SAE INTERNATIONAL

CYBER PHYSICAL SYSTEM SECURITY

November 2016

Associate Professor and Associate Head
University of Connecticut, ECE Department

SAE G-19A Chairman Emeritus

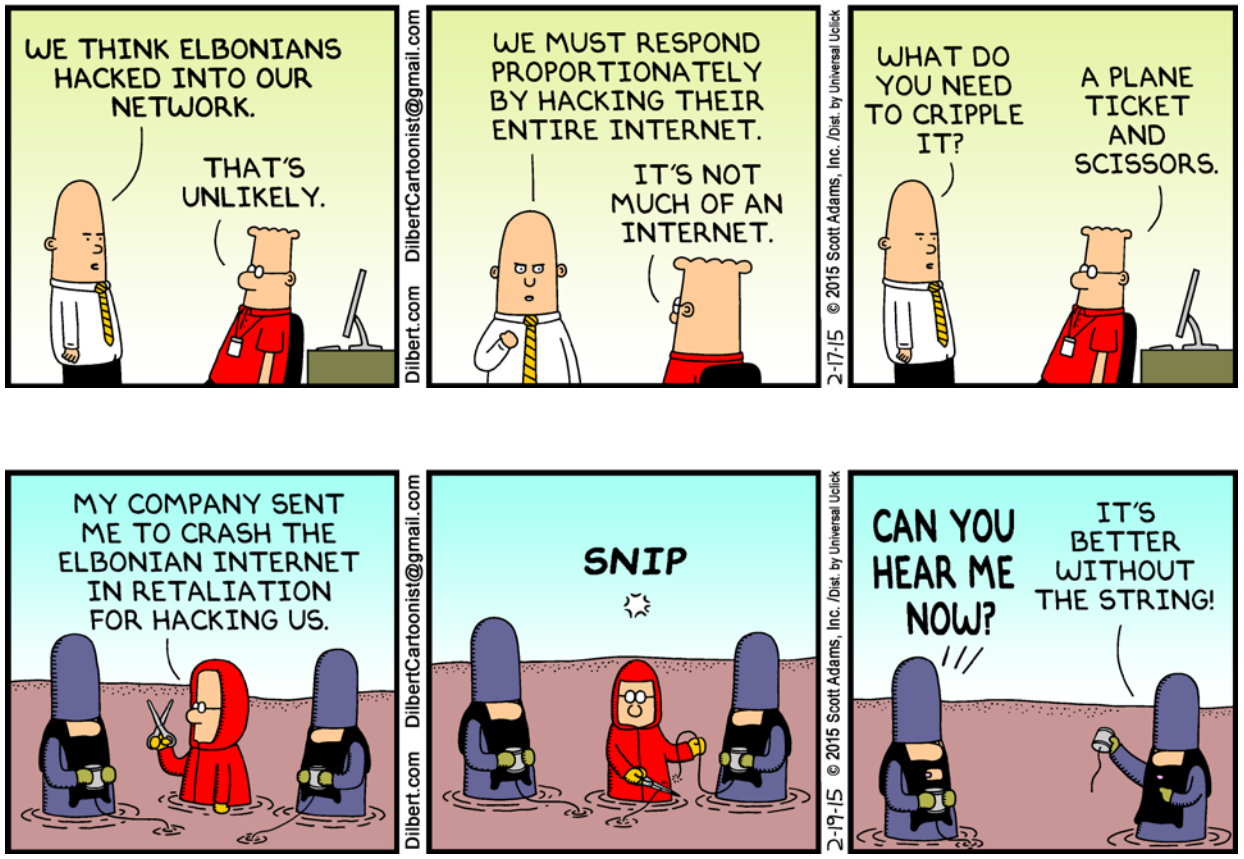
SAE G-19A Tampered Subcommittee Chair

University of Virginia

SAE International

www.sae.org

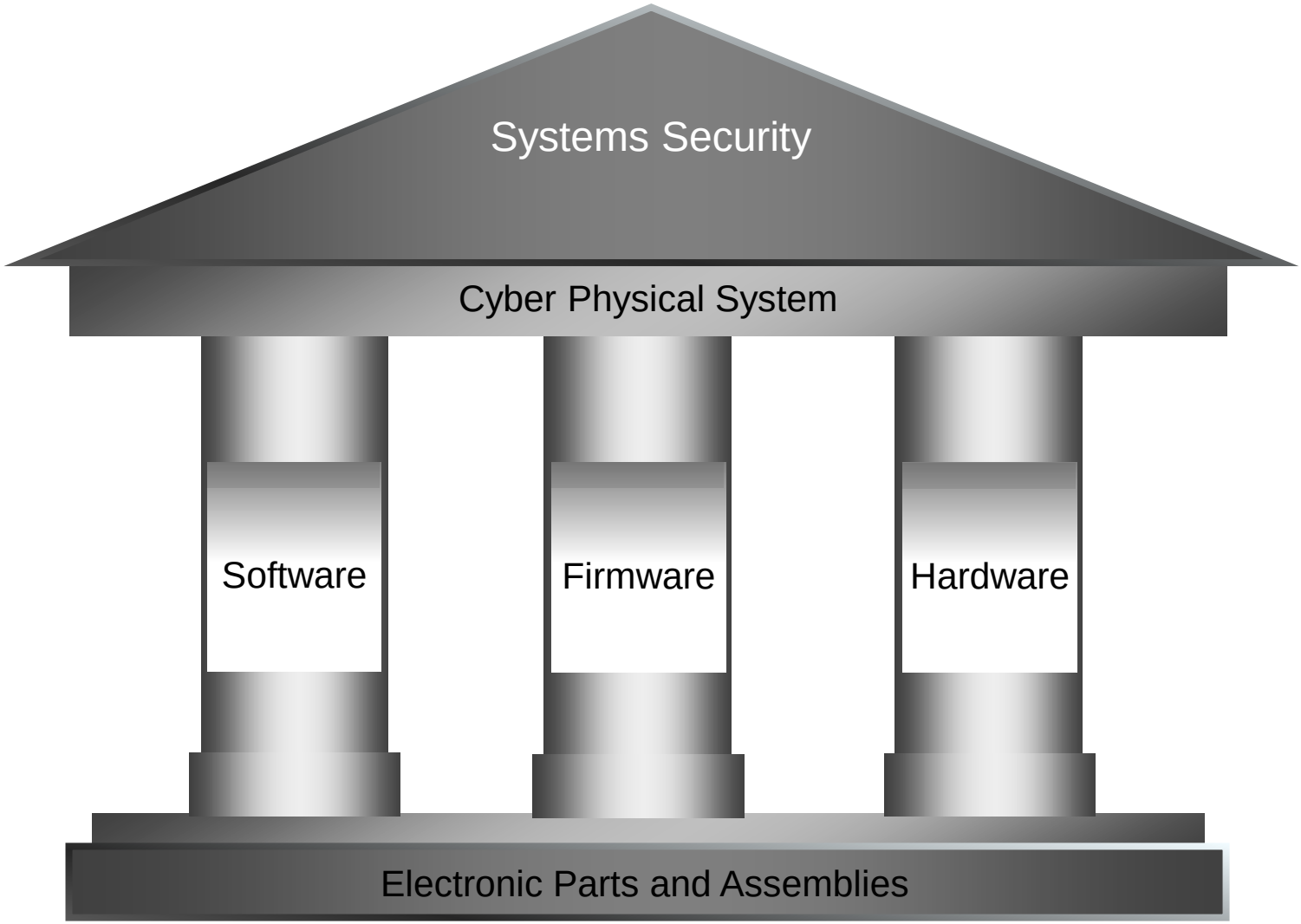
Time for Action! Dilbert Gets Hacked!



Course Objectives

- **Awareness and Understanding of the Threat**
- **Impact and Consequences**
- **Terms, Definitions and Taxonomy**
- **Introduction to Cyber Physical Systems Security (CPSS)**
- **CPSS Challenges and Business Impact**
- **Industry Efforts**
  - SAE G-19A Tampered Subgroup
  - CPSS and the Systems Engineering Approach
- **Recommended Next Steps**
- **Future Work and Research Needs**

Holistic Systems Security Engineering Approach to Cyber Security



Cyber Physical Systems (CPS)

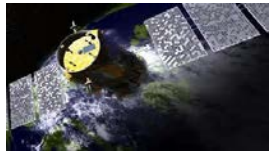
Cyber-Physical Systems also known as "smart" systems are interacting networks of physical and computational components.

