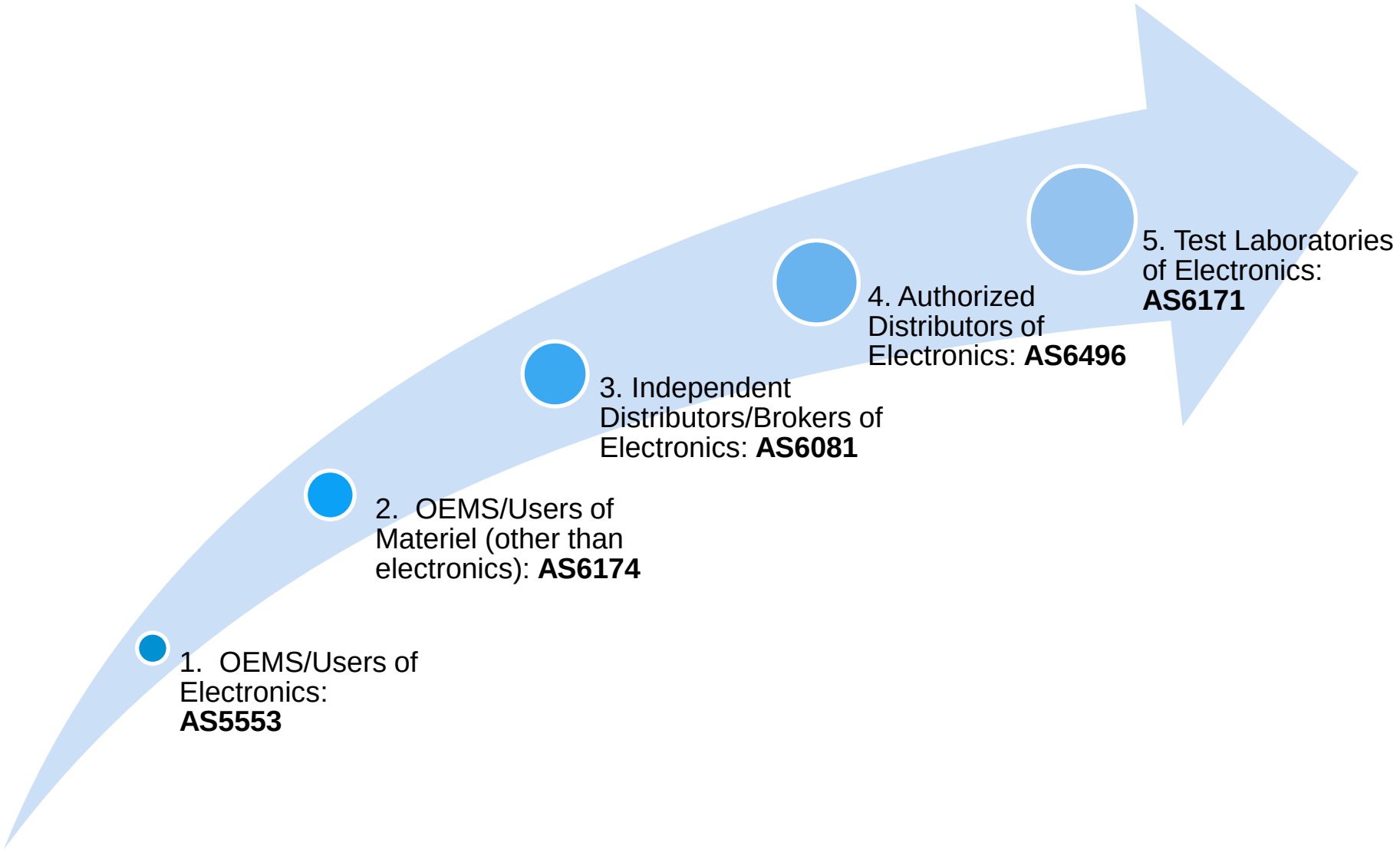
SAE INTERNATIONAL

SAE INTERNATIONAL STANDARDS- COUNTERFEIT AVOIDANCE, DETECTION, MITIGATION AND DISPOSITION

November
2015

Director, Washington Operations
SAE International
www.sae.org

G-19 & G-21 Counterfeit Prevention & Detection Standards



SAE G-19 & G-21 Document Proposed Roadmap, September 2013

SAE Counterfeit Avoidance Steering Group

G-19 Counterfeit Electronic Components Committee Oversight
Phil Zulueta, SAE G-19 Chairman

G-21 Counterfeit Materiel Committee Oversight
Wayne Moss, Bob Tipton, SAE G-21 Co-Chairman

Auditor Competency (Asxxxx)

Proficiency Test Provider
(ISO/IEC 17043 Accredited)

Certification Body
(IAF & ISO/IEC 17021 Accredited)

Test Provider
(Accredited to ISO/IEC 17025 & Certified to AS9100 and/or ISO 9001)
Operator(s) Certified to PT Scheme for Identified AS6171 Test Methods

Original Component Manufacturer
(Certified to AS9100 and/or ISO 9001)

Distributor
(Certified to AS9120 and/or ISO 9001)

Authorized/ Franchised

Broker/ Independent

Original Equipment Manufacturer/User/MRO
(Certified to AS9100 and/or AS9110 and/or ISO 9001)

Test Provider
(Certified to AS9100 and/or ISO 9001)

AS6171, Test Methods Standard; Counterfeit Electronic Parts
Document in progress. Dan DiMase & Sultan Lilani, Subcommittee Co-Chairman, Mike Megrdichian, Document Coordinator, SAE **G-19A**

Asxxxx, Compliance Standard or Guide
(Includes Audit Checklist)
Bill Scofield, Brian Worden - Subcommittee Co-Chairmen, SAE **G-19C**

ASxxxx, OCM Counterfeit Mitigation Subcommittee. Subcommittee Proposed. SIA, SRC Proposed Co-Chairpeople, SAE **G-19O**

