems are safety-critical
- Describes the relationship between system safety engineering process elements and system cybersecurity engineering process elements
- Describes analogies between system safety and system cybersecurity engineering *(TARA - HARA, Attack Tree Analysis - Fault Tree Analysis)*
- Describes unique aspects of system safety and system cybersecurity

  (Accident or Faults vs. Purposeful Malicious Attack)

5. Guiding Principles on Cybersecurity for Cyber-Physical Vehicle Systems

Provides some general guiding principles with respect to cybersecurity that are applicable to any organization.

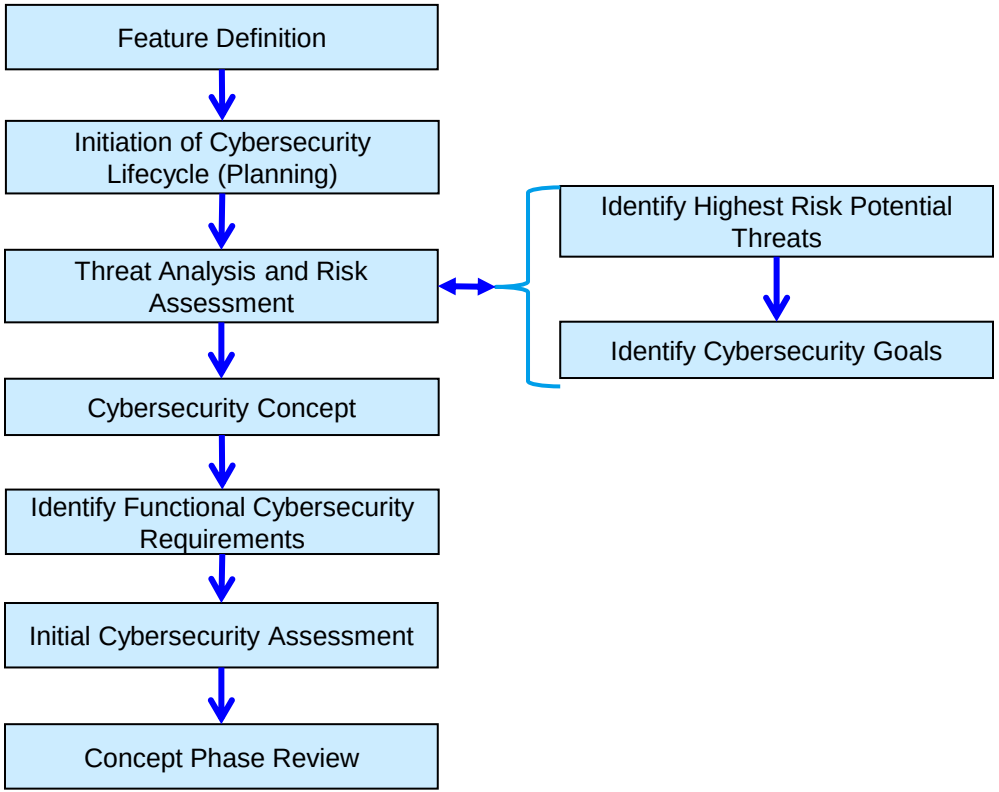
- Know your Feature's Cybersecurity Potential
- Understand key cybersecurity principles
- Consider the vehicle owners' use of the feature
- Implement cybersecurity in concept and design phases
- Implement cybersecurity in development and validation
- Implement cybersecurity in incident response
- Cybersecurity considerations when the vehicle owner changes

6. CYBERSECURITY PROCESS OVERVIEW

As with system safety, cybersecurity must be built into the feature rather than added on at the end of development. Building cybersecurity into the design requires an appropriate lifecycle process from concept phase through production, operation, service and decommissioning.

- Motivation for a well-defined and well-structured process
- Process Framework
  - Overall management of cybersecurity
  - Concept Phase
  - Product Development
    - Product Development: System Level
    - Product Development: Hardware Level
    - Product Development: Software Level
  - Production, Operation and Service
  - Supporting Processes
- Milestone and Gate Reviews

Concept Phase Flow Diagram



Source: J3061™
Copyright SAE International

7. OVERALL MANAGEMENT OF CYBERSECURITY

Creating, fostering, and sustaining a cybersecurity culture that supports and encourages effective achievement of cybersecurity within the organization.

