

Hardware CWE™ Special Interest Group (SIG)

Gananand Kini, Bob Heinemann, Luke Malinowski,
Gage Hackford, Chris Lathrop, Steve Christey Coley,
Alec Summers

MITRE

May 12, 2023



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Agenda

REMINDER: This meeting is being recorded.

- **Housekeeping and Announcements**
- **Working Items for this meeting:**

1	4.11 Release Announcement	Steve C	5 min
2	D3FEND and CWE Mention	Mike S	5 min
3	CWE Key Concepts – Selection from HOST Presentation	Bob H	20 min
4	SAE G-32 Call for Participation in HwA Standard	Joel H	15 min
5	Side Channels vs Covert Channels (if time allows)	Bob H	15 min



Housekeeping

- **Schedule:**

- **Next Meeting:**

- **Scheduled for June 9**

- **12:30 – 1:30 PM EST (16:30 – 17:30 UTC)**

- **Microsoft Teams**

- **Contact: cwe@mitre.org**

- **Mailing List: hw-cwe-special-interest-group-sig-list@mitre.org**

- **Minutes from previous meetings available on our GitHub site:**

- <https://github.com/CWE-CAPEC/hw-cwe-sig>



Announcements

- **Reminder: April SIG was cancelled. Welcome back.**
- **CWE 4.11 Released April 27**
- **CWE/CAPEC Board Meeting Occurred on Feb 15**
- **D3FEND / CWE Integration Presentation Next Month**



4.11 Release Notes

Steve C (MITRE CWE)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Significant changes for CWE 4.11

- **New "Custom" presentation filter (details in a later slide)**
 - Users can customize which details they see in individual CWE entries
- **New Comprehensive Categorization for Software Assurance Trends View**
 - 23 new categories related to the new view
 - "Memory safety" is a highlight
- **Updates to the "Software Development View" (CWE-699) and "Weaknesses Introduced During Design" View (CWE-701)**
- **ICS/OT specific details added to many CWEs, from ICS/OT SIG**
 - Highlight: mappings to secure-design-oriented 62443
- **Modernized memory-safety related mitigations based on D3FEND**
- **Mapping Notes added to over 300 Categories**
 - Roughly: "Do not map to this CWE entry, because it's a Category, not a Weakness"
- **Automated code analysis detection methods added to many CWEs**
- **Updated hundreds of reference URLs**



Improvements to View CWE-701: Weaknesses Introduced During Design

- **CISA's recent emphasis on "Secure By Design / Secure By Default" aligns with CWE's progression in recent versions**
 - Consider CWE 4.9's "new" entries about default credentials
- **In CWE 4.10 and earlier, View CWE-701 was built from an XPath query**
 - Roughly: "Weakness entries whose Mode of Introduction was in the Architecture/Design Phase"
- **For CWE 4.11, we made the following changes:**
 - Modify the query, but avoid Variants and Pillars
 - Update content that inappropriately included Design as a phase in Mode of Introduction
- **Issues**
 - (Steve C opinion: "it's design/implementation turtles all the way down")
 - What is "design" to software might be "implementation" in hardware
 - Agile and other methodologies do not necessarily distinguish between "design" and "implementation"
 - Sometimes the same CWE can be both (e.g., authN in a web app by trusting a cookie value, versus a communications protocol that's spoofable)



Custom Filtering

Edit Custom Filter

Conceptual	Operational	Mapping Friendly	Select All
<input checked="" type="checkbox"/> Related Weaknesses		<input checked="" type="checkbox"/> Potential Mitigations	
<input checked="" type="checkbox"/> Weakness Ordinalities		<input checked="" type="checkbox"/> Demonstrative Examples	
<input checked="" type="checkbox"/> Applicable Platforms		<input checked="" type="checkbox"/> Observed Examples	
<input checked="" type="checkbox"/> Background Details		<input checked="" type="checkbox"/> Functional Areas	
<input checked="" type="checkbox"/> Alternate Terms		<input checked="" type="checkbox"/> Affected Resources	
<input checked="" type="checkbox"/> Relationships		<input checked="" type="checkbox"/> Memberships	
<input checked="" type="checkbox"/> Modes Of Introduction		<input checked="" type="checkbox"/> Taxonomy Mappings	
<input checked="" type="checkbox"/> Exploitation Factors		<input checked="" type="checkbox"/> Related Attack Patterns	
<input checked="" type="checkbox"/> Likelihood Of Exploit		<input checked="" type="checkbox"/> References	
<input checked="" type="checkbox"/> Common Consequences		<input checked="" type="checkbox"/> Notes	
<input checked="" type="checkbox"/> Detection Methods		<input checked="" type="checkbox"/> Content History	
Reset	Clear	Submit	Cancel