ASxxxx, Compliance Standard or Guide
(includes Audit Checklist)
Bill Scofield, Brian Worden - Subcommittee Co-Chairmen, SAE **G-19C**

AS6496, Authorized Distributor Counterfeit Mitigation Sub-com. Document in progress Kevin Sink & Robin Gray Co-Chairman, SAE **G-19AD**

Asxxxx, Compliance Standard or Guide (Includes Audit Checklist) Bill Scofield, Brian Worden, Sub-com. Chairmen, SAE **G-19C**

ARP6178, Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors. Worksheet and User Guide Published 2011-12-19
Dan DiMase & Fred Schipp, Subcommittee Co-Chairmen, SAE **G-19DR**

AS6081, Counterfeit Electronic Parts Avoidance, ID's. Published 2012-11-7. Rev. A in progress Phil Zulueta Chairman, SAE **G-19D**

AS6301, Compliance Standard or Guide (includes Audit Checklist) Bill Scofield, Brian Worden, Sub-com. Chairmen, SAE **G-19C**

AS5553A, Fraudulent/ Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. Issued 2009-04-02. Rev. A published 2013-01-21. Sarah Skinner, Subcommittee Chairperson, SAE **G-19CI**

AS6462, AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria Includes Audit Checklist. Published 2012-11-01. Rev. A in progress.
Bill Scofield, Brian Worden - Subcommittee Co-Chairmen, SAE **G-19C**

AS6174, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel
Published 2012-05-09. Rev. A in development. Wayne Moss, Bob Tipton – Subcommittee Co-Chairmen. Materiel Subcommittee, SAE **G-21**

AS6174, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel
Commodity Slash Sheets in Rev. A document. Wayne Moss, Bob Tipton – Subcommittee Co-Chairmen. Materiel Subcommittee, SAE **G-21**

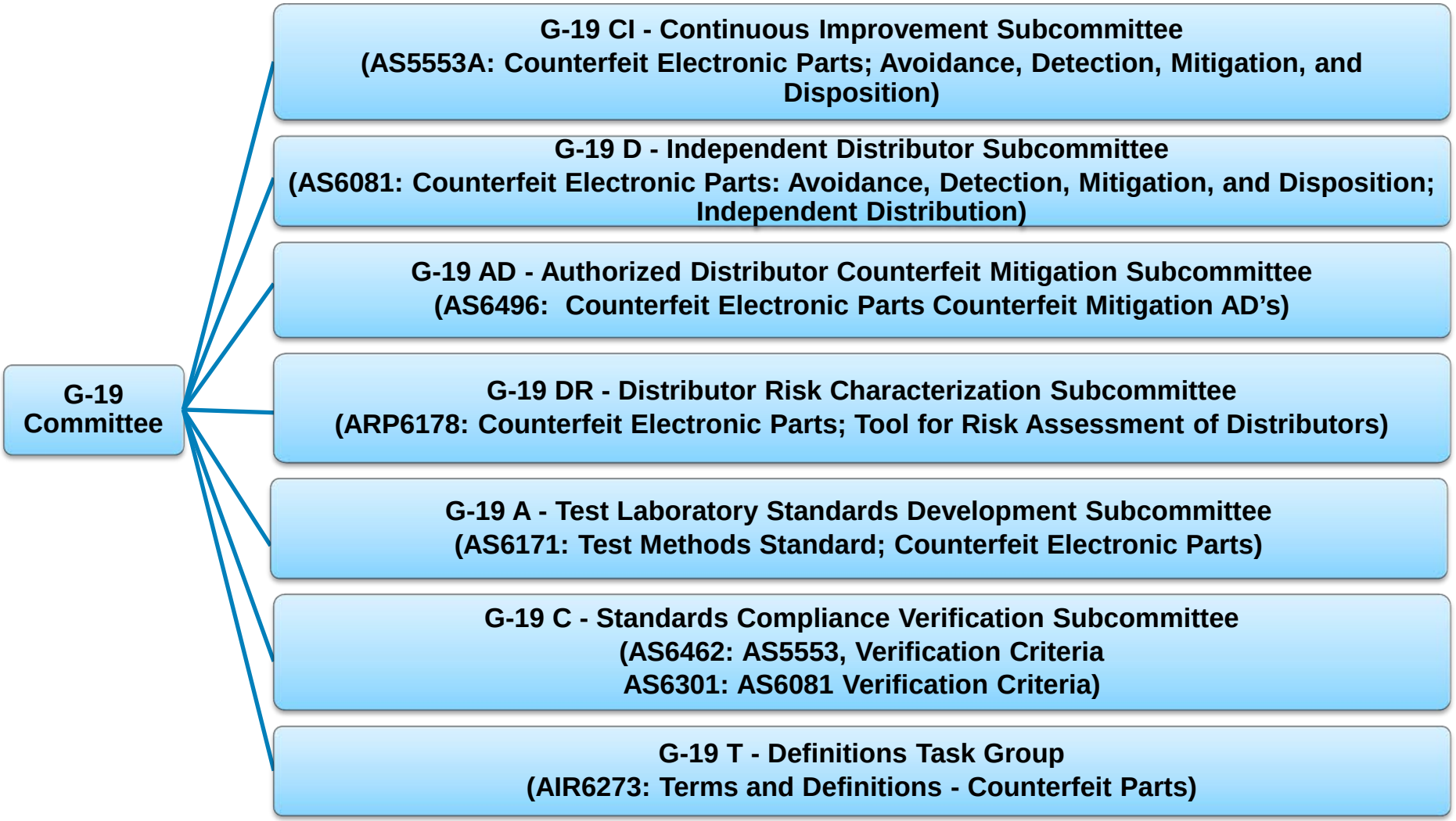
Asxxxx, Compliance Standard or Guide
(Includes Audit Checklist)
Bill Scofield, Brian Worden - Subcommittee Co-Chairmen, SAE **G-21C**

AIR6273, Terms and Definitions – Fraudulent/Counterfeit Electronic Parts
Document in progress. Kirsten Koepsel, Subcommittee Chairperson, SAE **G-19T**

ASxxxx, Anti-Tamper and Transportation Security
Subcommittee Proposed. TAPA, CBP, Express Carrier Proposed Co-Chairpeople, **G-19AT**

Published | In Development | Gap

G-19 Subcommittees Formed Since 2009



Summary of SAE G-19/G-21 Aerospace Standards

Standard	Title	Status
SAE AS5553A (G19-CI)	Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition	Issued January 2013 and available at www.sae.org. Rev B in development
SAE AS6462 (G19-C)	Verification Criteria for Certification against AS5553	AS5553 verification criteria for first release published – 2011-11. Discussions underway for certification programs/schemes. Rev. A verification criteria in ballot
SAE AS6171 (G19-A)	Test Methods Standard; Counterfeit Electronic Parts	In draft; Individual test methods balloted. Main document balloting in process
SAE AIR6273 (G19-T)	Terms and Definitions:	In draft.

