G-32 Overview - Addressing the Need for a Cross-Industry Collaboration for Cyber-Physical Systems Security

June 2020

Daniel DiMase

Opening Agenda

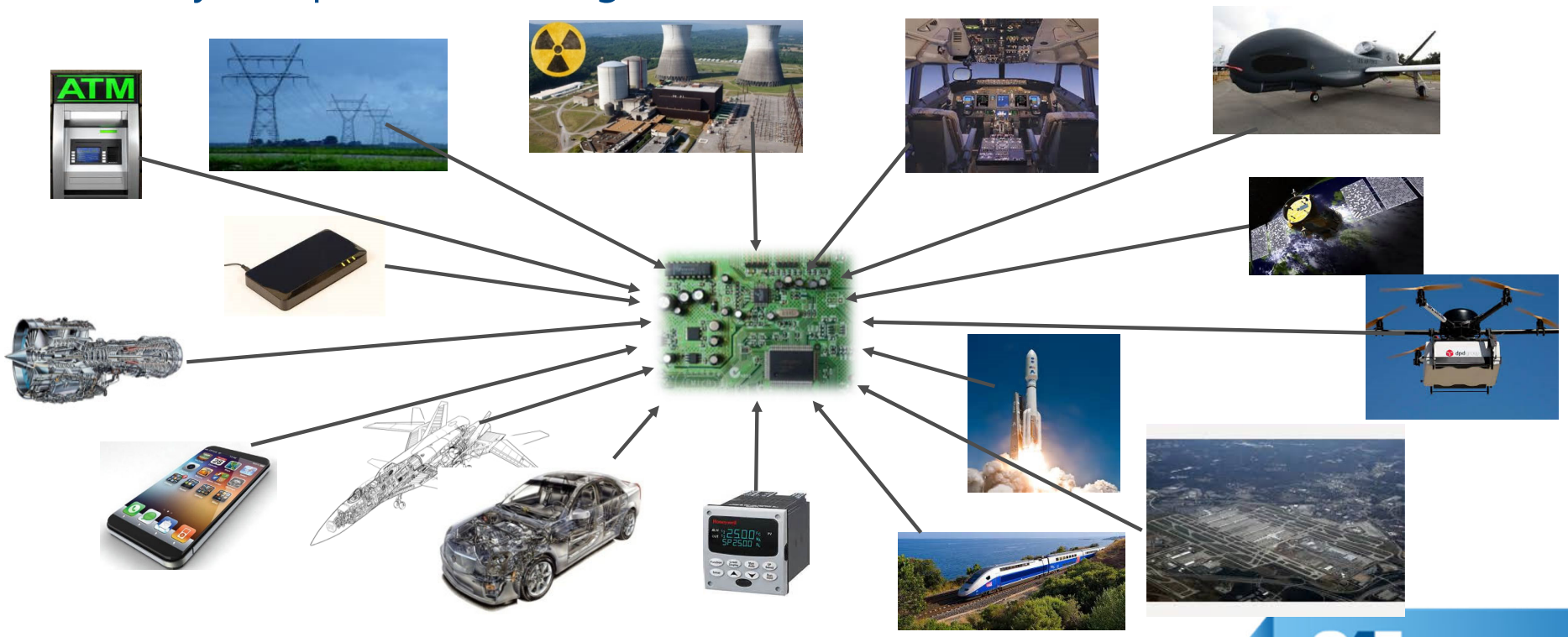
- Terms, Definitions and Taxonomy
- What's Different from Traditional Cyber Security?
- Awareness and Examples of the Threat
  - Impact and Consequences
- SAE G-32 Cyber Physical Systems Security Committee Overview & Objectives

Ensuring Cyber Physical Systems Security

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Cyber Physical Systems (CPS)

A Cyber Physical System (CPS) is a system in which a mechanism is controlled or monitored by computer-based algorithms.



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

What is different from traditional Cyber Security?

Cyber security definition is[1] - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Cyber Physical Systems Security

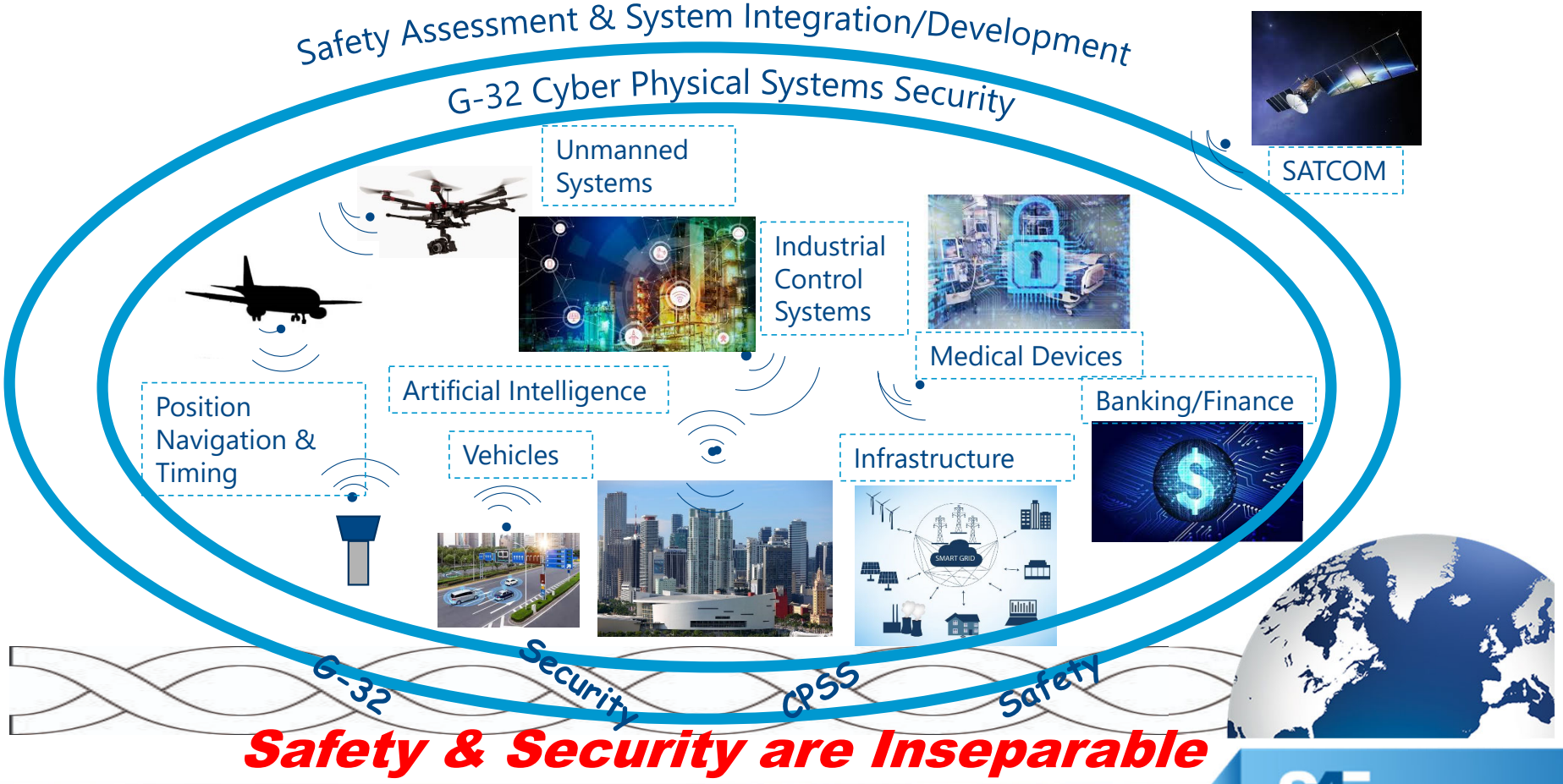
New cyber RISKS come from threats that can exploit weaknesses and vulnerabilities in cyber physical systems with the integration of complex hardware, software, and firmware. These vulnerabilities drive establishment of the area of cyber physical systems security.

- Proactive and coordinated efforts are needed to provide security and resilience for cyber physical systems.

[1] *https://www.merriam-webster.com/dictionary/cybersecurity*

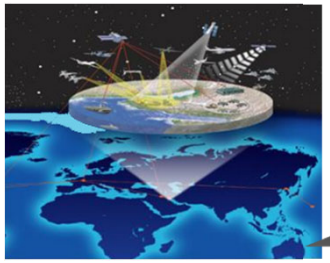
Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Interactions of G-32 and Others



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Understanding Cyber Physical Systems and Systems Security Engineering



System Safety & Cyber Security

System Integration

Cyber Physical System

Software

Firmware

Hardware

Electronic Parts and Assemblies

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Cyber Security - Problem Statement

- Threats to security covers a broad range of attack vectors with the integration of complex hardware, software, and firmware supporting the cyber physical system
- Attack vectors are introduced through vulnerabilities in electronic parts associated with tampering and from sources that have not been verified for trust
- Attack vectors are introduced through hostile code at the time of software or firmware updates
- Cyber system vulnerabilities include software, hardware, firmware, adjacent systems in the network, energy supplies, supply chain, and users who interface with it
- Requires a holistic risk management framework that addresses physical, information, cognitive and social domains to ensure resilience

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

How realistic are the threats? Cyber News in Aviation

Hackers just found serious vulnerabilities in a U.S. military fighter jet[35]

"They were able to get back in through the back doors they already knew were open," Will Roper, the Air Force's top acquisition official, told me in an exclusive briefing of the results. **He pinned the weaknesses on decades of neglect of cybersecurity as a key issue in developing its products, as the Air Force prioritized time, cost and efficiency.**

Hackers can easily hack the plane's CAN bus system and take control of key navigation systems[32 & 33]

"The Department of Homeland Security issued an alert Tuesday warning that small aircraft are vulnerable to hackers that can gain physical access to a plane. **It warned that a hacker can easily manipulate aircraft telemetry data, which can result in loss of control of the airplane.**"

Aviation Faces Increasing Cybersecurity Scrutiny[41]

"IOActive researcher Ruben Santamarta disclosed security flaws in an on-board network component … that he said **could allow a remote attacker to reach the sensitive avionics network** — aka the crew information systems network — on the plane."