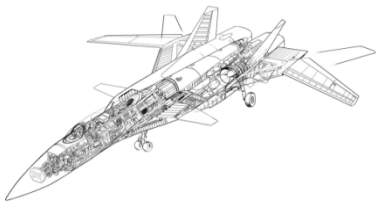
Cyber Physical Systems (CPS)

Examples of Cyber Physical Systems Include:





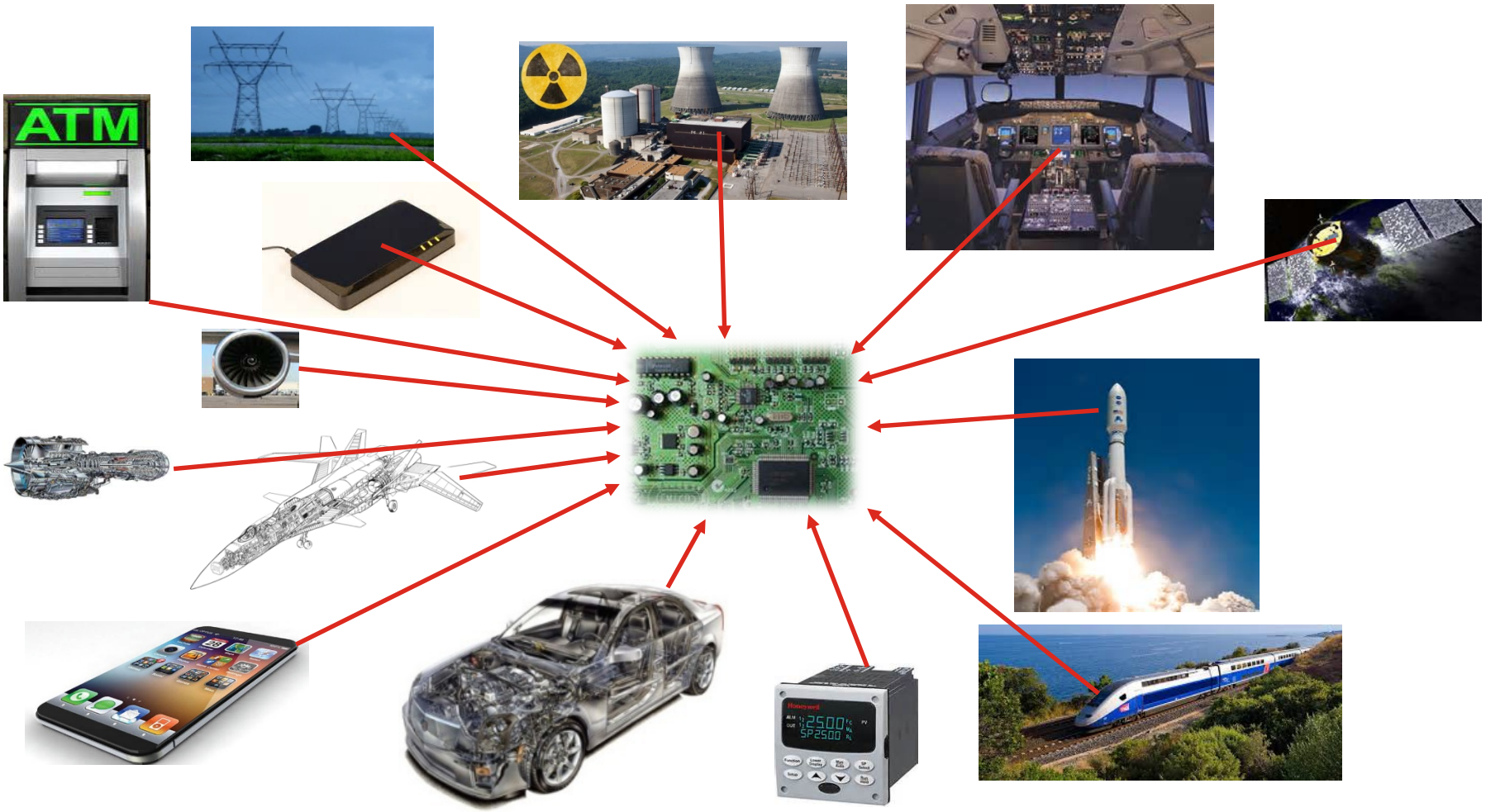




Cyber Physical Systems (CPS)

Cyber Physical Systems all contain electronic “brains” controlled by electronic parts:



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.**

How realistic are the threats?

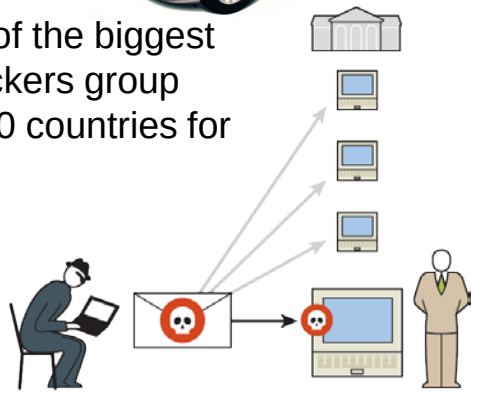
Western Digital, Seagate, Toshiba and other top manufacturers have spying software deep with in the hard drives providing the means to eavesdrop on the majority of the world's computers, according to cyber researchers and former operatives.[9]

F-Secure has unearthed a new attack, HAVEX, against industrial control systems that targets mainly European utilities firms. ”Researchers suspect they are simply gathering intelligence in preparation for a more serious attack.”[13]

“Key sweeper is a stealthy Arduino-based device, camouflaged as a functioning USB wall charger, that wirelessly and passively sniffs, decrypts, logs and reports back (over GSM) all keystrokes from any Microsoft wireless keyboard in the vicinity.”[10]