Summary of SAE G-19/G-21 Aerospace Standards

Standard	Title	Status
SAE AS6081A (G19-D)	Counterfeit Electronic Parts Avoidance – Independent Distributors	Published 2012-11. Rev. A in development.
SAE AS6301 (G19-C)	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Independent Distributors Verification Criteria	In draft.
SAE ARP6178 (G19-DR)	Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors	Published 2011-12.
SAE AS6496 (G19-AD)	Authorized Distributor Counterfeit Mitigation	Published 2014-08
SAE AS6174 (G-21)	Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel	Rev. A Published 2014-07. Rev B and slash sheets (refrigerants, fasteners) soon

QUESTIONS?

Director, Washington Operations
SAE International

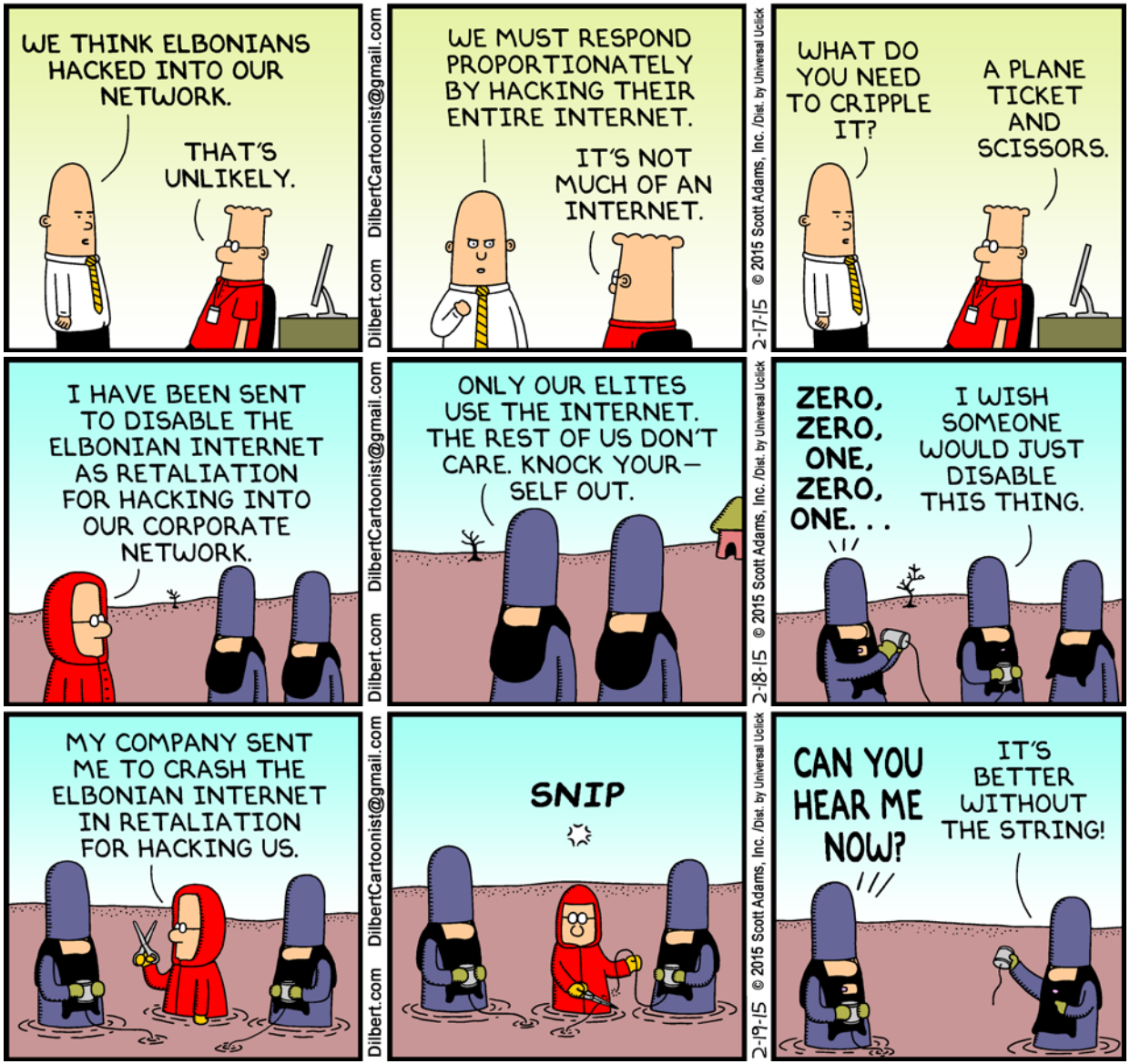
SAE INTERNATIONAL

ENSURING HARDWARE CYBER SECURITY

September 2015

SAE G-19A Committee Chair
SAE International
www.sae.org

Time for Action! Dilbert Gets Hacked!