"A researcher at cybersecurity company IOActive, **was able to spy on all those planes due to vulnerabilities in satellite communications equipment**, such as antennas sending data up to aircraft and the modems within. All could be exploited remotely, without needing physical access to the hardware."[31]

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Cyber News in Automotive

Chinese Hackers Find Over a Dozen Vulnerabilities in BMW Cars[56]

Chinese security researchers have discovered more than a dozen vulnerabilities in the onboard compute units of BMW cars, some of which can be exploited remotely to compromise a vehicle.

A flaw in a connected alarm system exposed vehicles to remote hacking[57]

The researchers said it was easy to locate a nearby car, unlock it, and drive away.

Team of hackers take remote control of Tesla Model S from 12 miles away[58]

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Cyber News in Medical Devices

Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch[59]

"Medical device maker Abbott… announced it is voluntarily recalling some 465,000 pacemakers to install a firmware update to patch cybersecurity vulnerabilities in the devices."

Hospital Medical Devices Used As Weapons In Cyberattacks[60]

"Security firm discovered malware-infected medical devices in three hospitals hit by data breaches. … a new report confirms that hospital medical devices are being abused by cybercriminals and possibly cyberspies as a stepping-stone within healthcare networks to nab valuable healthcare identities and information."

IoT security warning: Cyber-attacks on medical devices could put patients at risk[61]

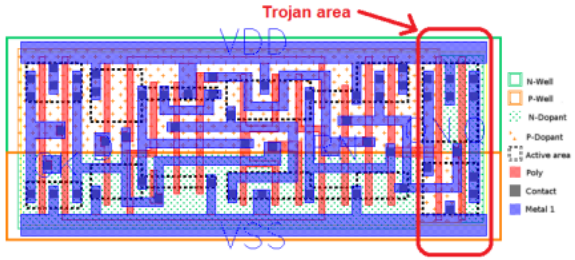
"Cyber-attacks on connected devices could therefore result in "severe consequences on patient safety", which could even result in injury or worse."

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Vulnerabilities, Embedded Malware and Hardware Trojans

Dopant Trojans:[14]

"A gate of the original design is modified by applying a different dopant polarity to specific parts of the gate's active area." This Trojan can essentially disable the embedded encryption protection of a chip.



How To Hack An Aircraft[34]

"After the 2008 crash of Spanair flight 5022, it was discovered that a central computer system used to monitor technical problems in the aircraft was infected with malware."

ProASIC Hacking:[16]

The paper explained how a cheap and simple approach was able to negate the encryption protection of the device.

Cyber Physical System Susceptible to Compromising Attacks Due to Electronic Parts with Vulnerabilities or Embedded Malware or Hardware Trojans

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

SAE G-32 Cyber Physical Systems Security Committee – Call to Action

- Cultivate a vigorous group (on-going)
- Everyone should reach out to their contacts to enlist new group members
- Cultivate the best Subject Matter Experts (SMEs) to help
- Draft standard(s) that integrates domains of consideration for requirements definition and risk different areas of concern for the system that includes consideration for hardware and software components (HwA/SwA)

Addressing Assurance, Security and Resiliency

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

SAE G-32 Committee Charter

2.1 Scope

…Though this committee is chartered under the SAE Aerospace Council's authority, its **documents are intended for broad industry use** (commercial, defense, and other high reliability and/or critical systems in aerospace, transportation, medical, etc.).

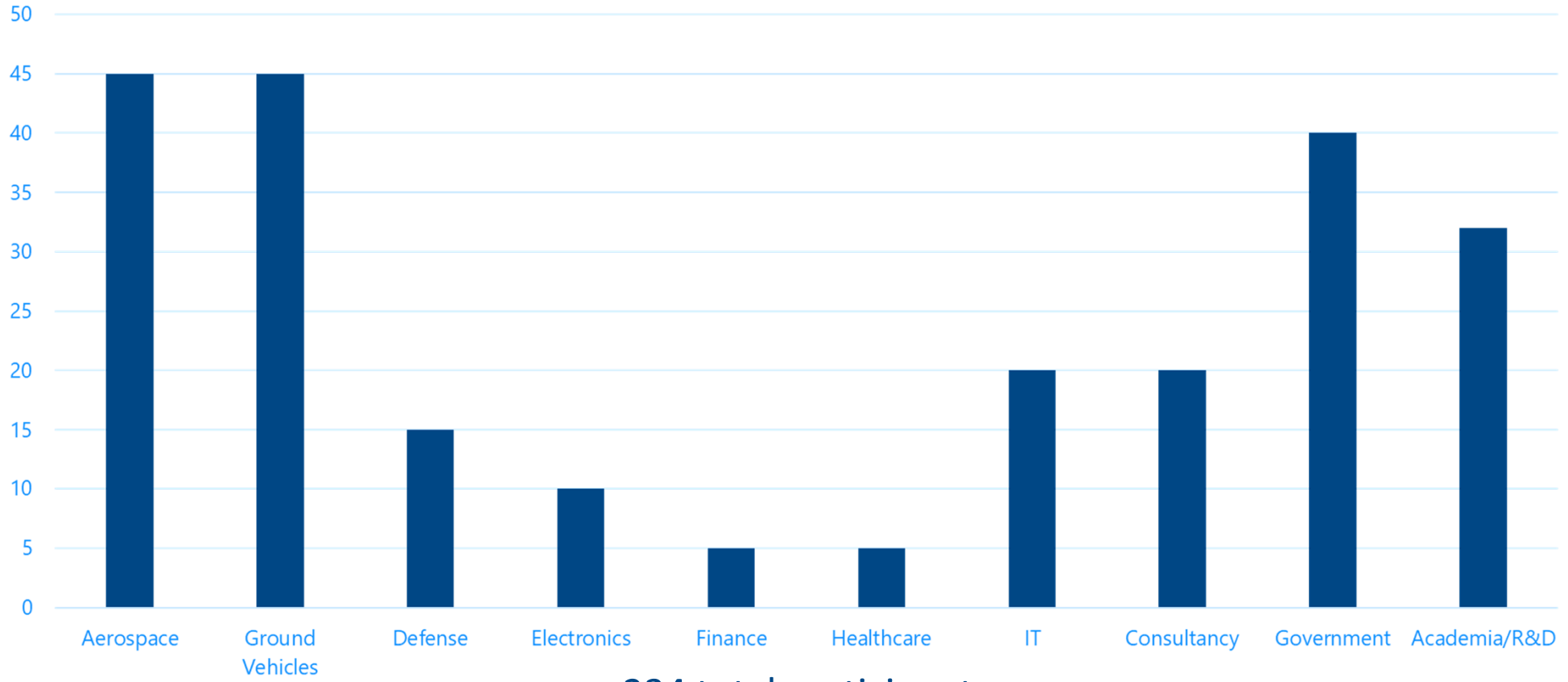
2.2 Objectives

SAE G-32 shall utilize and coordinate the knowledge, experience, and skills of technical experts in the field of CPSS to:

1. Characterize and address the risk to CPSS, assess vulnerabilities, and recommend System Engineering focused mitigation actions.
2. Share the knowledge of how vulnerabilities are introduced and exploited in cyber physical systems.
3. Document best practices for addressing areas of concern utilizing existing processes, procedures, and standards.
4. Develop a taxonomy for CPSS.
5. Establish standard methods for identifying vulnerabilities in cyber physical systems introduced at any point in the CPSS life cycle and mitigating impacts.
6. Develop validation and verification methods to ensure requirements are addressed.