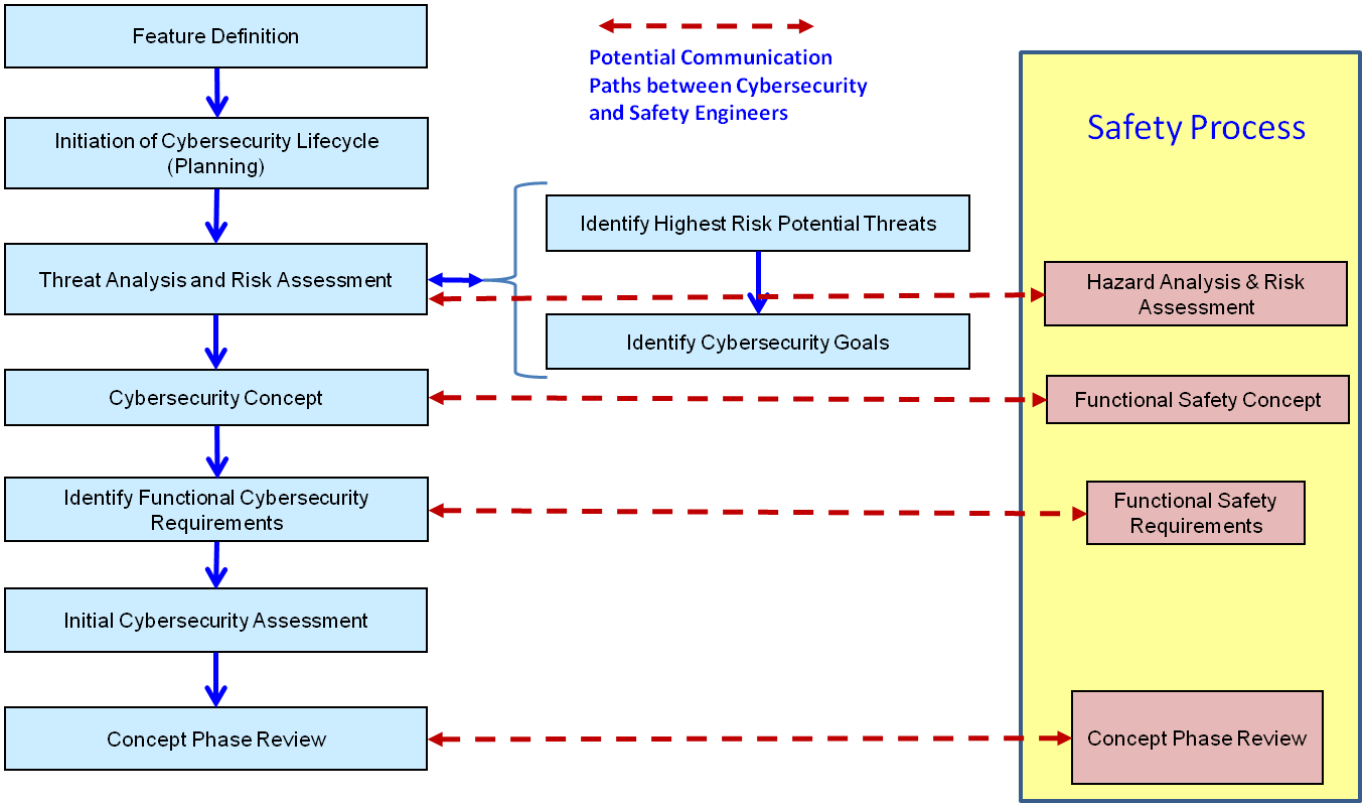
- Cybersecurity Culture
- Measuring Conformance to a Cybersecurity Process
- Identifying and Establishing Communication Channels
- Developing and Implementing Training and Mentoring
- Operation and Maintenance Activities
    - Incident Response Process
    - Field Monitoring Process

8. PROCESS IMPLEMENTATION

This section describes in detail the activities in each of the cybersecurity lifecycle phases discussed in the cybersecurity process overview section (Section 6). For each lifecycle phase, the activities are described and a description of a possible implementation of the activities is provided.