Course Objectives

- **Awareness and Understanding of the Threat**
- **Current Government Policy – DFARS**
- **Terms, Definitions and Taxonomy**
- **Introduction to Cyber Physical Systems Security (CPSS)**
- **Industry Efforts**
  - SAE G-19A Tampered Subgroup
  - CPSS and the Systems Engineering Approach
- **Recommended Next Steps**
- **Future Work**

Problem Statement and Executive Response

- **Attack vectors are applied to vulnerabilities in electronic parts* associated with tampering (as defined by the SAE organization).**

- **These threats to hardware assurance and security cover a broad range of attack vectors in cyber physical and industrial control systems supporting the U.S. critical infrastructure and national security.**

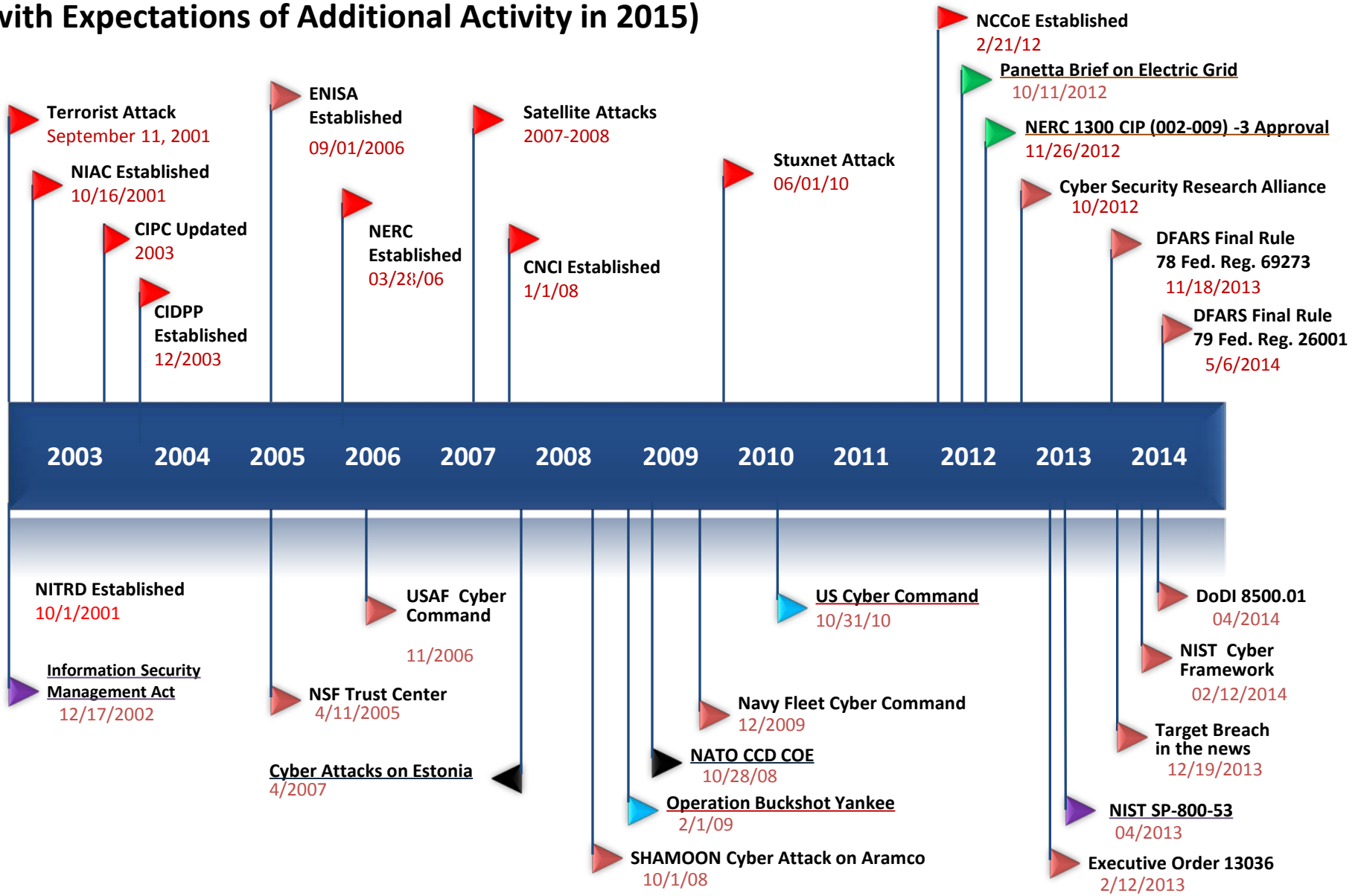
- **In response, Executive Order 13636 - *"Improving Critical Infrastructure Cybersecurity"* calls for the development of a *Cybersecurity Framework* (NIST, 2013), which is charged with the task of adopting and implementing risk-based standards to identify high-risk infrastructure and select alternatives for risk mitigation.**

---

*Definition of electronic part includes circuit assemblies as defined by DoD

A Partial Listing of Major Cyber Physical Systems Related Milestones

(with Expectations of Additional Activity in 2015)



Industry data breaches and cyber attacks increased in 2014 by 23.9% compared with 2013 to 761 reported breaches exposing 83,176,279 records

(http://www.idtheftcenter.org/id-theft/data-breaches.html)

DFARS HOT TOPICS

Definition of *Electronic Part* Discussion
"Embedded Software or Firmware"
Implications*

Hardware Assurance & Security for Cyber Physical Systems

DFARS Requirements

- ***Electronic part*** **means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81). The term "electronic part" includes any embedded software or firmware.***

The Definition Implies Hardware Cyber Security Concerns

**Definition of electronic part DFARS 252.246-7007*

Cyber Physical Systems (CPS)