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

SAE G-32 Committee Members



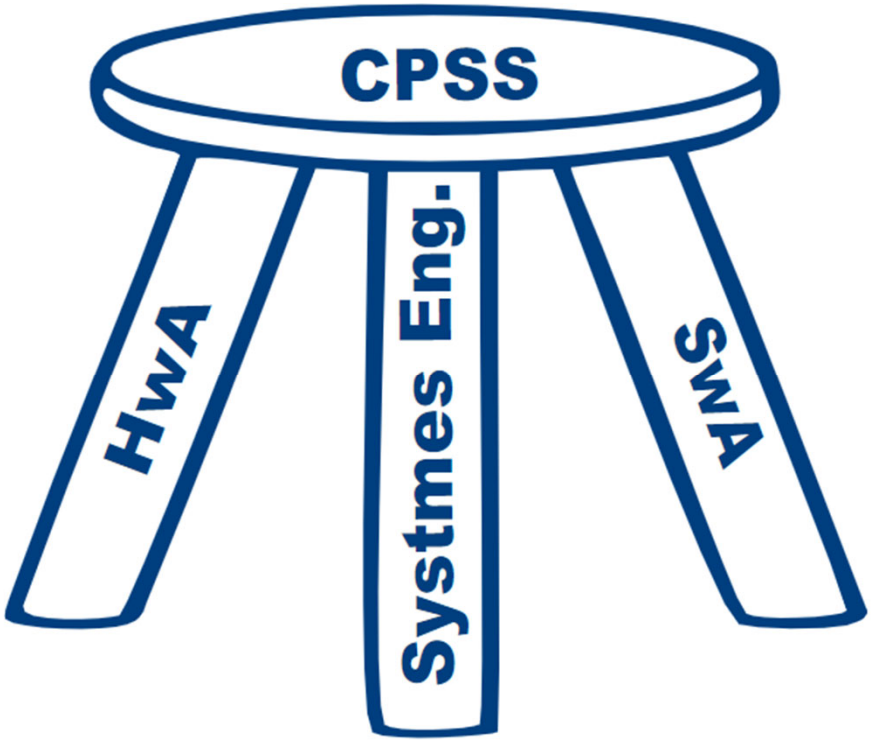
234 total participants

(as of May 28th, 2020)

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

SAE G-32 Committee Approach to Cyber Physical Systems Security

Cyber Physical Systems Security is enabled and supported by Systems Engineering (including Systems Security Engineering), Software Assurance, and Hardware Assurance



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Structure & Documents

Leverage existing standards and invent only when necessary

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Structure & Meetings

Main Committee – weekly WebEx

- Co-Chairs: Bill Scofield - Boeing and Daniel DiMase – Aerocyonics

SwA Subgroup – weekly WebEx

- Co-Leads: Andreas Schweiger – Airbus and Chris Sundberg - Woodward

HwA Subgroup – bi-weekly WebEx

- Co-Leads: John Hallman - OneSpin Solutions

Risk Management Framework Subgroup – weekly WebEx

- Co-Leads: Howard Miller - LBW Insurance & Financial Services and Zach Collier - Collier Research Systems

Systems Security Engineering V Overlay Subgroup – weekly WebEx

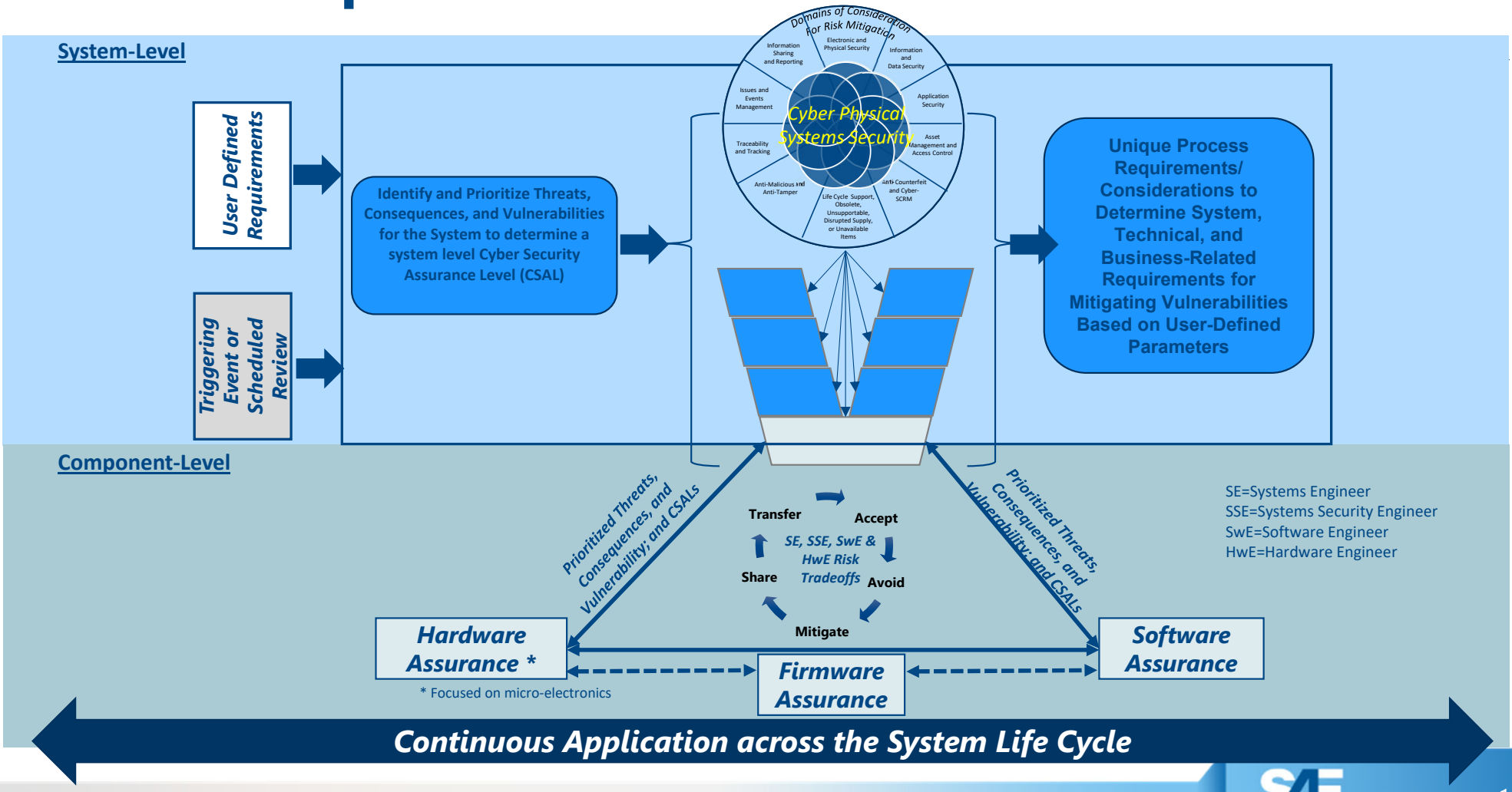
- Co-Leads: Jay Mandelbaum - Institute for Defense Analyses (IDA) and Gloria D'Anna - Ford Motor Company