D3FEND / CWE Integration

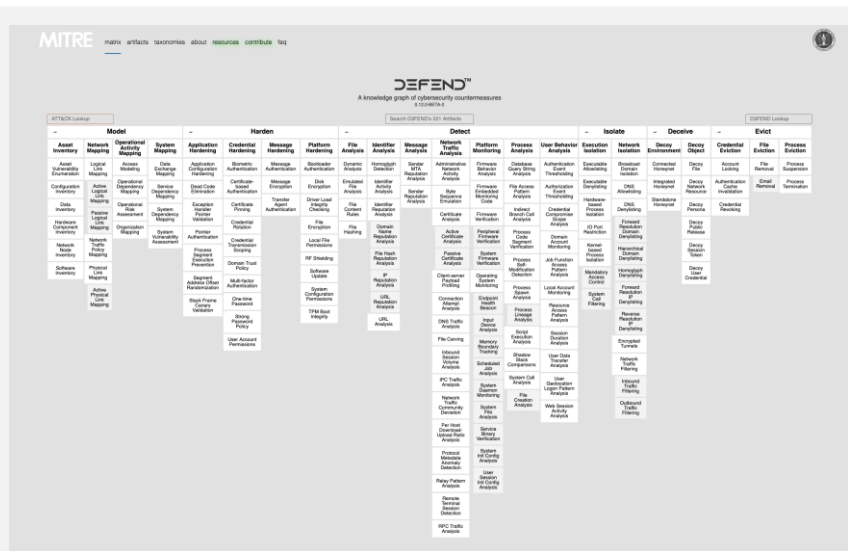
Mike Smith (MITRE)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

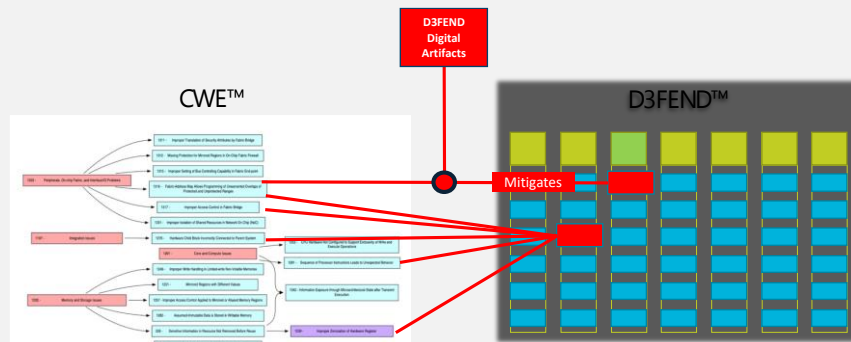
D3FEND Knowledge Graph Teaser

Structured knowledge for cyber countermeasures



- Articulates defensive tactics & techniques
- Cites 100s of intellectual property documents
- Expressed in industry standard formats
- Vendor-agnostic semantic representations

- Relationships to CWE (T25) & ATT&CK® techniques are **inferred** through an intermediate model of digital artifacts (components)
- The graph is queried to create new insights and connections between cyber offense and defense
- Community on GitHub & Slack, d3fend.mitre.org
- Planning to add significant hardware additions to D3FEND ontology



CWE Key Concepts: Selection from HOST Presentation Bob H (MITRE CWE)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

What is a weakness?

Weakness

- **A condition** in a software, firmware, hardware, or service component that, under certain circumstances, **could contribute** to the introduction of **vulnerabilities**.
- Applies to the dimensions of behavior, property, resource, technology, or language.

Vulnerability

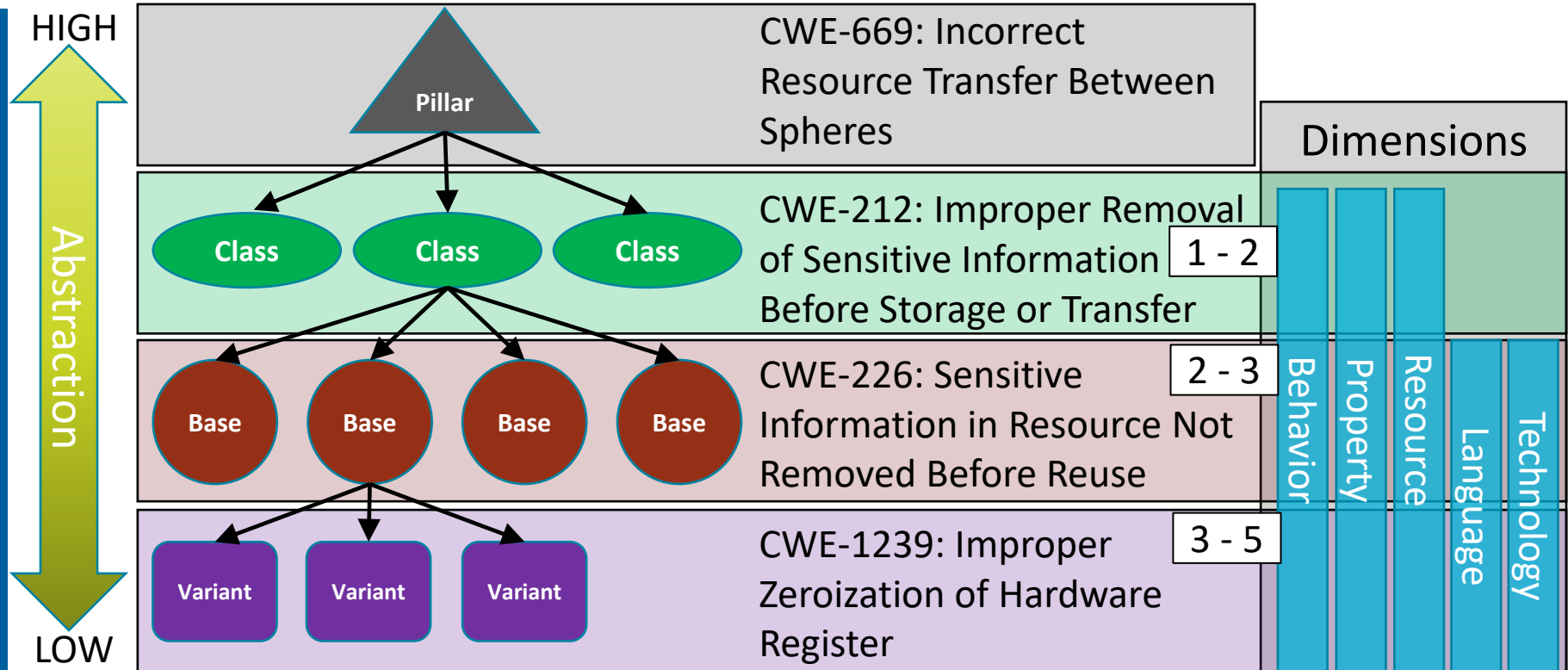
- **A flaw** in a software, firmware, hardware, or service component **resulting from a weakness** that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components.