Tangible Output*

Power

Refined Oil

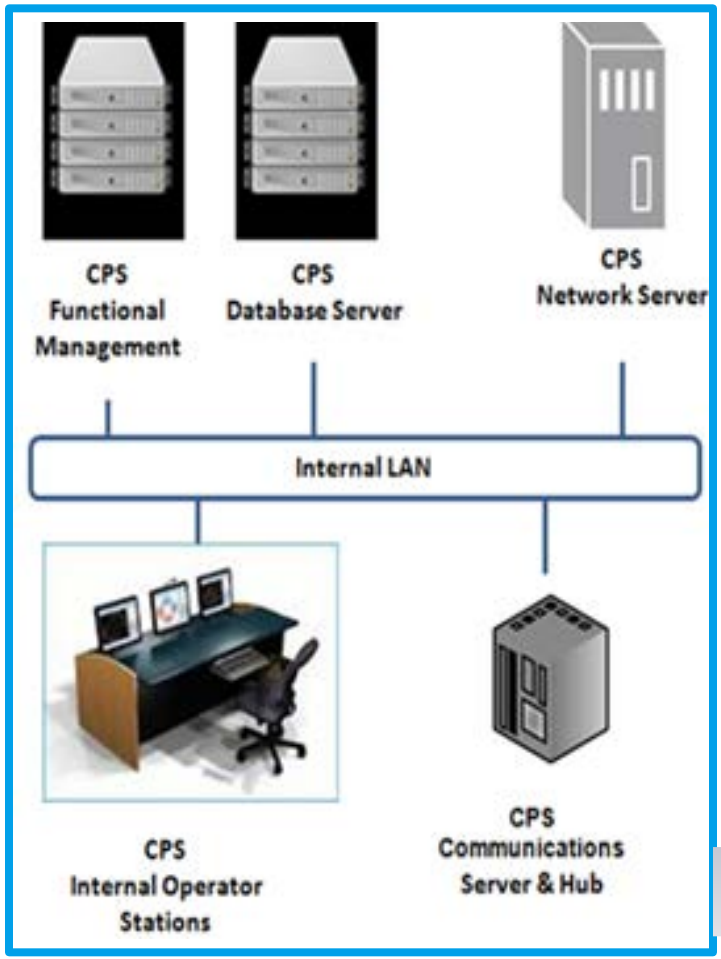
Financial Transaction

Communication

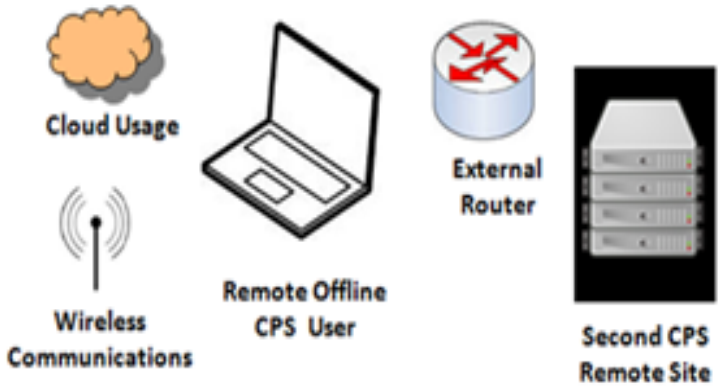
Patient Health Status

Water Pressure

*** Per NITRD CPS**



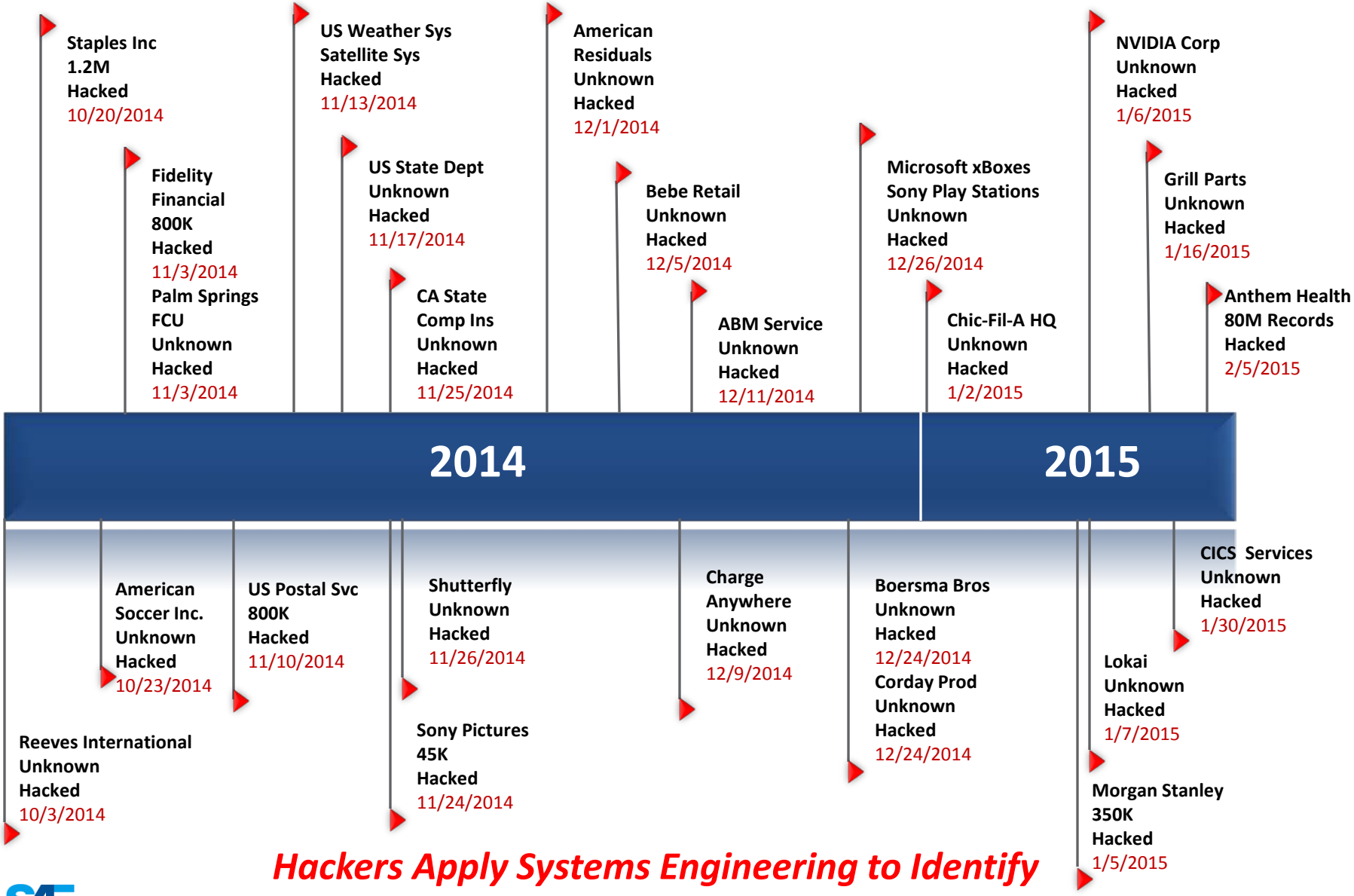
Connected to Numerous Cyber Physical Systems



External Communication

CPS Includes Industrial Control Systems and IT.