Illustrative Example Subgroup – bi-weekly WebEx

- Co-Lead: Kenneth Crowther – GE Global Research

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Conceptual Framework

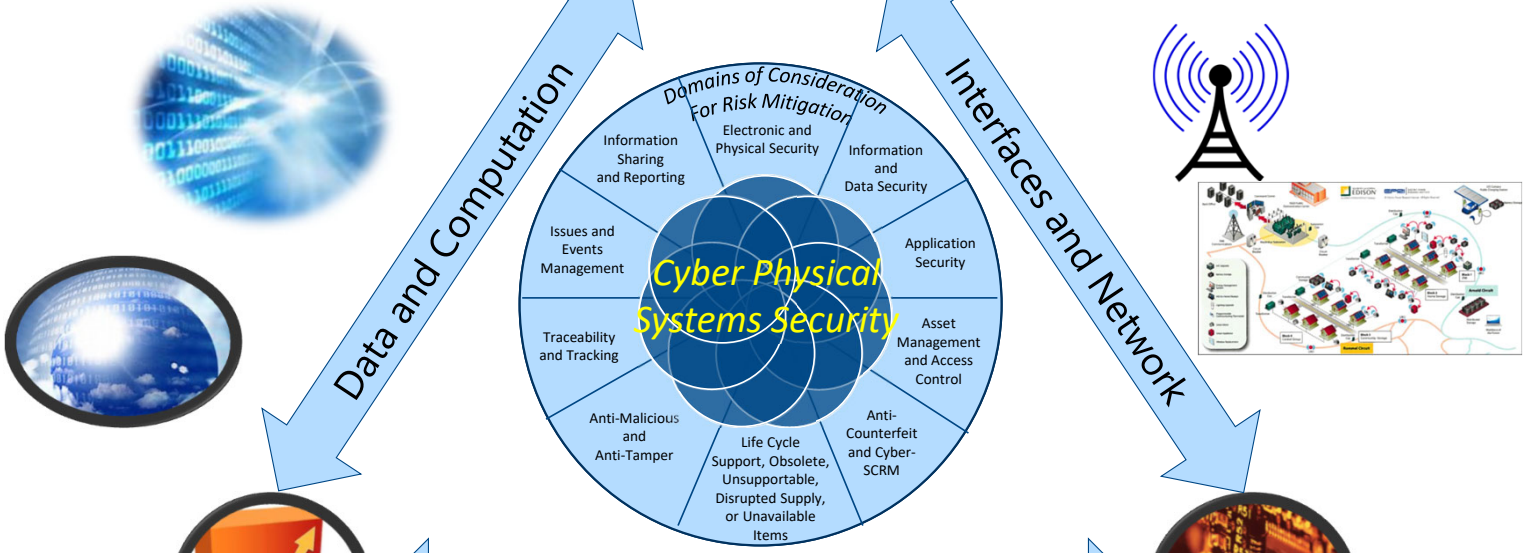


Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Risk Mitigation

Threat, Consequence, Vulnerability

Prioritized Actions based on Risk Mitigation



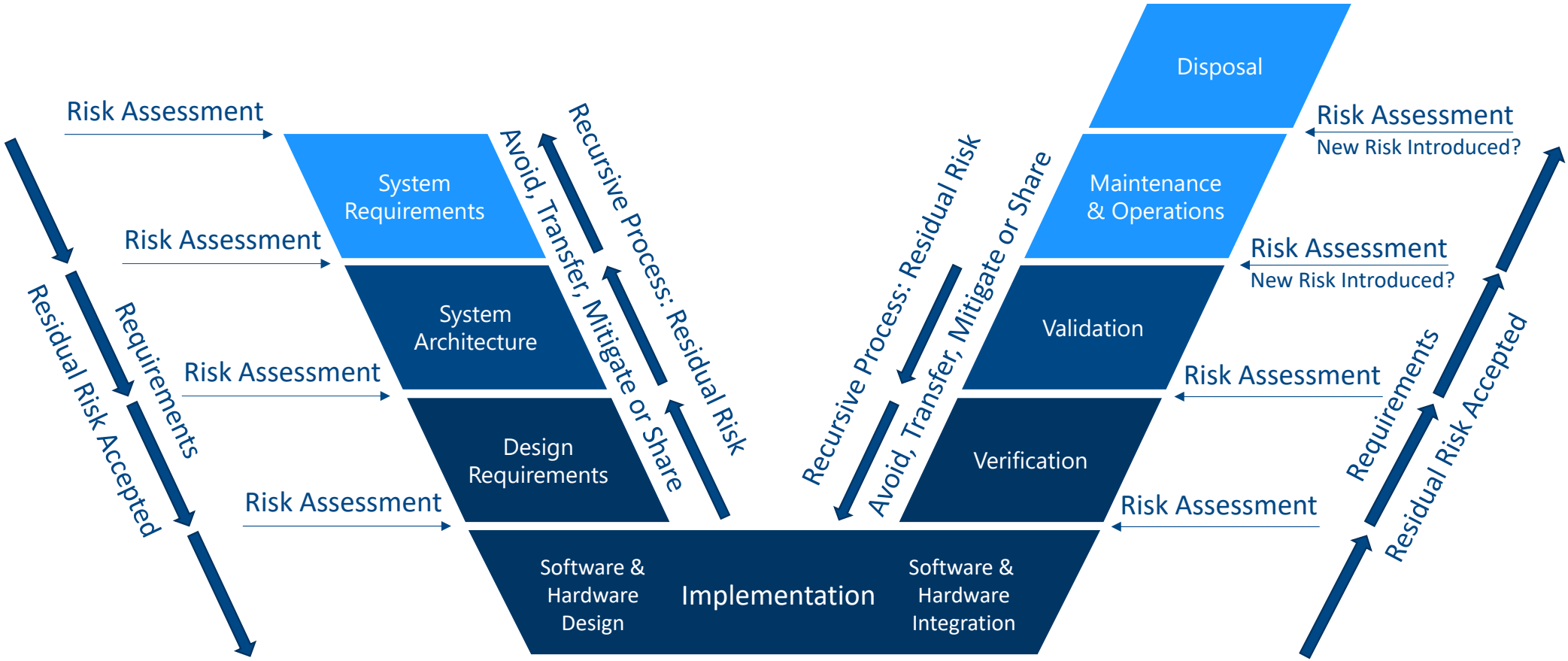
Software

Electronics Hardware and Firmware

Critical for the Protection of CPS through Modernization and Migration - essential to defending the homeland, building security globally, deterring aggression, and remaining prepared against any adversary

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 V-Overlay



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

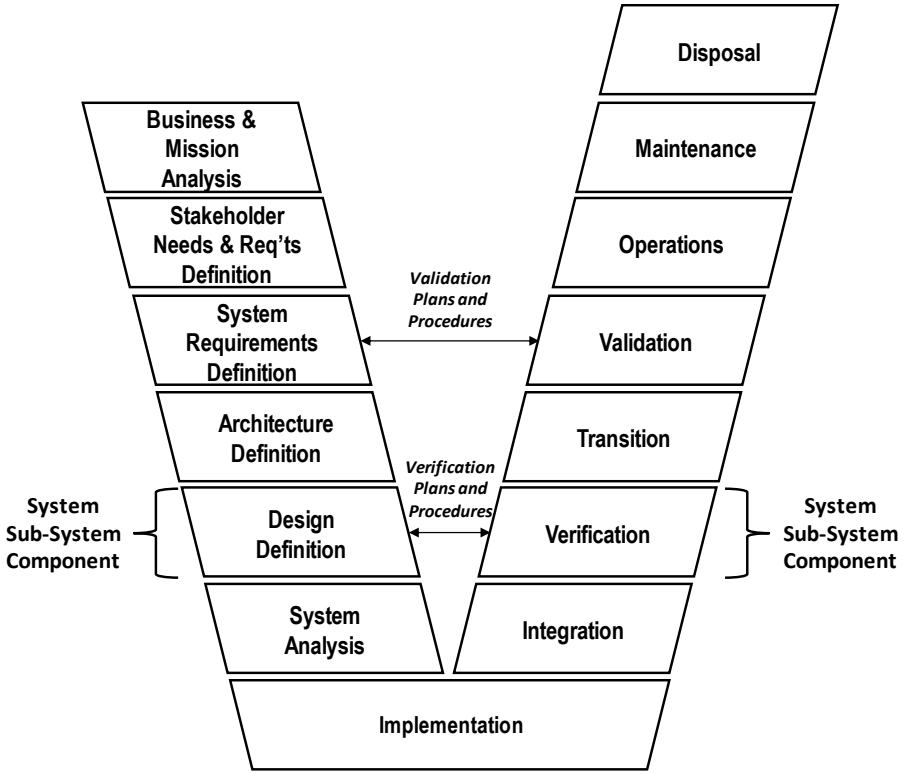
“V” Overlay Sub-committee Accomplishments and Plans

- Developed first draft of a standard that—
  - Establishes requirements—
    - To apply a CPSS “V” overlay to the 14 systems engineering technical processes
      - Overlay contains the security engineering activities and tasks where additional CPSS content may be warranted
    - To develop requirements to manage CPSS risks within the SE processes
    - To assess CPSS risks after a triggering event and take appropriate action
    - For a CPSS Engineering Plan (CPSSEP)
    - For reporting
- Working on defining key terms

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Requirement to Apply a CPSS V Overlay

- As a baseline, an organization shall follow the systems and software engineering technical processes established by ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*, and the security engineering extensions established by NIST Special Publication 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* or equivalents
- The organization shall perform and document the CPSS activities and tasks associated with the fourteen systems and software engineering technical processes



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Requirement to Develop Requirements to Manage CPSS Risk

- The organization, as part of its system and software engineering process to manage CPSS risks to an acceptable level, shall establish, (1) software assurance and hardware assurance requirements and (2) functional and non-functional requirements for all other domains of consideration
  - Domains of consideration reflect the areas to consider, when determining whether and how to control CPSS risks related to prioritized weaknesses and vulnerabilities that could impact the CPS

    - **Electronic security**
    - **Physical security**
    - **Information security**
    - **Data security**
    - **Asset management**
    - **Access control**
    - **Life cycle support**
    - **Obsolete, unsupportable, disrupted supply, or unavailable items**
    - **Anti counterfeit**
    - **Cyber-supply chain risk management**
    - **Application security**
    - **Issues and Events Management**
    - **Traceability and tracking**
    - **Anti malicious**
    - **Anti tamper**
    - **Information sharing and reporting**

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Requirement to Assess and Take Appropriate Action after a Triggering Event

- A “triggering event” is an occurrence (at any point in the life cycle) which indicates a potential need for changes to the CPSS controls that are in place; categories include
  - Changes in the existing design or interfaces
  - Changes in the risk profile of a system
  - Planned security assessments
- The organization shall conduct a CPSS risk assessment in accordance with its CPSSEP when a triggering event occurs at any point in the life cycle of the product to determine the need to
  - Revise the CPSSEP
  - Revise the CPSS functional, non-functional, and assurance requirements associated with the domains of consideration
  - Re-initiate the systems and software security engineering process to mitigate, transfer, or share unacceptable levels of risk identified in the assessment
  - Report