A Weakness is a Root Cause for a Vulnerability

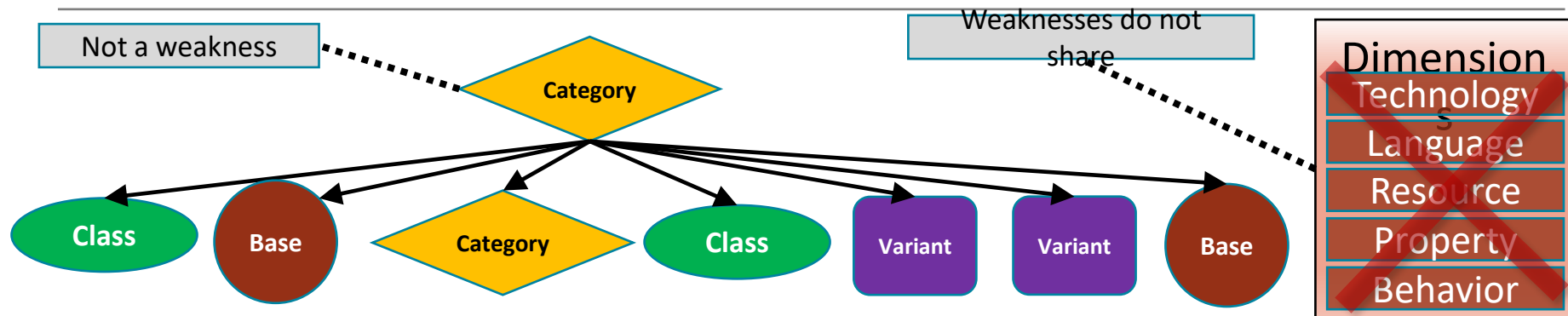


CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE Weakness Abstraction Levels



CWE Categories (Arbitrary Collections of Convenience)



- **C** Physical Access Issues and Concerns - (1388)
 - **C** Improper Handling of Physical or Environmental Conditions - (1384)
 - **B** Improper Protection against Electromagnetic Fault Injection (EM-FI) - (1319)
 - **B** Improper Protection Against Voltage and Clock Glitches - (1247)
 - **B** Improper Handling of Single Event Upsets - (1261)
 - **B** Improper Handling of Faults that Lead to Instruction Skips - (1332)
 - **B** Improper Handling of Hardware Behavior in Exceptionally Cold Environments - (1351)
 - **B** Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques - (1278)
 - **V** Comparison Logic is Vulnerable to Power Side-Channel Attacks - (1255)
 - **B** Improper Protection of Physical Side Channels - (1300)
 - **B** Semiconductor Defects in Hardware Logic with Security-Sensitive Implications - (1248)

CWE Views

- **CWE List -> Latest Version**
- **A subset of CWE entries that provides a way of examining CWE content.**
- **Views can either be hierarchical or flat**

Common Views	External Mappings	Helpful Views
<ul style="list-style-type: none">• By Software Development• By Hardware Design• By Research Concepts	<ul style="list-style-type: none">• CWE Top 25• Most Important HW Weaknesses• Software Fault Clusters• OWASP Top 10 (2021)• Etc.	<ul style="list-style-type: none">• Introduced During Design• Introduced During Implementation• Software Written in C• Etc.



Call for Participants: SAE G-32 CPS HwA Standard Joel Heebink (Aerocyonics)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



G-32 HwA Subgroup Presentation HW CWE SIG

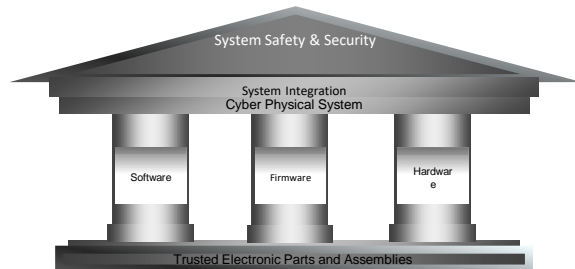
Bronn Pav, Joel Heebink

5/12/2023

G-32 Cyber Physical Systems Security Committee

•G-32 Mission

- ❖ Develop standards by characterizing and addressing the risks to Cyber Physical Systems Security (CPSS), assessing weaknesses and vulnerabilities, and recommending System Engineering focused mitigation actions defined by the operational, functional, and architectural systems engineering elements.
- ❖ Share and establish standard methods for identifying weaknesses and vulnerabilities in cyber physical systems introduced at any point in the CPSS life cycle and mitigating impacts.
- ❖ Develop validation and verification methods to ensure security requirements are addressed.