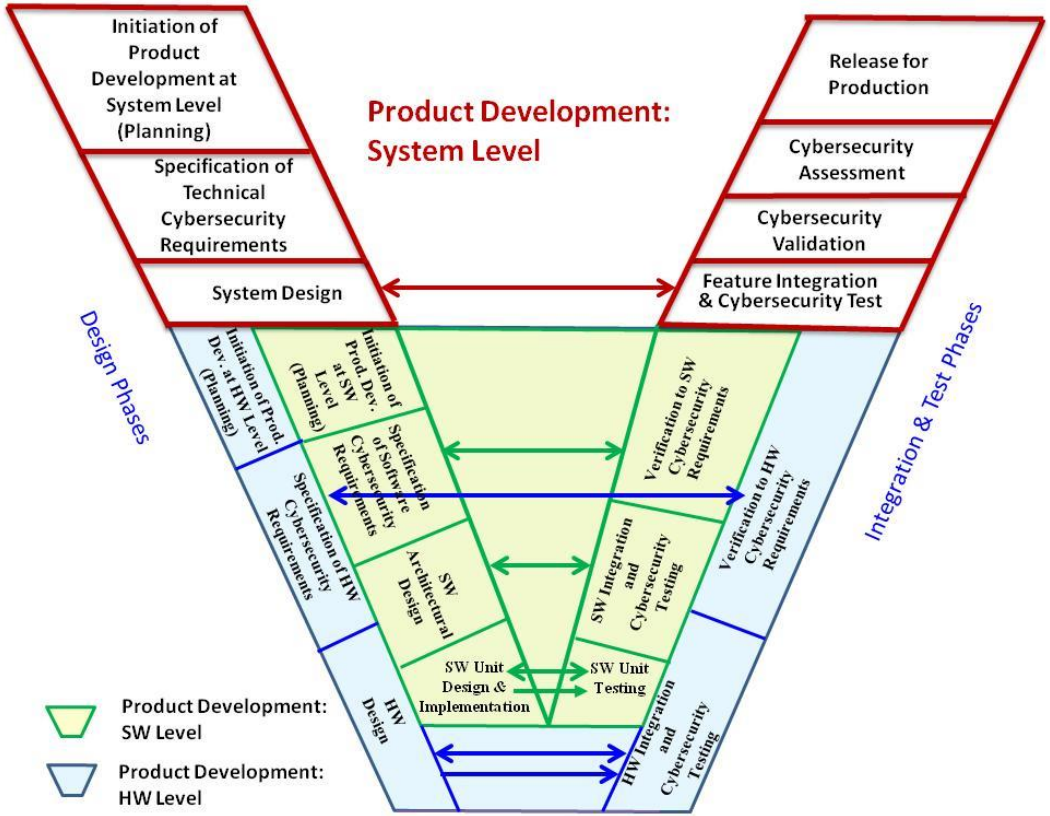
- Applying a Cybersecurity Process Separately with Integrated Communication Points to a Safety Process
- Applying a Cybersecurity Process in Conjunction with a Safety Process
- Concept Phase
- Product Development at the System Level
- Product Development at the Hardware Level
- Product Development at the Software Level
- Production, Operation and Service
- Supporting Processes

Potential Communications Paths During the Concept Phase Activities



Source: J3061™
Copyright SAE International

Cybersecurity V Model Relationship Between System, Hardware and Software Development Activities



Source: draft document J3061™
Copyright SAE International

APPENDIX A: DESCRIPTION OF CYBERSECURITY ANALYSIS TECHNIQUES

This sections provides a description of different analysis methods. This helps guide the reader to determine which method may better suit their needs and also provides a start on how to apply a particular one.

- Overview of Threat Analysis, Risk Assessment, & Vulnerability Analysis Methods
  - EVITA Method (E-safety Vehicle InTrusion protected Applications)
  - EVITA Applied at the Feature Level using THROP (Threat and Operability Analysis)
  - TVRA (Threats, Vulnerabilities and Risks (TVR) of a system to be Analyzed)
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  - HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety)
  - Attack Trees
  - Software Vulnerability Analysis
- Overview of Cybersecurity Testing Methods
  - Types of Penetration Testing
  - Red Teaming
  - Fuzz Testing

APPENDIX B: EXAMPLE TEMPLATES FOR WORK PRODUCTS

- OCTAVE Worksheets
  - OCTAVE Allegro, Information Asset Risk Worksheet
  - OCTAVE Allegro, Risk Mitigation Worksheet

APPENDIX C: EXAMPLES USING IDENTIFIED ANALYSES

- EVITA Application using THROP
- OCTAVE
- Attack Tree Analysis
- HEAVENS

APPENDIX D: SECURITY & PRIVACY CONTROLS DESCRIPTION AND APPLICATION

This appendix lists a sample set of 14 security control families and 5 privacy control families and a few controls within each family that might be applicable for automotive system security. The scope of coverage includes design, manufacturing, customer operation, maintenance, and disposal.