“Cars today are loaded with computers networked to each other, and those can be hacked remotely.” A laptop is all that’s needed in order to “take control of many of the car’s functions, including the braking and acceleration.”[11]

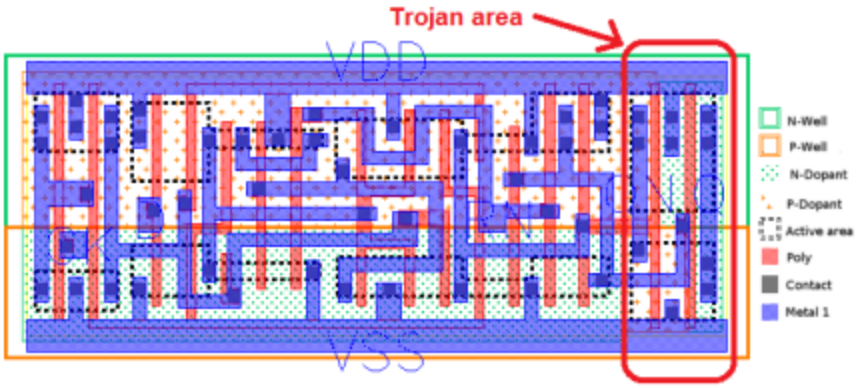
Kaspersky has revealed one of the biggest cyber-heists ever with the hackers group attacking over 100 banks in 30 countries for a bounty of $1Billion.[12]



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.



Thumb Drive Virus Takes Down the Pentagon: [15]

"The most serious cyber attack on the US military's networks came from a tainted flash drive in 2008, forcing the Pentagon to review its digital security," said former Deputy Defense Secretary William Lynn.

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 Embedded Malware or Hardware Trojans

Systems Security – Electronic 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

A German Patriot missile system stationed on the Turkish-Syrian border was reportedly hacked by a "foreign source" and carried out "unexplained commands“ suspected to be enabled through a computer chip which guides the missile, or through a real-time information exchange which allows the missiles to communicate with their control system.