Contact: Dorothy Lloyd, DLloyd@sae.org for more information or to participate on G-32 Committee.

Gloria D'Anna
Ford
Co-Chair, USA

Bill Scofield
Boeing
Co-Chair, USA

Joel Heebink
Aerocyconics
Secretary, USA

Global Contributors

Aircraft/Engine Manufacturers, Automotive, Commercial Vehicles, Tier 1 and 2 Suppliers, Operators, Regulators, MRO Service providers, IT Product & Service Providers, Consulting Firms and Standards Organizations.

If you would like to Contribute to the work of SAE G-32, please visit:
<https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG32>.

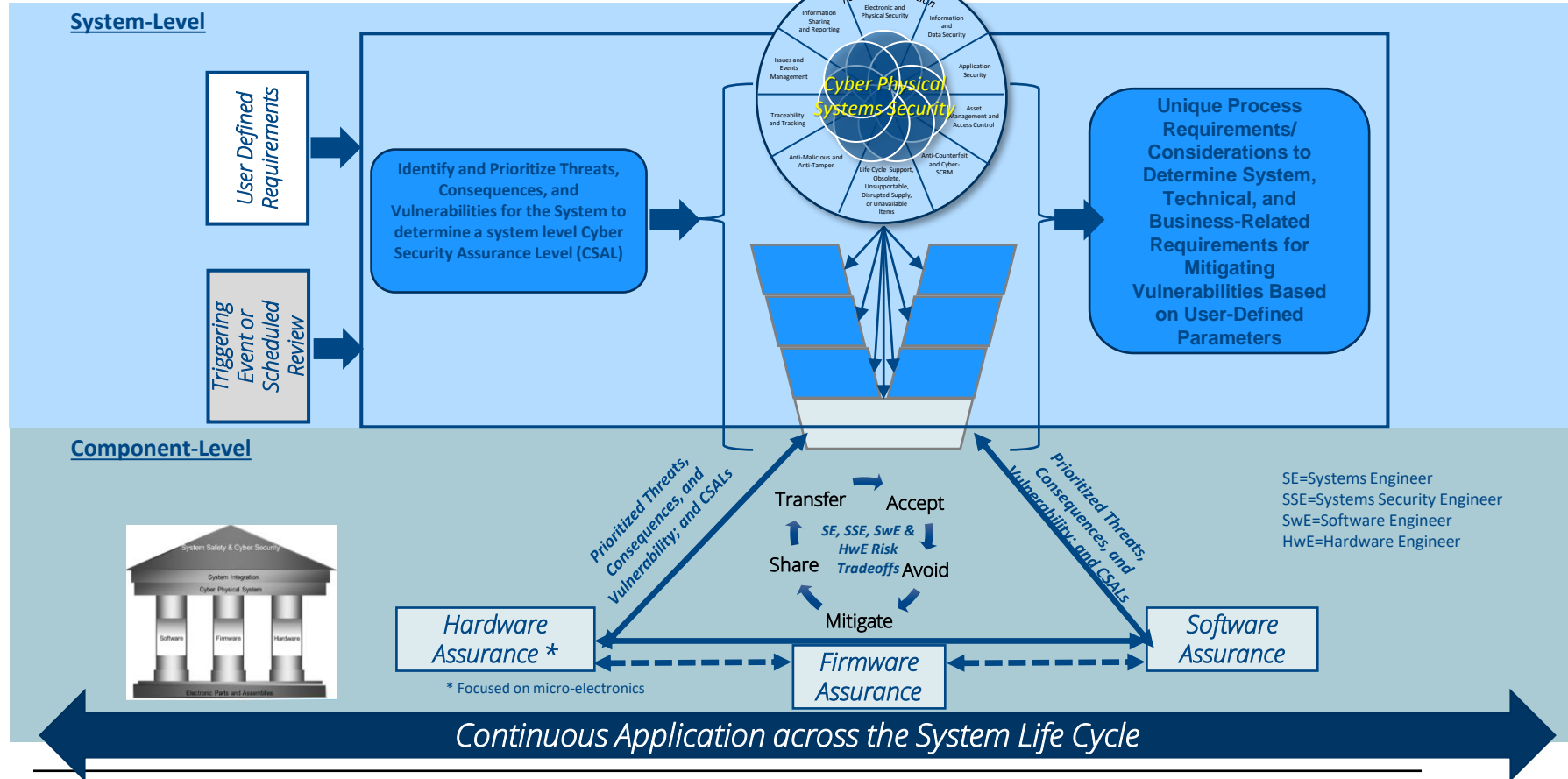
Standards in Progress for the Commercial Aviation, Defense and other high reliability and/or critical systems in aerospace, transportation, medical, etc.