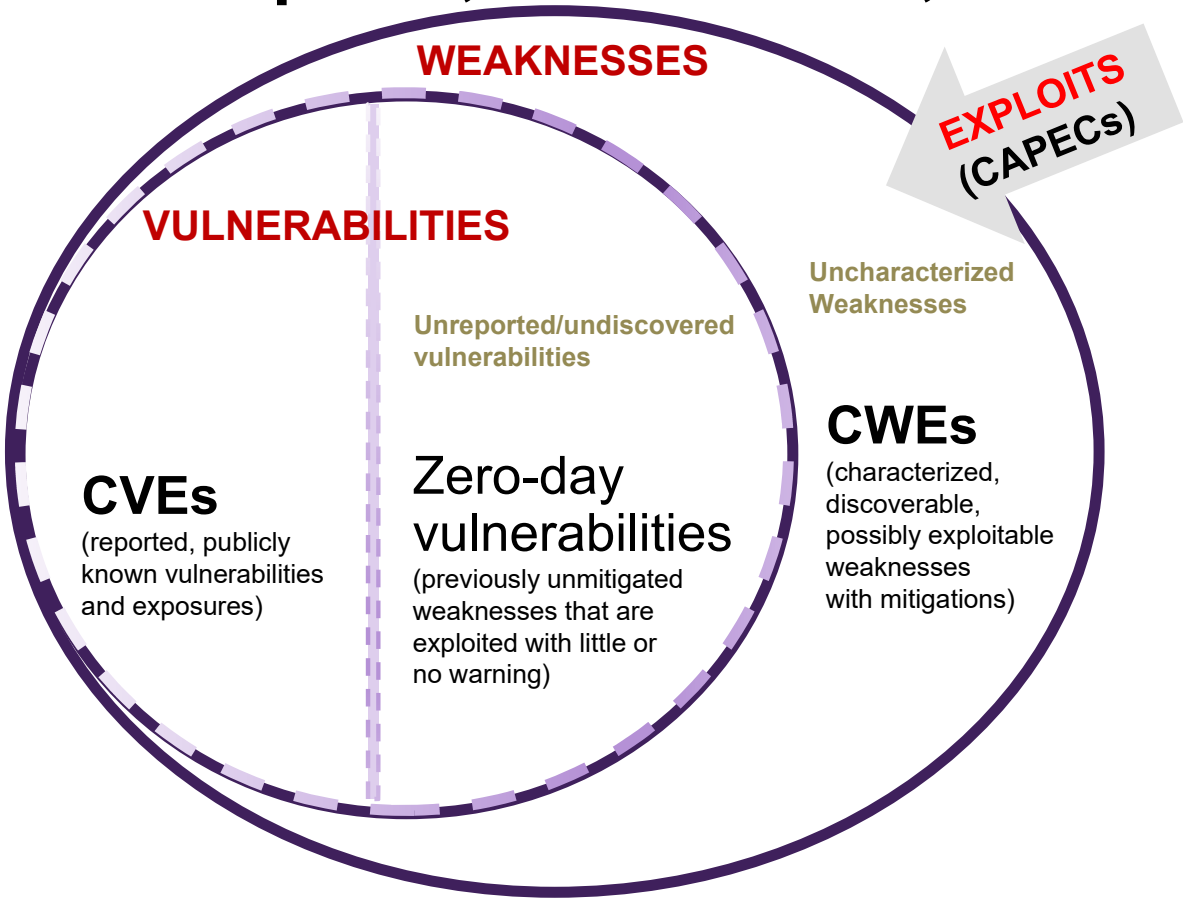
Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Requirements for CPSSEP and Reporting

- The organization shall develop and implement a risk based CPSSEP that establishes requirements for cyber physical systems in accordance with the requirements specified herein
- The organization shall report in accordance with its enterprise reporting policy when there has been an exploitation (or credible threat of the exploitation) of a weakness resulting in a vulnerability that could impact the business or mission needs

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

The G-32 HwA & SwA Subgroups are Addressing Component Level Exploits, Weaknesses, and Vulnerabilities



The existence of an exploit designed to take advantage of a weakness (or multiple weaknesses) and achieve a negative technical impact is what makes a weakness a vulnerability.

What is Hardware Assurance (HwA)?

The processes, practices or methodologies employed to achieve a level of confidence that microelectronics function as intended and are free of exploitable weaknesses and known vulnerabilities, either intentionally or unintentionally designed or inserted, throughout the life cycle.

Note. Microelectronics (also known as microcircuits, semiconductors, and integrated circuits) include the material physical components, programmable logic devices (PLD), and interfaces with embedded software and/or intellectual property.

Hardware may be extremely difficult and costly to "fix"

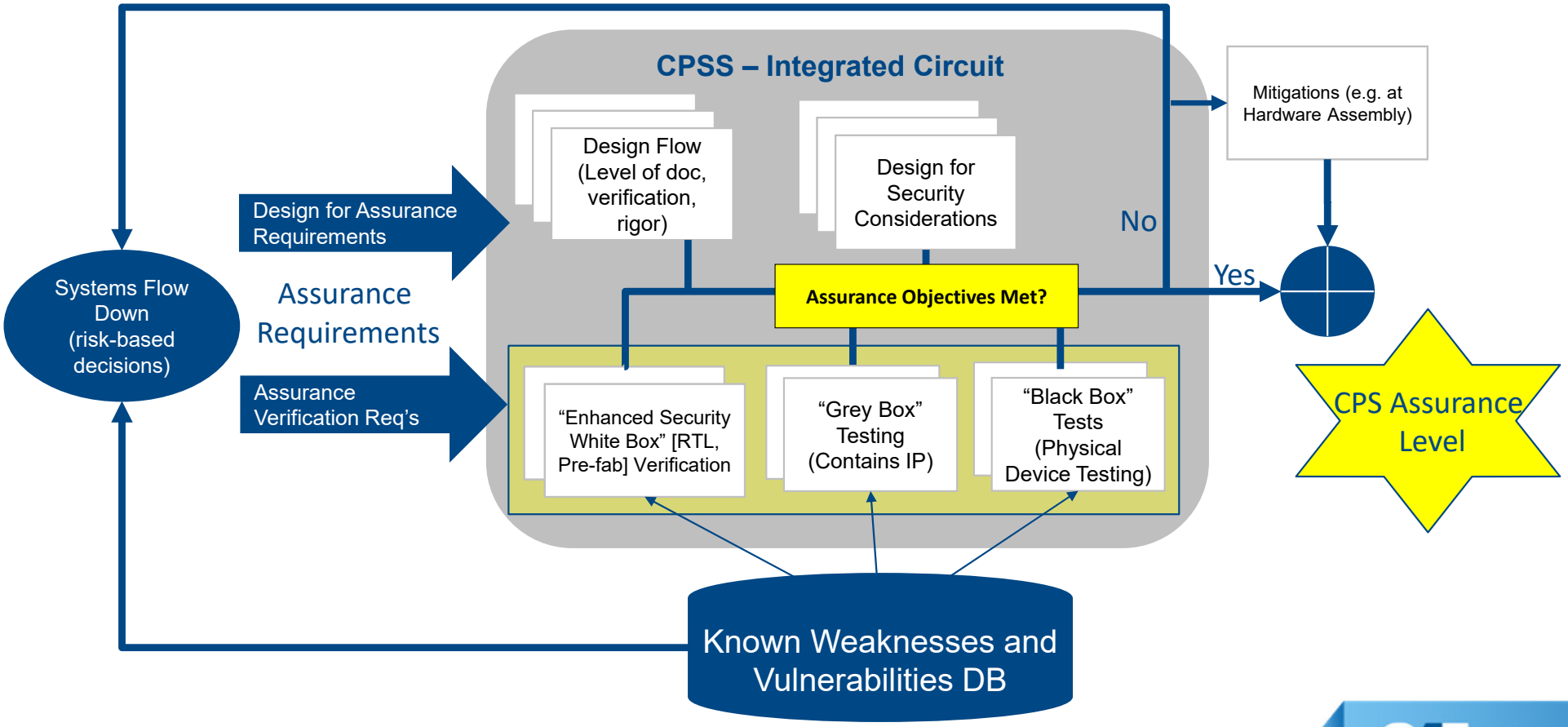
Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 HwA Subgroup Task and Objectives

- Develop Hardware Assurance guidance, specifically for Integrated Circuits, in coordination with the CPSS Standard
- Define CPSS Hardware Assurance Reference Framework
  - Define a CPSS Hardware Process
  - Document CPSS Hardware Best Practices
  - Identify CPSS Hardware Tools
  - Establish Common CPSS Hardware Vulnerability Scoring System (leveraging existing standards – G19A CDC/CTC)
- Facilitate continuous monitoring and sharing of known CPSS weaknesses and vulnerabilities
  - Utilize other Hardware Vulnerability Database efforts – (CWE, TAME)
- Provide a consistent results across industry, government, and defense
- Provide a platform for introducing HwA expertise to industries
- Standardize test methods addressing HwA for microelectronics

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Scope - The CPSS Hardware Assurance "Box"



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 JA6801 HwA Subgroup High-Level Outline

- Assurance Requirements to ***Mitigate Weaknesses and Vulnerabilities*** (input from SE-V Main Specification JA7496)
  - Assurance Case: a reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).
- Levels of Assurance
  - Definition of levels and tenets that aid in parts selection and design.
- Design Flow (Level of Documentation, Verification, Rigor)
  - Capture level of rigor that is documented throughout the design flow process (did you follow other standard guidelines of an IC? Did you follow UVM? Did you use multiple verification tools?)
  - We want to capture the level of confidence of the pedigree of design (what was the qualification/experience of org. test/verifying?)
- Design for Security
  - Guidance for the use of particular design and security elements (e.g. logic locking, obfuscation/anti-tamper, finger printing, functional testing, secure JTAG port/securing self-test)
- White Box, Grey Box, Block Box Verification
  - Tools, techniques, and best practices during requirements, design, implementation, and iterative verification phases

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

What is Software Assurance (SwA)?

The processes, practices or methodologies employed to achieve a level of confidence that the software functions in the intended manner and is free from exploitable weaknesses and vulnerabilities, either intentionally designed or accidentally inserted at any time during its lifecycle.

Note. Software includes embedded code and programmable logic.