Six Months of Recent Notable Hacking Attacks



Hackers Apply Systems Engineering to Identify Vulnerabilities in Cyber Physical Systems

SAE INTERNATIONAL

What are the Challenges for CPS-Security?

- The dependencies of CPS on technology
- **HW /SW Vulnerabilities make the possibility of disruption greater than ever**
- CPS Stakeholder loss of confidence has high impact to business
- Scalability of the CPS-security design
- CPS Performance prediction
- **Advancement of attacker's capabilities**
- **Highly sophisticated clones**
- Attacker's intent
- Security and Privacy in CPSS
- Modeling and Simulation
- **Lack of detection for embedded chip features**
- CPS Risk Assessment and Decision Analysis
- CPS Resiliency Definition

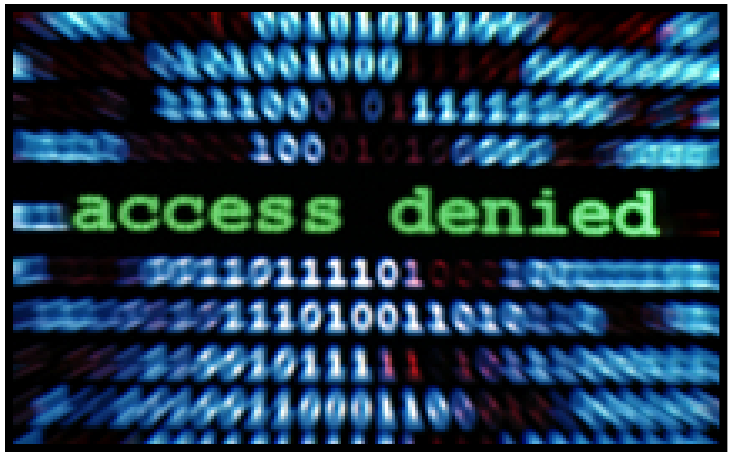
Source:
2014 CHASE Workshop
Cyber Physical Systems Panel

Panel members included:
DHS, DOD, NIST, NSF, and Government Consultants

Hardware Cyber Security

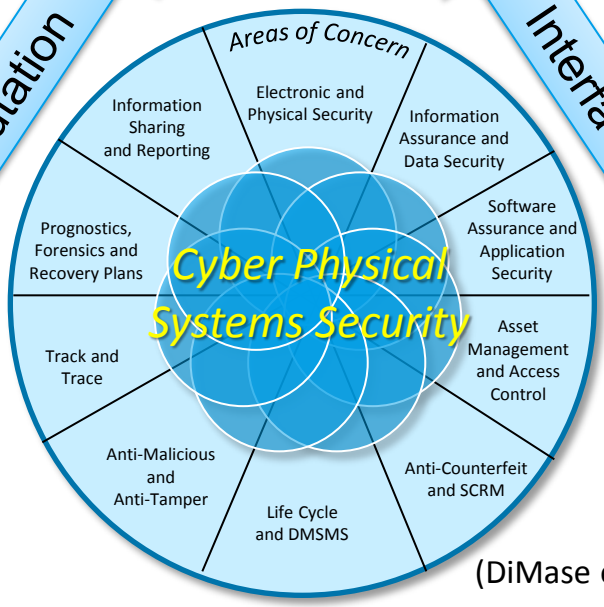
Cyber Physical Systems Security **is a complex topic with areas of concern that need to be addressed to maintain resilient systems.**

- **Need to establish a taxonomy that enables a common understanding for integrating an approach.**
- **Elements of the approach include current and future risk assessment, presentation of any gaps, and resolution to mitigate risks across areas of concern.**
- **Cyber ranges and improvements of test methods to detect vulnerabilities and threats needs to be developed.**



Cyber Physical Systems Security

Today's Cyber Physical Systems (CPS)



Data and Computation

Interfaces and Network

(DiMase et al., 2015)

Software

Command and Control

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

SAE INTERNATIONAL

Industry Efforts to Address Hardware Cyber Security Threats

Hardware Cyber Security

Electronic Piece Parts

Tampered: **A part modified for sabotage or malfunction.**

Tampering can occur at any phase of a part's life cycle [design thru usage].

For example:

- ***Tampered chips can act as silicon time bombs where their functionality is unexpectedly disrupted at a critical moment.***
- ***Tampered chips may contain backdoors that give access to critical system functionality or leak secret information to an adversary.***
- ***Tampered parts may also perform unauthorized or inappropriate functions that could cause loss of control of the system.***