[JA7496](#) Cyber Physical Systems Security Engineering Plan (CPSSEP) (Published: June 2022)

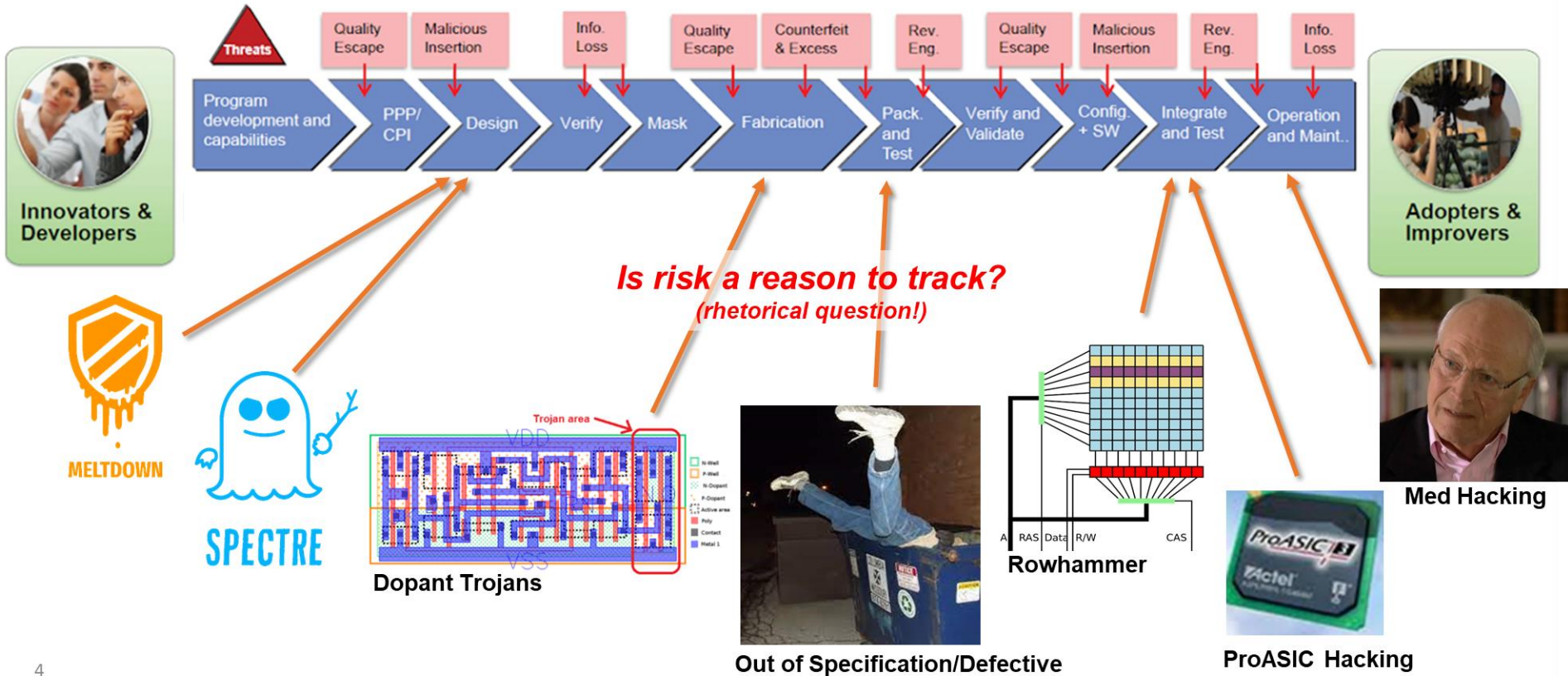
[JA6678](#) Cyber Physical Systems Security Software Assurance (Est. Publication: 2024)

[JA6801](#) Cyber Physical Systems Security Hardware Assurance (Est. Publication: 2024)

G-32 Conceptual Framework



The Microelectronics Threat Landscape - An Enormous Attack Surface





G-32 – Cyber Physical System Security (CPSS) Hw Assurance (HwA)

G32 Hardware Assurance Subgroup


- This Joint SAE Aerospace and Automotive Standard provides guidance and standardizes practices to:

GOALS:

1. clarify Hardware Assurance (HwA) requirements with CPS system engineering activities
2. identify and analyze risks associated with hardware components of concern
3. guide the evaluation (including cost and effectiveness) of potential countermeasures
4. evaluate the countermeasures and provide reports on the resulting implementations
5. maintain, control and report evidence of hardware assurance activities for compliance
6. support the adaptation of the risk model to triggering events

Objective: Document process to build and collect assurance claims of a microelectronic component that are verified throughout development, integration and end-system use

SAE has provided this Draft document for the SAE Committee. This document is SAE copyrighted, intellectual property. It may not be shared, downloaded, duplicated, or transmitted in any other way without SAE's approval. Please contact your staff representative for additional information.

 JOINT DOCUMENT HARDWARE ASSURANCE	JA6801™	REV. X XX/XX/2022
	Issued 2022 TBD	Proposed Draft
TECHNIQUES FOR ESTABLISHING HARDWARE ASSURANCE IN EEE PARTS		

RATIONALE

This standard was created in response to a significant and increasing volume of cyber physical system exploits due to a broad range of attack vectors over the life cycle of the system. Attack vectors are introduced through weaknesses and vulnerabilities in electronic parts and software that could be used to compromise cyber physical system function or gain access to critical and sensitive system information. Attack vectors can be introduced through hostile code at the time of software or firmware updates. Cyber physical systems are susceptible to compromising attacks due to counterfeit tampered electronic parts with embedded malware or hardware Trojans or legitimate components with vulnerabilities due to the design. The Hardware Assurance process described in this standard verifies that electronic components function as intended and are assessed to identify known weaknesses and vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property.

FOREWORD

To assure customer satisfaction, industry organizations must produce, and continually improve, safe, reliable, secure, and resilient systems that meet or exceed customer and regulatory authority requirements. The globalization of industry and the resulting diversity of regional/national requirements and expectations has complicated this objective. Threats to cyber security cover a broad range of attack vectors with the integration of complex hardware, software, and firmware supporting the cyber physical system that further complicates the objective. Assessing cyber vulnerabilities can be daunting and depends on where one draws the boundaries. Cyber system vulnerabilities include software, hardware, firmware, adjacent systems in the network, energy supplies that power it, and users who interface with it. It is a pervasive threat environment.