APPENDIX E: VULNERABILITY DATABASES AND VULNERABILITY CLASSIFICATION SCHEMES

This appendix provides examples of dictionary and terminology sources for vulnerability databases (e.g. Common Weakness Enumeration, CWE) , vulnerability databases (e.g. BugTraq), and vulnerability classification schemes (e.g. Common Weakness Scoring System, CWSS).

APPENDIX F: VEHICLE LEVEL CONSIDERATIONS

Appendix F discusses aspects of vehicle-level Cybersecurity.

- Architecture design considerations and partitioning using the NIST approach
  Identify→ Protect→ Detect→ Respond→ Recover
- After vehicle sale considerations (defaults, erasing, etc.)
- End of life considerations
- Communication reporting expectations from the supplier

APPENDIX G: CURRENT SECURITY STANDARDS & GUIDELINES THAT MAY BE USEFUL TO AUTOMOTIVE INDUSTRY

Appendix G lists Standards and Guidelines from a variety of sources (e.g. NIST, FIPS, DHS, DARPA) that may be useful for members of the Vehicle Industry in understanding the overall Security realm, and in determining the details of implementing Cybersecurity into their organizations.

APPENDIX H: VEHICLE PROJECT AWARENESS

Appendix H summarizes the key research projects on Vehicle Cybersecurity beginning with 2004 and up through the present . Examples are EVITA, SESAMO, HEAVENS.

APPENDIX I: SECURITY TEST TOOLS OF POTENTIAL USE TO THE VEHICLE INDUSTRY

Appendix I lists some security test tool categories, and descriptions, for testing tools that may be of potential use to the vehicle industry for Cybersecurity.

- Static Code Analyzer
- Dynamic Code Analyzer
- Network Traffic Analyzer
- Vulnerability Scanner
- Fuzz Tester
- Exploit Tester
- Encryption Cracker
- Hardware Debugger
- Known Answer Tester
- Application Tester
- Interface Scanner
- Network Stress Tester

Current Status of J3061™ Surface Vehicle Recommended Practice

- Three formal internal committee ballots performed (86% approval or higher received)
- Completed the 28-day Motor Vehicle Counsel Ballot (80% participation with 70% approve and 10% waive)
- Released January 15, 2016

"SAE J3061™: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" is available for sale at http://standards.sae.org/j3061_201601/ and an on-demand webinar reviewing SAE J3061™ is also available

https://event.webcasts.com/starthere.jsp?ei=1080592

Special Thanks!