Efforts are required to define "level of confidence" and "free of known vulnerabilities"

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Committee Software Assurance

"focuses on developing a framework that provides a consistent result across industries, government, and defense; as well as a platform for introducing SwA expertise to industries"

- Software Assurance Security Process for developing and maintaining secured and trusted cyber physical software
- Standardize approach for mitigating weaknesses in cyber physical software
- Standardize approach for mitigating vulnerabilities in cyber physical software
- Up-to-date repositories of best practices for developing software for cyber physical systems
- Up-to-date database of tools, tips, techniques, and procedures for developing secured and trusted cyber physical software

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Committee Software Assurance Framework

Identification and mitigation of weaknesses, vulnerabilities, and threats

Process perspectives
- Repeatable tasks that can be defined as a process to be applied to software and have repeatable, understood output
- Develop the methods and reporting that will define what Software Assurance can incorporate

Development perspectives
- Find and address weaknesses, vulnerabilities, and threats early in the process
- Tools, techniques, practices that can be applied to development rigor addressing assurance issues

Identify exploitability
- Software Assurance can quantify the exploitability of a weakness, vulnerability or threat

White box: Tools, tips, techniques, and best practices during requirements, design, implementation, and iterative verification phases (left-hand side of the V-model)

Grey box: Tools, tips, techniques, and best practices during requirements, design, intgration of third party software, and iterative verification phases (left-hand side of the V-model)

Black box: Tools, tips, techniques, and best practices during test, integration, and iterative verification phases (right-hand side of the V-model)

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Risk Management Framework

Goal:

- **Provide a risk management framework for the G-32 that applies to CPSS, industry agnostic and applicable to various maturity levels.**

Objectives:

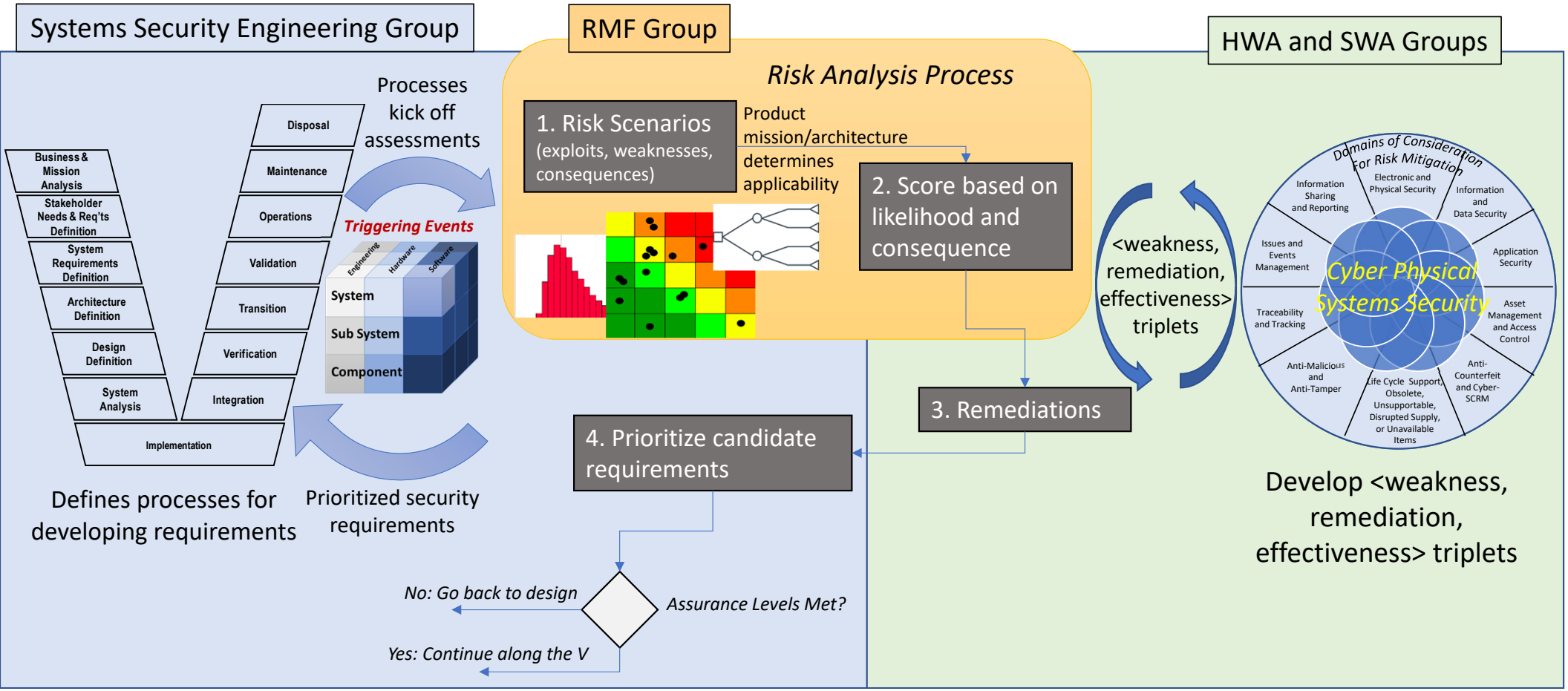
- Provide framework as a holistic context for the application of CPSS.
- Increase effectiveness of communicating CPSS strategy and implementation.
- Provide a top down approach, accessible to leadership down to specific practitioners assessing implementing controls. *Not specific to any legal requirements or frameworks.*
- Increase communication and decrease the friction of multiple interpretations of definitions and industry specific language and guidelines.
- Be able to include current and emerging risk related to CPSS.
- Provide an actionable approach to differentiate key risk initiatives for the organization.

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

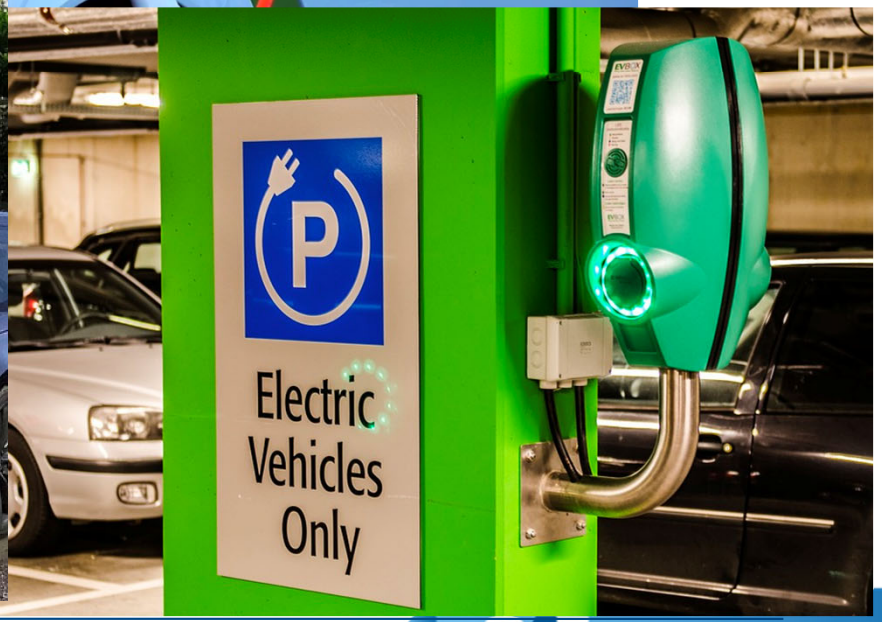
G-32 Risk Management Framework

Assurance Case Perspective

Overall goal: build/operate to requirements that provide adequate confidence that weaknesses have been mitigated within affordability constraints