Germany's President Joachim Gauck and his partner Daniela Schadt listen to commander of German troops in Turkey Colonel Stefan Drexter as they visit Patriot missile batteries in Kahramanmaras April 27, 2014.Osman Orsal/Reuters

Newsweek, July 8, 2015

Experts say that such a hack could lead to the battery failing to intercept incoming missiles or even firing at an unauthorized target.

These incidents may seem isolated but a cybersecurity expert at defense think tank RUSI, disagrees with this assumption. He believes that hacks of military missile systems may be more common than realized but go unreported for security reasons.

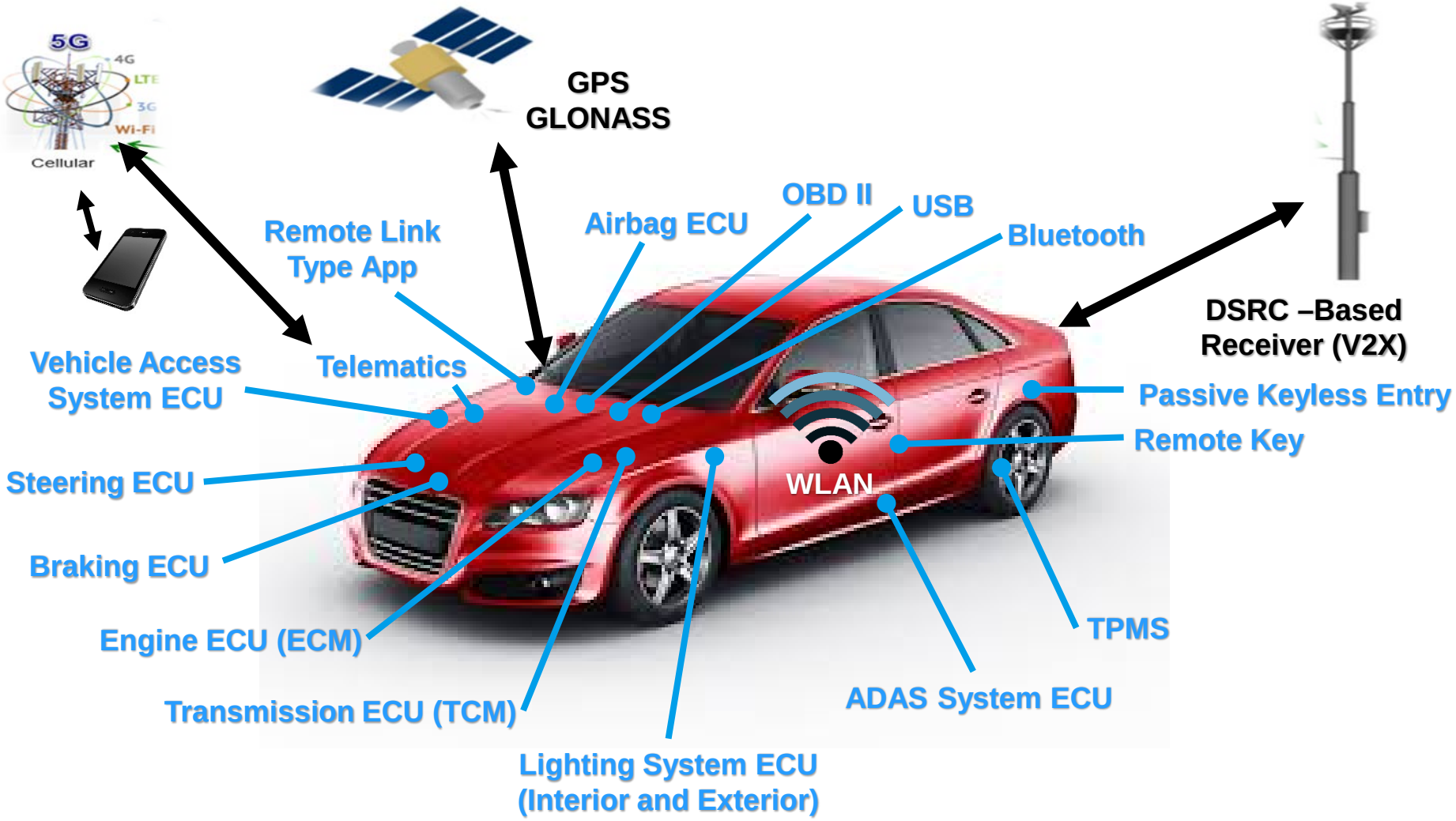