Additional Authors of J3061™

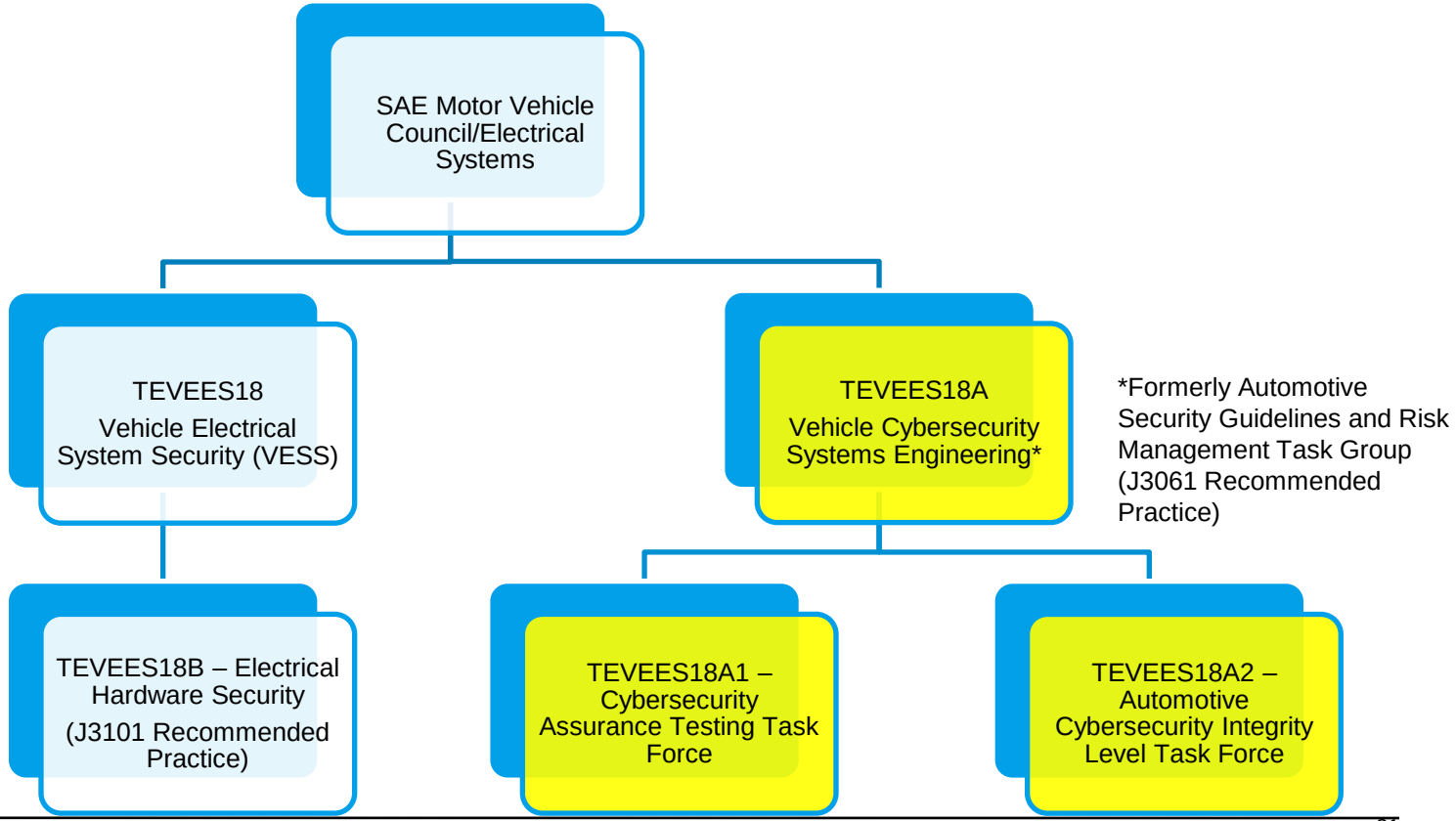
- Brian Anderson, SwRI
- Angela Barber, GM
- Kevin Harnett, DOT
- Mafijul Islam, Volvo
- Justin Mendenhall, Ford
- Steve Siko, FCA
- Priyamvadha Vembar, Bosch
- David Ward, MIRA
- Tim Weisenberger, DOT

In addition there were a number of other people that contributed to the development of the document and we would like to thank those people as well!

AGENDA

- Motivation
- Main Content of J3061™
- Current Status
- Future Plans

SAE Vehicle Cybersecurity Subcommittees



*Formerly Automotive Security Guidelines and Risk Management Task Group (J3061 Recommended Practice)

J3061 Future Plans

Objective: New SAE Committee (Vehicle Cybersecurity Systems Engineering) has the following Scope:

> *"To update the current J3061 recommended practice document to move J3061 closer to becoming a standard to allow cybersecurity robustness to be designed and built into cyber-physical vehicle systems"*

Work in Progress (WIP) to revise J3061 under new committee opened in February 2016

Areas to be Developed and Refined to Achieve Objective:

- Develop Common Threat Analysis and Risk Assessment Method and Corresponding **Automotive Cybersecurity Integrity Level (ACSIL)** Classification Scheme

- Identify Specific Details for each Lifecycle Phase in the Cybersecurity Process Framework
  - Associate specific process application details with each ACSIL

- Determine **Cybersecurity Countermeasure** Recommendations for each ACSIL

- Develop **Cybersecurity Assurance Testing** Recommendations

J3061 Future Plans (Cont'd)