Illustrative Example Electric Vehicle Charging Station and Services

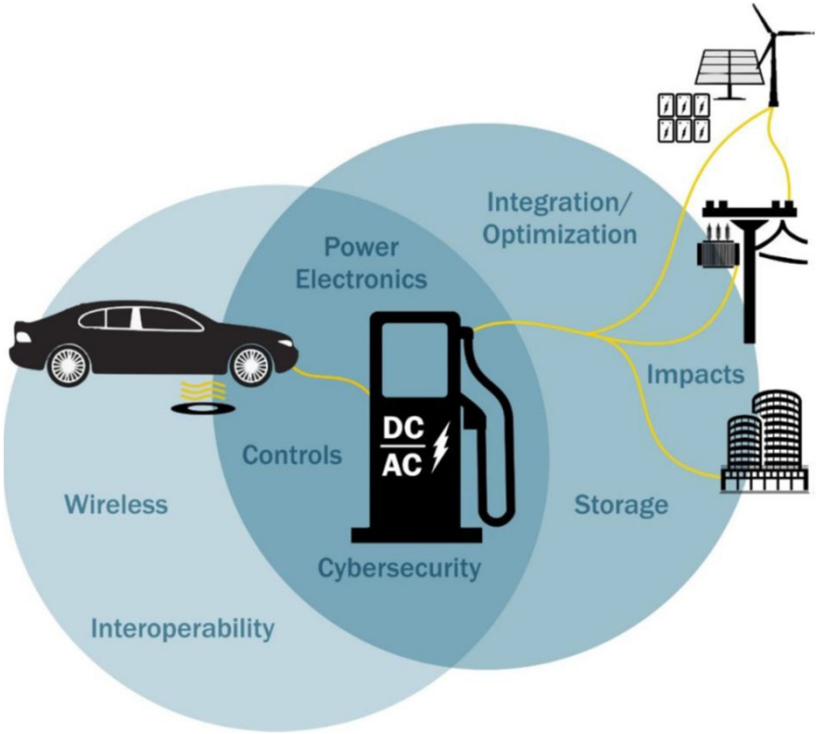


Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE
36

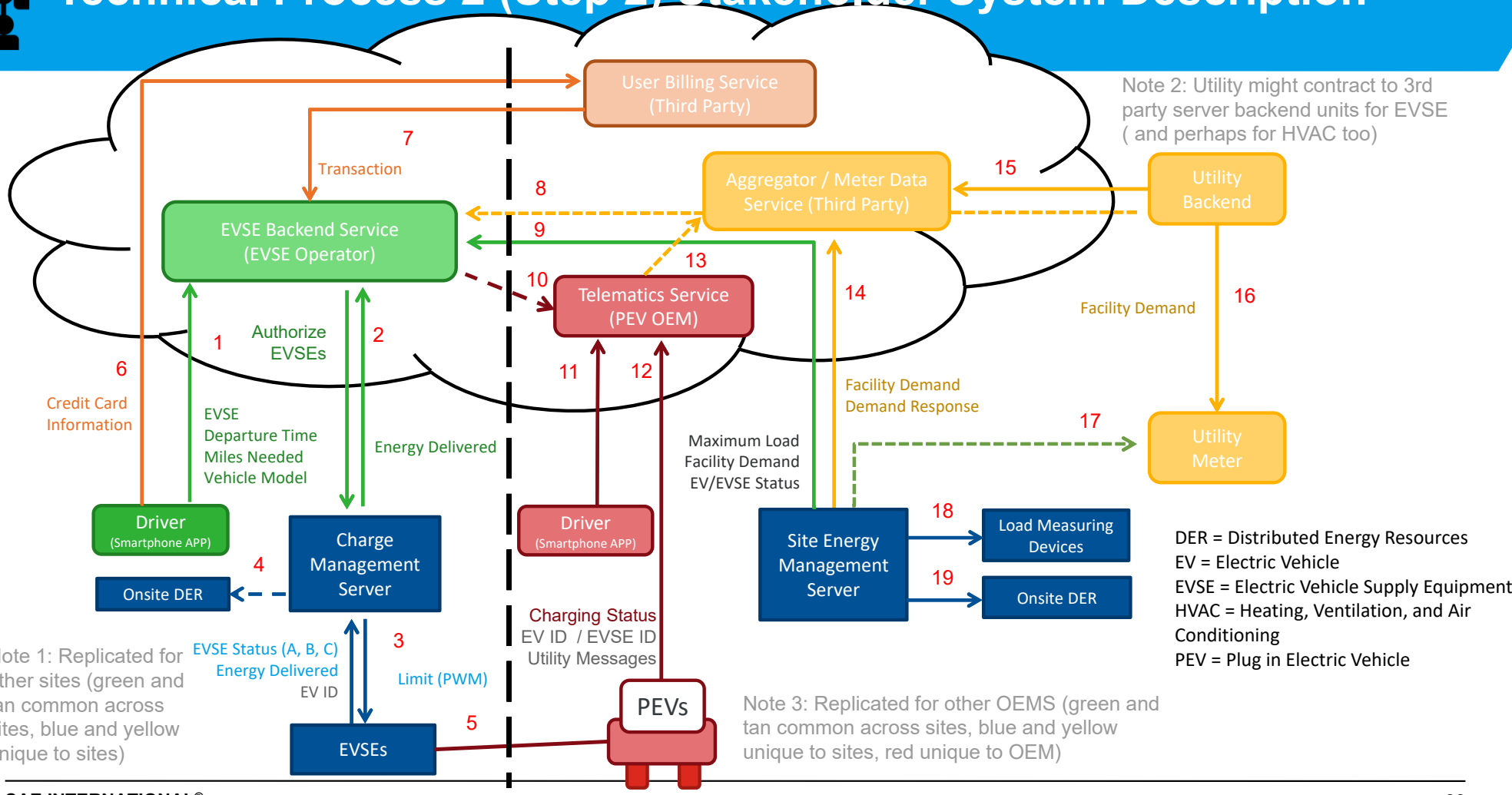
G-32 Illustrative Example Subgroup

Demonstrate implementation of the JA7496 Cyber Physical Systems Security Engineering Plan utilizing an Electronic Vehicle Charging Station as an example



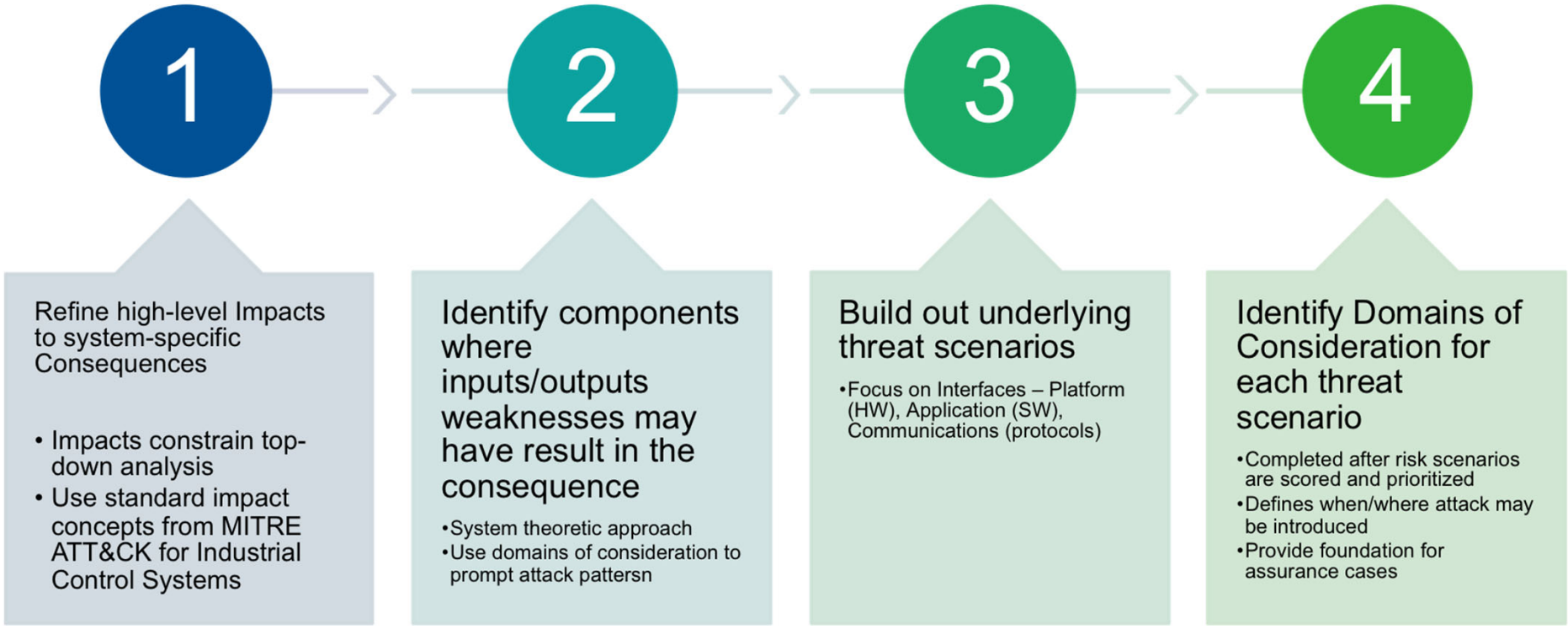
Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Technical Process 2 (Step 2) Stakeholder System Description



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE

Risk-Based Approach - Activities 3-5 for Technical Process 1 & 2



Copyright © SAE International. Further use or distribution is not permitted without permission from SAE

G-32 Phase I Project Milestones *(as planned)*

Milestone Date	Project Activities
July 2020	• ***JA7496: CPSSEP***—initial draft complete for all sections, except Definitions and Risk Management Framework "how" language • ***JA6801: CPSS HwA* AND *JA6678: CPSS SwA***—initial draft outlines complete
August 2020	• ***JA7496***—initial draft of Definitions section complete
December 2020	• ***JA7496***—initial draft review complete, including Risk Management Framework "how" language, and submitted for ballot • ***JA6801: CPSS HwA* AND *JA6678: CPSS SwA***—initial drafts complete
2Q 2021	• ***JA7496***—comment resolution complete • ***JA6801: CPSS HwA* AND *JA6678: CPSS SwA***—initial draft reviews complete and submitted for ballot
3Q 2021	• ***JA7496***—final publication, including Risk Management Framework and Illustrative example appendices
4Q 2021	• ***JA6801: CPSS HwA* AND *JA6678: SwA***—initial drafts' comment resolution complete
1Q 2022	• ***JA6801: CPSS HwA* AND *JA6678: SwA***—final publication

Enabling Cyber Security, Assurance, & Resiliency

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Future Work and Research Needs for Reference