This document standardizes requirements, practices, and methods related to the hardware, and more specifically the electronic parts, in cyber physical systems security across multiple industry sectors. It also provides a risk management framework that includes an integrated approach across physical, information, cognitive, and social domains to ensure resilience.

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reserves each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2021 SAE International
All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-486-7222 (inside USA and Canada)
Tel: +1 724-776-4870 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS: <http://www.sae.org>

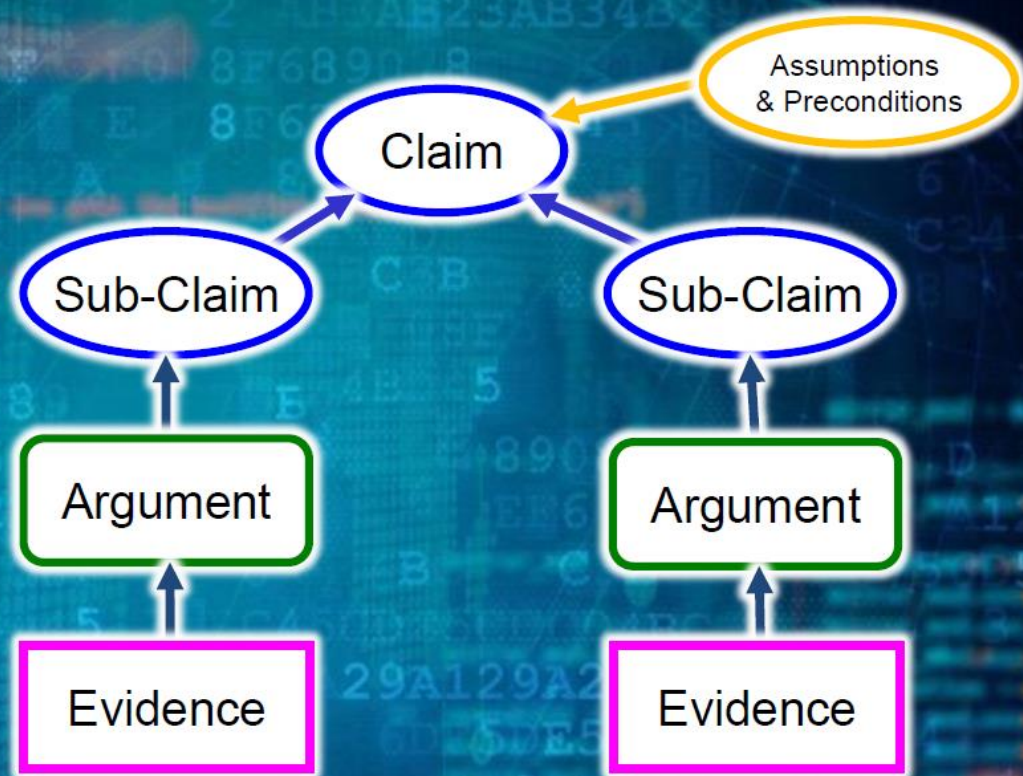
For more information on this standard, visit
<https://www.sae.org/standards/content/PRODCODE/>