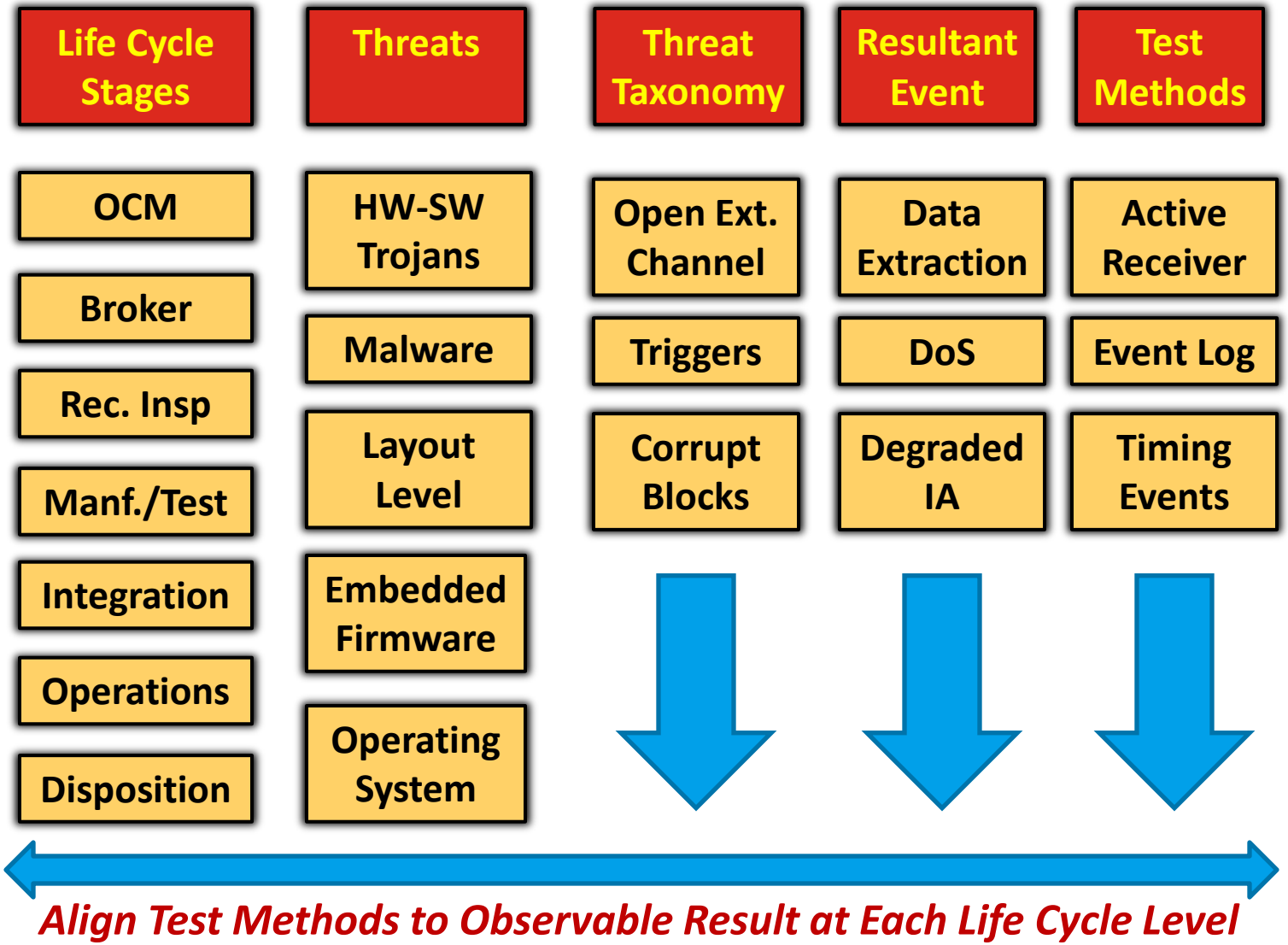
Tampered Counterfeit Electronic Parts May Include Maliciously Altered Firmware or Software

SAE G-19A Tampered Subgroup Efforts

- **For the first release of AS6171, SAE G-19A has proposed an assessment of a programmable device as part of the evaluation (to determine if it is pre-programmed).**
- **G-19A main committee voted unanimously to form a "Tampered" subgroup.**
- **Summarized Scope & Expected Outcome:**
  - Advance the knowledge of how advanced malicious features are introduced and applied in electronic parts.
  - Develop a detailed taxonomy of defects associated with tampered counterfeit parts.
  - Develop cost effective test methods capable of detecting defects associated with tampered counterfeit parts.
  - Establish and standardize methods for detecting the presence of malicious features in electronic parts that could be introduced at any point in the component life cycle.

G-19A Tampered Subgroup Effort is Limited to Electronics Piece Parts.