TEVEES18A1 – Cybersecurity Assurance Testing Task Force

- Develop appropriate SAE documentation for cybersecurity assurance testing and evaluation
- The task force shall become more familiar with what types of testing and ***evaluations*** are effective in measuring claims of cybersecurity development practices and mechanisms
- The task force shall work towards creating a consistent framework where all ***systems and components*** throughout the extended supply chain are *evaluated with a common set of criteria*
- The goal is to produce a common means of ***evaluation criteria*** wherein Stakeholders can sign off on the hardware and software ***configuration*** received with confidence that the expected level of cybersecurity ***evaluation criteria*** has been **met**.
- The task force shall leverage existing work that has been previously accomplished by security experts and testing organizations

J3061 Future Plans (Cont'd)

Automotive Cybersecurity Integrity Level (ACSIL) Classification Task Force Objectives

- Review existing classification schemes from other industries and existing ideas that were presented at SAE or that may be being proposed or used in other organizations

- Determine to use either an existing classification scheme or create a new classification scheme specific for the automotive industry from the existing or proposed methods or ideas
  - A new classification scheme would most likely be an integration or merging of existing or proposed methods

- Determine a Threat analysis and Risk Assessment (TARA) method that would work with the classification scheme or from which we could map into a specific level in the cybersecurity integrity level classification scheme
  - This will require reviewing existing TARA methods and deciding on an existing method, or a tailored version of existing methods

- Determine how to relate the ACSIL for safety-related threats to the ASIL from ISO 26262

J3061 Future Plans – Standards Development Issues

- ISO/TC 22/SC 32 (Electrical and Electronic Components and General System Aspects)
- Germany, supported by the Verband der AutomobileIndustrie (VDA) members, are interested to develop an "international" standard for automotive security – *"Road Vehicle - Automotive Security Engineering"*
- SAE/US proposed to develop a joint SAE/ISO "international" standard for automotive cybersecurity – "*Road Vehicles – Vehicle Cybersecurity Engineering*"
  - Propose using J3061 as the foundation and follow the SAE standards development process
    - The SAE international standards development process is quicker than the ISO standards development process
      - Would allow a joint SAE/ISO international cybersecurity standard to be developed more quickly
      - J3061 was developed to be used as a foundation for a standard development
  - Extensive discussion and agreement between SAE, ISO,VDA on this proposal since July of 2015
  - Each organizations' ballot process will be followed.
  - Follows existing Pilot program proposal for Joint Standards Development between ISO and SAE (already underway)
- SAE/ISO Negotiation still in progress
  - Both SAE and ISO issued their own New Work Item Proposal (NWIPs)
  - No conclusion if a joint effort will be agreed to
  - SAE/ISO Meeting in Berlin (June 2016)

New webinar: “Keys to Creating a Cybersecurity Process from the J3061 Process Framework”

Session 1

Brief History of Automotive Security and Cybersecurity

Cyber-Physical Systems

Reactive vs. Proactive Approach to Cybersecurity

What is a Process?

Key Concepts in Cybersecurity Defined

Introduction to J3061

When to Apply a Cybersecurity Process

Cybersecurity Process Overview

Session 2 Cybersecurity Process Details

Overall management of cybersecurity

Concept phase

Product development at the system, hardware and software levels

Session 3 Production, Operation and Service

Supporting Processes

Relationship between Cybersecurity Process and Safety Process

Review of Appendices A, C-E, G-I

Tailoring the J3061 Process Framework into an Internal Process

Examples of Key Analysis Activities

Summary

http://training.sae.org/webseminars/wb1604/

Thank You!

If interested in participating in any of the 4 SAE Cybersecurity Committees:

TEVEES18 – Vehicle Electrical System Security
TEVEES18A – Automotive Security Guidelines and Risk Management
(J3061 Recommended Practice)
- Reopened as full Committee - 'Vehicle Cybersecurity Systems Engineering'
TEVEES18A1 – Cybersecurity Assurance Testing Task Force
TEVEES18A2 – Automotive Cybersecurity Integrity Level (ACsIL) Task Force
TEVEES18B – Electrical Hardware Security
(J3101 Recommended Practice)

Contact:
Lorie Featherstone <lfeather@sae.org>