The Basics of an Assurance Case

Claim =
assertion to be proven

Argument =
how evidence supports claim

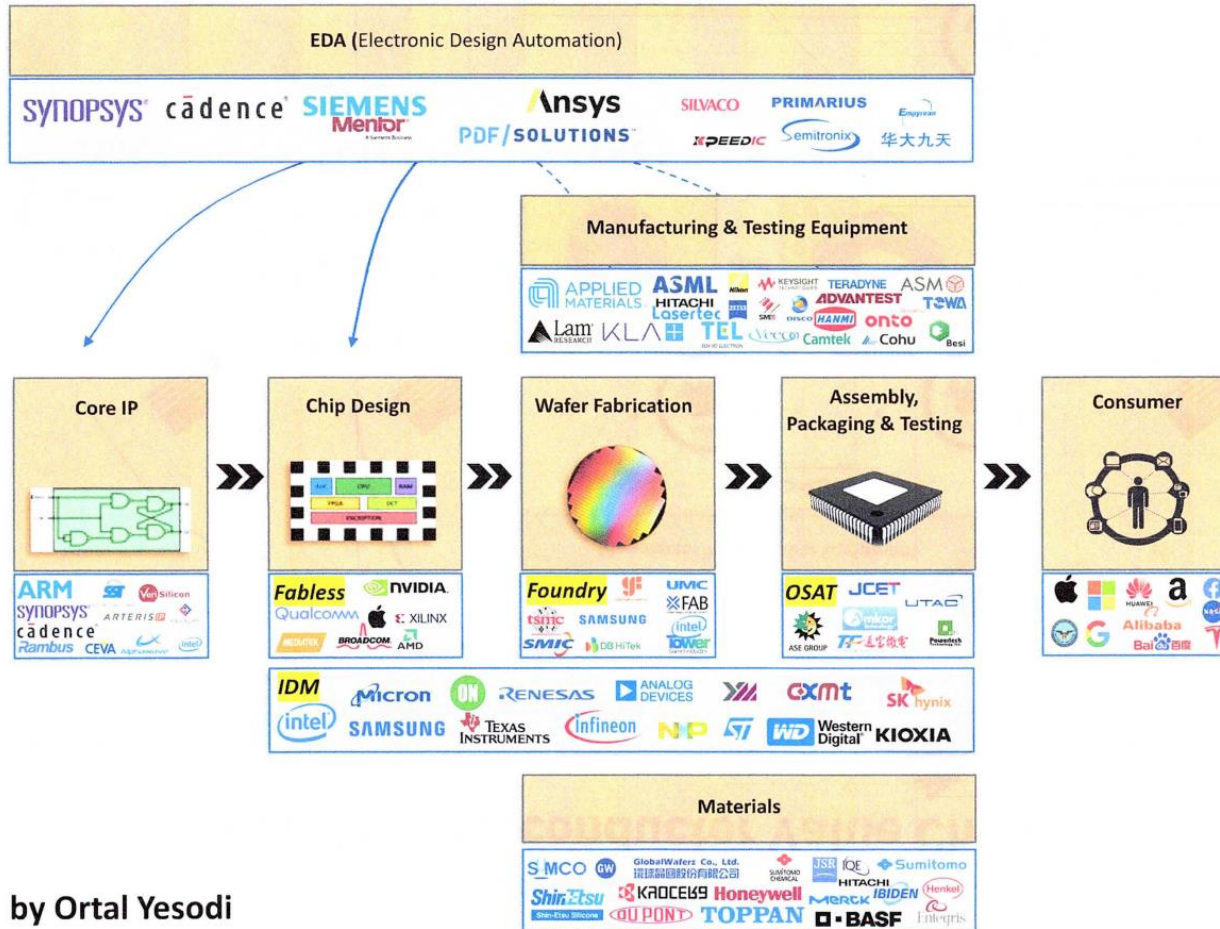
Evidence =
required documentation



Conceptual Timeline for JA6801

Action	Q1 CY23	Q2 CY23	Q3 CY23	Q4 CY23	Q1 CY24	Q2 CY24	Q3 CY24	Q4 CY24
Integrate existing written standard into scope outline		October 2023						
Incorporate risk scoring framework from the CHEST projects for quantifying assurance metrics into the standard			December 2023					
Complete Draft requirements for completing assurance case within each supply chain phase				March 2024				
Complete risk-based framework process for evaluating risk in different supply chain lifecycle phase					June 2024			
Complete integrating examples as guidance within each lifecycle phase						October 2024		
Standard draft and review for ballot submission							December 2024	

US Semiconductor Value Chain



by Ortal Yesodi

The SAE G-32 HwA Subgroup Help Request

The ASK: Contribute and participate in the drafting of the standard document including the processes for the assessment and mitigation of risks for their particular phase of the supply chain and committing your participation as:

- Full contributor/author/editor – potentially 5+ hours per week
- Meeting attendance/contributor – 1 to 2 hours per week
- Liaison role, comment on document only – as needed to review document

Please Contact One of the Following

Bronn Pav

bronn.pav@aerocyonics.com

401-251-2188

Daniel DiMase

daniel.dimase@aerocyonics.com

401-398-2343

Joel Heebink

joel.heebink@aerocyonics.com

401-365-6145

Dorothy Lloyd

dorothy.lloyd1@sae.org

724-772-8663



Thank you!

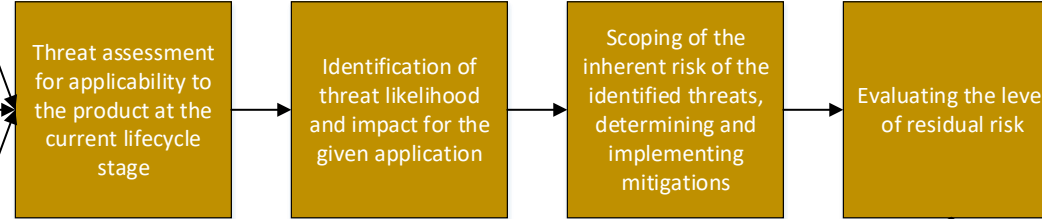
Threat Inputs

Certificate Authority
from previous
lifecycle stages

Threat matrix
applicable to the
current lifecycle
stage

Threats applicable
to previous lifecycle
stages that were
discovered after the
initial assessment
was performed

Threat Assessment



Certificate
Authority for the
current lifecycle
stage

BOM/
deployment/etc.
(stage
dependent)