SAE G-19A Tampered Subgroup Efforts

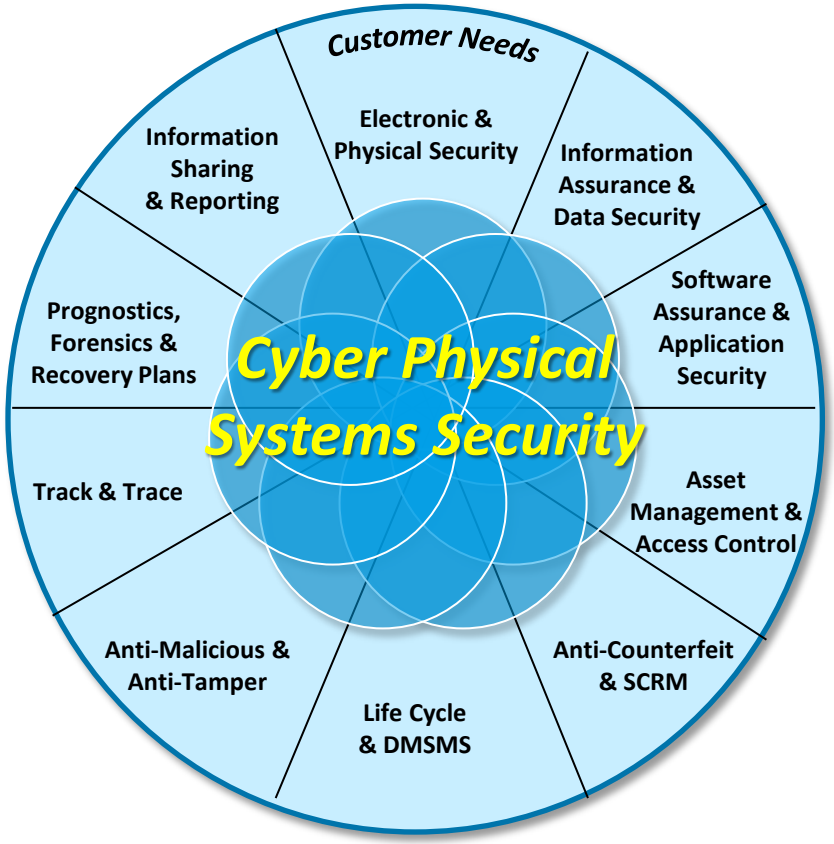


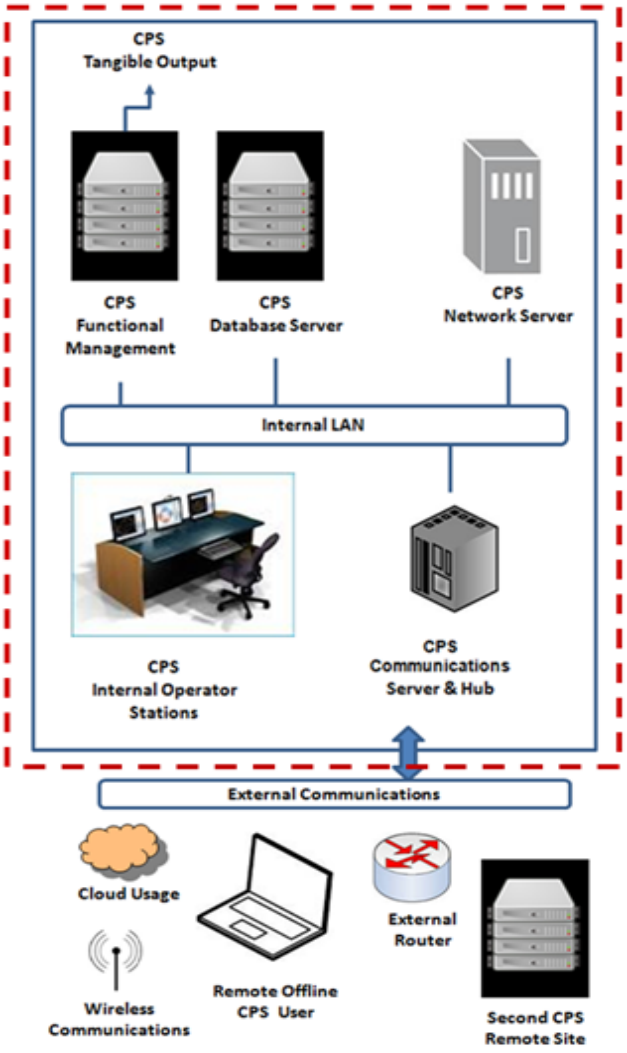
Malware Expression Table

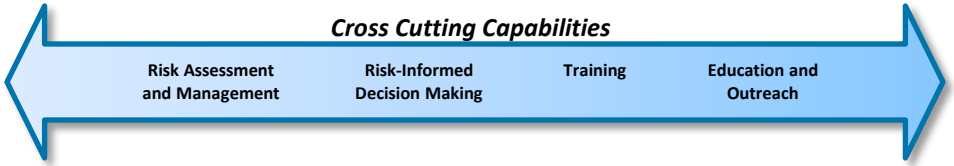
Unintended Communication Channel	Hardware Modification (enables invasive operations)	Security Defect (Component Level)	Interruption of Functional Behavior	Differ from Test Reference Part (operation, or physical)
I/O ports and points of information leakage	Functions outside of the specifications of the part (Designed-in or Tampering)	Backdoor unlocking	Non-uniform or random failures.	Component Physical Analysis :
Undocumented access to information. Unintended from buyer perspective.		Security feature failure (includes Dopant, and other HW attacks) Security side-affects/leakage	Premature failure (incoming through lifecycle reliability issues). Deny of access to memory Destroy information (overwrite or erasure) Disclose memory Distort information (modify memory)	•Visual Inspection • X-Ray, • Plating (leads XRF) • FTIR/RAMAN • Die attachment (SEM-EDS) • Thermal Signature • EMI, RF, Magnetic • Scanning Acoustic Microscopy

CPSS for Assemblies & Subsystems

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective







Introduces an Integrated Approach to the Problem that Includes Assemblies and Subsystems

Recommended Next Steps

- Support and expedite (if possible) SAE G-19A efforts to develop cost effective test methods capable of detecting defects associated with tampered parts. The group could use additional engineering SMEs.
- Support and expedite (if possible) SAE G-19A efforts to establish and standardize methods for detecting the presence of malicious features in electronic parts that could be introduced at any point in the component life cycle.
- Support from FPGA and ASIC designers who would design enabling technologies for this type of testing.
- Support and expedite (if possible) the developing cyber physical systems security effort from the SAE systems engineering committee.

Engineering SMEs Taking a Lead to Close Gaps. Organizations Could Assist by Identifying Engineering SMEs and Supporting their Participation in the Two Groups.

Future Work and Research Needs

- Identify where we have weaknesses and gaps in policy, services, and technologies in all the areas of concern as we formulate solutions for more robust, resilient cyber physical systems that protect our critical infrastructure that these systems support.
- Research is needed to design and build real-world models and ranges supporting experimentation and validation for embedded malware, hardware Trojans, and CPSS.
- Operational CPSS modeling tools will enable cost-effective, risk-based cyber resiliency requirements.
- Research is needed for detection tools for embedded malware and hardware Trojans.
- Research for User assessment toolsets will lead 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.

Summary

- **Awareness and Understanding of the Threat**
- **Current Government Policy – DFARS**
- **Terms, Definitions and Taxonomy**
- **Introduction to Cyber Physical Systems Security (CPSS)**
- **Industry Efforts**
  - SAE G-19A Tampered Subgroup
  - CPSS and the Systems Engineering Approach
- **Recommended Next Steps**
- **Future Work**

QUESTIONS?

SAE G-19A Committee Chair
SAE International