- Research is needed to design and build real-world models and ranges supporting experimentation and validation for embedded malware, hardware Trojans, and cyber physical systems security.
- Operational CPSS modeling tools are needed to enable cost-effective, risk-based cyber resiliency requirements.
- Research is needed for detection tools for microelectronics weaknesses and vulnerabilities, whether intentional or unintentional.
- Research for User assessment toolsets are needed to sustainable trust and agility in a resilient, trusted supply chain.
- Support to emerging system-on-chip architectures is needed for designed-in cyber resiliency and security.
- Support to emerging track and trace authentication taggants.
- Adoption of IT industry's use of penetration testing and code reviews in cyber physical systems.
- Domain separation for in-system networks and safety critical systems.
- Implement a layered approach to security.
- Develop secure over-the-air update capabilities.
- Hire dedicated staff and high-level managerial positions focused on cyber physical systems security.
- Collaborate with researchers and independent security firms to test system digital security, identify cyber physical systems security vulnerabilities and offer solutions to resolve them.
- Develop CPSS Knowledge Base within newly formed Consortiums and with CPSS College Curriculum.
- **Call for action for standard work to codify cyber physical systems security from a systems engineering perspective.**

Enabling Cyber Security, Assurance, & Resiliency

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Participation Information

Daniel DiMase – CPSS Main Committee
Aerocyonics, Inc.
Desk: +1 (401) 398-2343
daniel.dimase@aerocyonics.com

John Hallman – HwA Subgroup
OneSpin Solutions
Desk: +1 (321) 536-8250
john.hallman@onespin.com

Dr. Jay Mandelbaum -
Systems Security Engineering V Overlay Subgroup
Institute for Defense Analyses (IDA)
Desk: +1 (703) 845-2123
jmandelb@ida.org

Gloria D'Anna –
Systems Security Engineering V Overlay Subgroup
Ford Motor Company
Desk: +1 (313) 390-2651
gdanna3@ford.com

Dr. Brian Cohen – HwA Subgroup/Technical Advisor
CyberTech Solutions
Desk: +1 (703) 624-4888
brianscohen@cybertechsol.net

Dr. Kenneth Crowther – Illustrative Example Subgroup
GE Global Research
Mobile: +1 (804) 201-1039
Kenneth.Crowther@ge.com

William Scofield – CPSS Main Committee
Boeing
Desk: +1 (206) 662-3913
william.h.scofield@boeing.com

Howard Miller – Risk Management Framework Subgroup
LBW Insurance & Financial Services, Inc.
Desk: +1 (661) 702-6039
HowardM@lbwinsurance.com

Dr. Andreas Schweiger– SwA Subgroup
Airbus Defence and Space GmbH
Desk: +49 (84-59) 816-7087
andreas.schweiger@airbus.com

Chris Sundberg – SwA Subgroup
Woodward, Inc.
Desk: +1 (970) 498-3383
christopher.sundberg@woodward.com

Dr. Zachary Collier - Risk Management Framework Subgroup
Collier Research Systems
Desk: +1 (904) 312-0451
Zachary@CollierResearchSystems.com

Dorothy Lloyd – Standards Specialist
SAE International
Desk: +1 (724) 772-8663
dlloyd@sae.org

Judith Ritchie – Director, Government and Industry Affairs
SAE International
Desk: +1 (202) 975-1508
Judith.ritchie@sae.org

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

BACKUP

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

G-32 Main Committee

Co-chairs: Bill Scofield & Daniel DiMase

Project Milestones

- Initial Draft: Projected completion July 4th, 2020
- Initial Draft Review: Projected completion December 7th, 2020
- Submit for Ballot: December 7th, 2020
- Comment Resolution: Projected completion Q2 2021
- Final Publication: Projected completion Q3 2021

Next Steps

- Continue the review Domains of Consideration
- Review 14 Technical Areas from V Overlay subgroup
- Review remaining input from RMF Subgroup and Illustrative Example Subgroup

Tasks Completed

- Outline Development – January 2020
- Agreement to publish JA Surface Vehicle/Aerospace Document, multi-sector specification – February 2020
- JA7496 “Cyber Physical Systems Security Engineering Plan (CPSSEP)” WIP initiated in SAE System - February 13, 2020

Issues/Help Needed

- Input needed for high-level risk requirements integrated into the 14 technical areas of the SE-V overlay process from the RMF subgroup to meet project milestones
- Need to make a determination if Phase I release will include additional RMF detail describing an example of how risk is done without delaying project milestones
- Input needed from Illustrative Example Subgroup to meet project milestones

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

V Overlay Sub-Group

Co-leads: Jay Mandelbaum & Gloria D'Anna

Project Milestones

- Definitions projected 2020-08-01

Next Steps

- Begin definitions work for V overlay terms
- Develop list of terms for V Overlay definitions and review existing definitions for those terms
- Continue first draft of technical processes

Tasks Completed

- 2020-02-21 first sections of first draft of technical processes section sent to Main Committee for review
- 2020-03-15 first draft of domains of consideration section
- 2020-04-24 first draft of reporting section
- 2020-05-01 first draft of triggering events section
- 2020-05-30 first draft of all technical processes

Issues/Help Needed

- None

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

RMF Sub-Group

Co-leads: Howard Miller & Zach Collier

Project Milestones

- July 2020 – The goal is to have the “what” language of the standard complete
- December 2020 – The goal is to have the “how” language of the standard complete
- Ballot in concert with JA7496 as appendix: December 7th, 2020
- Comment resolution: Q2 2021
- Publish as JA7496 appendix: Q3 2021

Next Steps

- Continue to work through the 14 technical processes
- Need to coordinate with Systems Engineering V Overlay Group on risk-related definitions

Tasks Completed

- Coordinated with the Systems Engineering V Overlay Group to define the overall structure of the standard
- Currently working through drafting risk-based text the 14 technical processes

Issues/Help Needed

- Need to determine how existing practices on vulnerabilities and weaknesses will be incorporated
- Need to think more, with the help of the other Groups, on how the determination of assurance levels will work
- Inputs from key industry/government sectors to assure that adoption of the resulting work will conform with already established standards/viewpoints

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

Illustrative Example Sub-Group

Co-lead: Kenneth Crowther

Project Milestones

- Complete draft (maintain pace with JA7496 development): about July 24, 2020
- Ballot in concert with JA7496 as appendix: December 7th, 2020
- Comment resolution: Q2 2021
- Publish as JA7496 appendix: Q3 2021

Next Steps

- Create elicitation framework for implementing technical processes 1 and 2 approaches for JA7496 draft
- Develop approach for technical processes 3-7 ("left side of V") for illustrative implementation of Phases
- Draft initial report for committee initial technical processes

Tasks Completed

- Created high-level architecture and business/mission design for electric vehicle charging station for the example
- Developed approach for technical processes 1-2 for illustrative implementation of JA7496 CPS security activities
- Regrouped with committee for direction of standard with suggestions from main committee

Issues/Help Needed

- Rely on V-overlay, RMF, and other groups to establish the main framework – will always lag their drafts and implementation
- Need to reach broadly for electric vehicle charging stations specifics across SAE to be consistent with other standards/outcomes
- Complex, multi-level problem with inconsistent judgments on focus for illustrative example. Need to maintain focus with just enough complexity to retain relevance.

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

HwA Sub-Group

Co-lead: John Hallman

Project Milestones

- Initial Draft: Outline completion July 4th, 2020
- Initial Draft completion December 7th, 2020
- Initial Draft Review: Projected completion Q2 2021
- Submit for Ballot: Q2 2021
- Comment Resolution: Projected completion Q4 2021
- Final Publication: Projected completion Q1 2022

Next Steps

- Organize details of working session into the outlined document structure
- Break off into small SME groups to write detailed sections on White Box Methods for HwA Verification, Black Box Methods, and HwA Requirements from Known Hardware Weaknesses
- Complete Design Flow and Design for Security Sections of document, including references to other documents and standards

Tasks Completed

- JA6801 “Cyber Physical Systems Security Hardware Assurance” WIP initiated in SAE System – April 8, 2020
- Established a core group of bi-weekly SME participants from multiple industry sectors
- Completed 4 weekly 2-hour working sessions to capture main section details
- First round of outline complete – May 2020

Issues/Help Needed

- Need additional lead or co-lead(s)
- Need SMEs willing to dedicate time to write specific sections of the outlined document
- Input needed from Systems Level to define/document process to flow proper HwA assurance requirements to IC
- Input needed from SMEs to identify methods and metrics available today versus research and emerging
- Input needed from Illustrative Example Subgroup to include specific example down to the hardware component (IC) level

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.

SwA Sub-Group

Co-leads: Andreas Schweiger & Chris Sundberg

Project Milestones

- Initial Draft: Outline completion July 4th, 2020
- Initial Draft completion December 7th, 2020
- Initial Draft Review: Projected completion Q2 2021
- Submit for Ballot: Q2 2021
- Comment Resolution: Projected completion Q4 2021
- Final Publication: Projected completion Q1 2022

Next Steps

- Revision of outline
- Definition of relevant terms
- Definition of outline completion July 4th draft

Tasks Completed

- JA6678 “Cyber Physical Systems Security Software Assurance” WIP initiated in SAE System – November 8, 2019

Issues/Help Needed

- Input needed for target assurance requirements from V Overlay Subgroup
- Input needed from Illustrative Example Subgroup
- Need SMEs willing to dedicate time to write specific sections of the outlined document

Copyright © SAE International. Further use or distribution is not permitted without permission from SAE International.