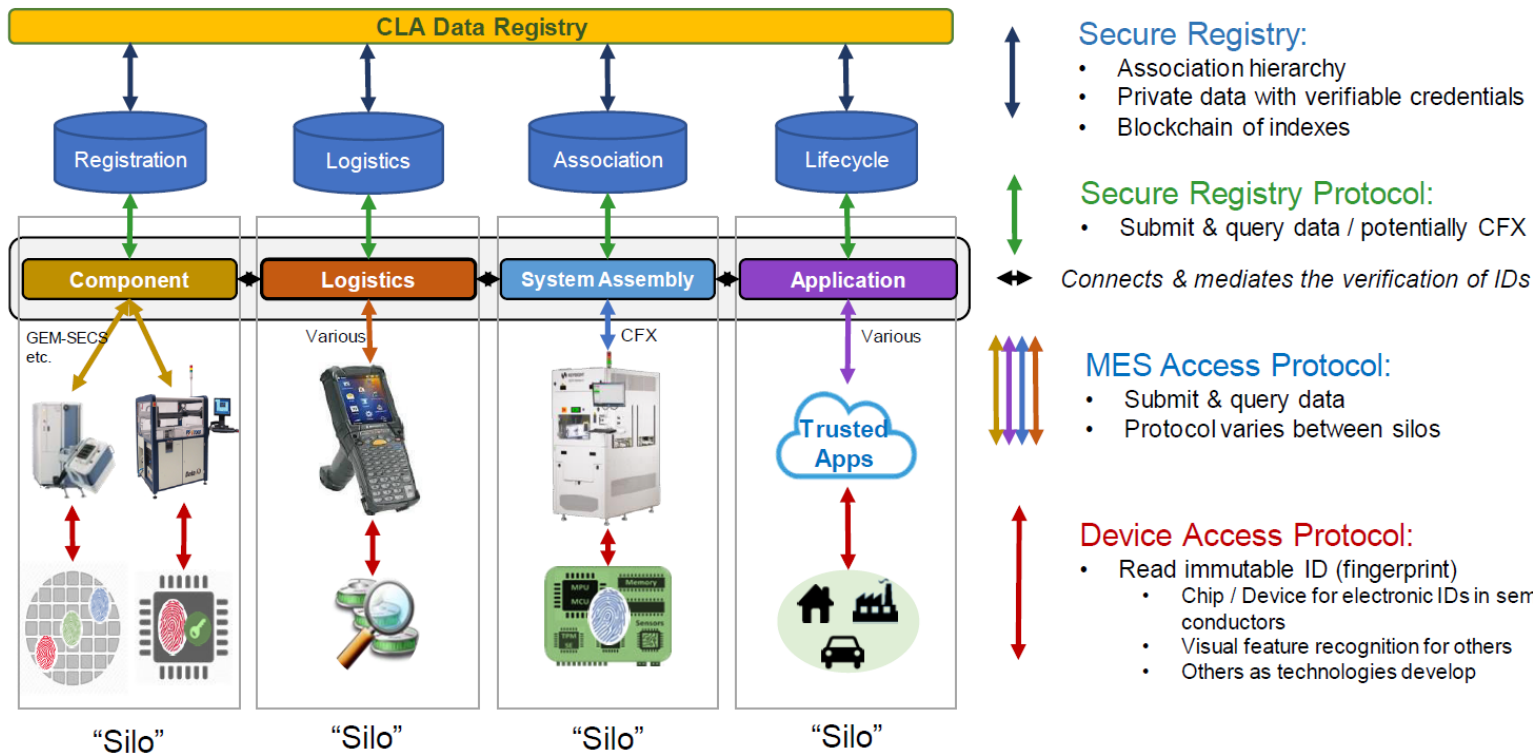
Assessment Outputs

Assurance Defined (from SAE JA7496)

- ASSURANCE: Grounds for justified confidence that a claim has been or will be achieved.
 - NOTE 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated.
 - NOTE 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims. For further guidance on assurance, refer to the ISO/IEC 15026 document series.
- 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).

Component-Level Authentication

Components of IPC-1783



Other Related IPC Standards

- **IPC-1782 “Standard for Manufacturing and Supply Chain Traceability of Electronic Products”**

This standard establishes minimum requirements for manufacturing and supply chain traceability based on perceived risk. It applies to all products, processes, assemblies, parts, components, equipment and other items used in the manufacture of printed board assemblies and in mechanical assembly. (Revision will include “Secure Supply Chain” section outlining packaging and logistics requirements and 4 levels of security options for each material, process, event, and asset owner)

- **IPC-1791 “Trusted Electronic Designer, Fabricator and Assembly Requirement”**

This standard provides minimum requirements, policies and procedures for printed board design, fabrication and assembly organizations/companies to become trusted sources for markets requiring high levels of confidence in the integrity of delivered products. (Elements include: quality systems, chain of custody, risk management, and security)

- **IPC-2591 “Connected Factory Exchange”**

This standard establishes the requirements for the omnidirectional exchange of information between manufacturing processes and associated host systems for assembly manufacturing. This standard applies to communication between all executable processes in the manufacture of printed board assemblies, automated, semi-automated and manual, and is applicable to related mechanical assembly and transactional processes. This standard also sets the messaging requirements for equipment to be listed on the IPC-CFX-2591 Qualified Products List (QPL).

Source: IPC

Next Meeting (June 9)

CWE@MITRE.ORG

- **Mailing List:** hw-cwe-special-interest-group-sig-list@mitre.org
 - **NOTE:** All mailing list items are archived publicly at:
 - <https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/>
- **What would members of this body like to see for the next HW SIG agenda?**
- **Questions, Requests to present? Please let us know.**



Backup



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Covert Channels and Side Channels

- This is a discussion item on the GitHub
- Accidental transmission vs intentional transmission
- "A side channel is where information **leaks accidentally** via some medium that was not designed or intended for communication; a covert channel is where the **leak is deliberate**." – *Ross Anderson*
- Hardware view should have coverage in the hardware view –*Jason Oberg*
- CWE-514 is a class weakness for Covert Channels
- Covert Channels should be in the HW categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test Problems.
–*Paul Wortman*
- Should we place CWE-514 in the HW View? Or create a base of CWE-514 and put that into the HW view?

CWE-514: Covert Channel

Description

- A covert channel is a path that can be used to transfer information in a way not intended by the system's designers.

Extended Description

- Typically the system has not given authorization for the transmission and has no knowledge of its occurrence.