SAE G-19A Tampered Subgroup Efforts

- **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.
- **The Tampered Subgroup is:**
  - Characterizing the tampered defect taxonomy in order to first map out the areas of vulnerability in a microelectronic device.
  - Drafting both advanced techniques and low cost test processes to identify tampered parts throughout a microelectronic parts lifecycle.
  - Binding these test methods with the taxonomy for coverage so industry and government actors can tailor the solution with confidence for each application.

G-19A Tampered Subgroup Effort

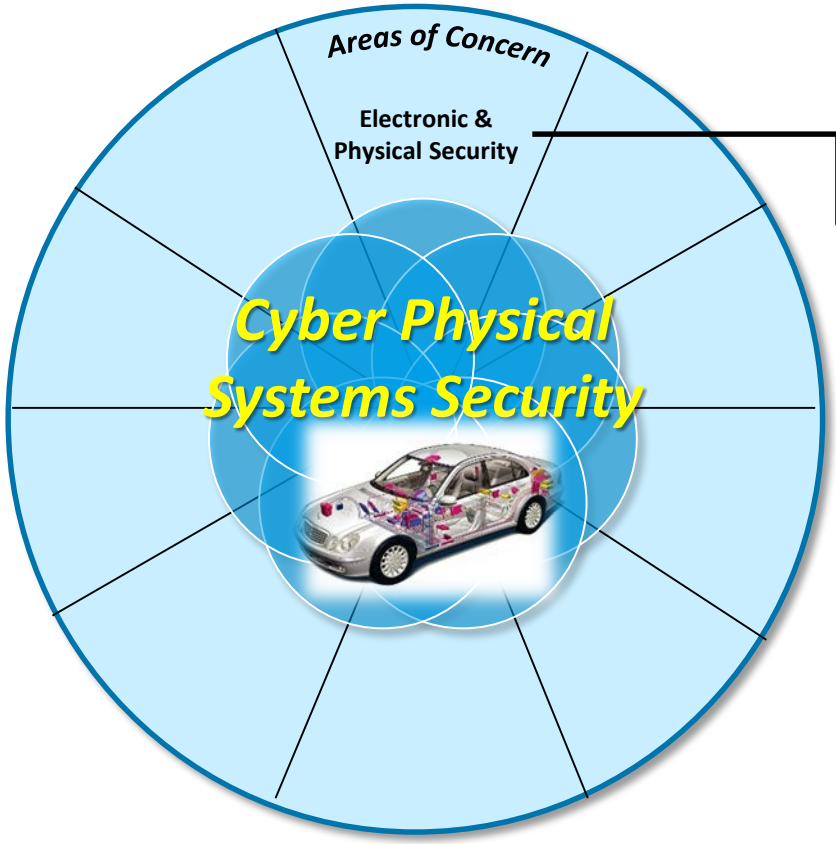
is Currently Limited to Electronics Piece Parts

Cyber Physical Systems Security



Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

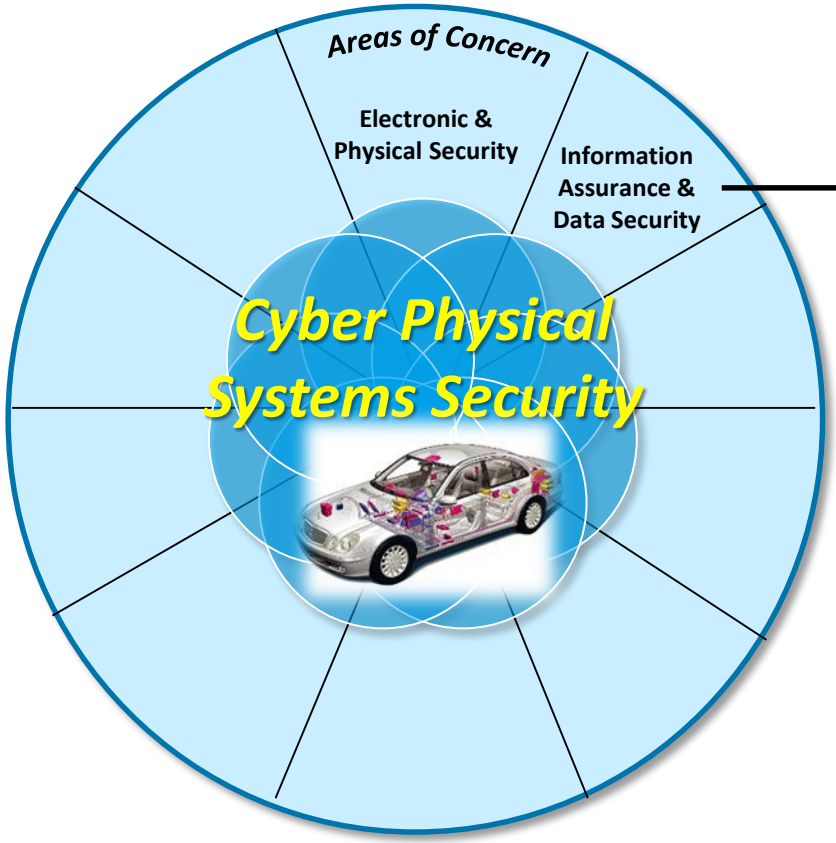


Security for both direct and indirect electronic controls to the Cyber Physical System

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

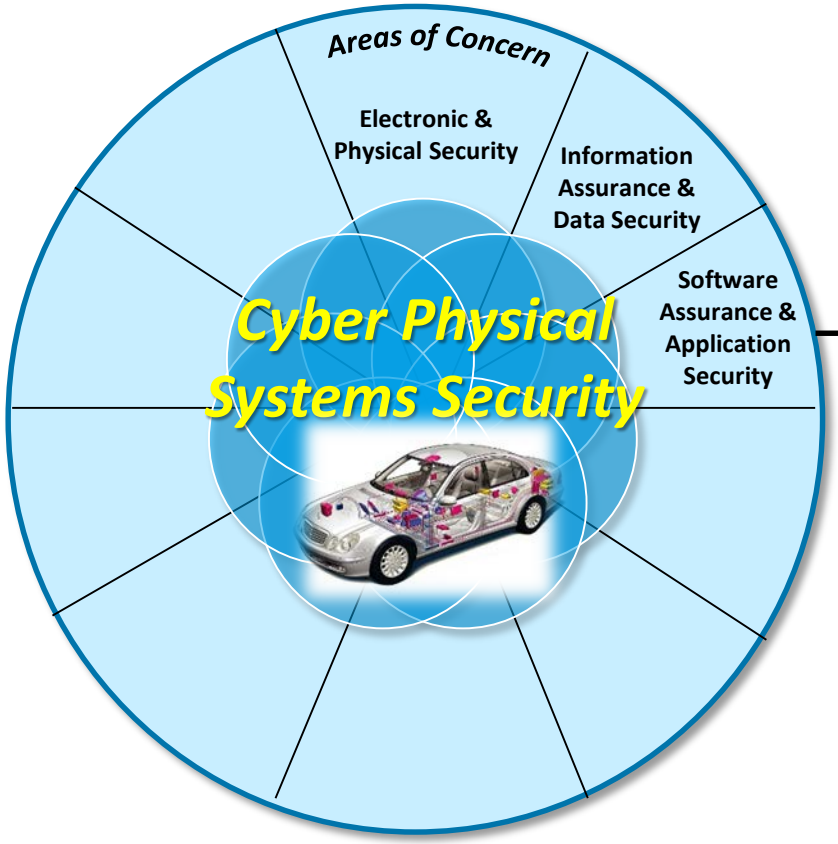


Prevent “hacking” or stealing of Personal Identifiable Information and Cyber Physical System Data.

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

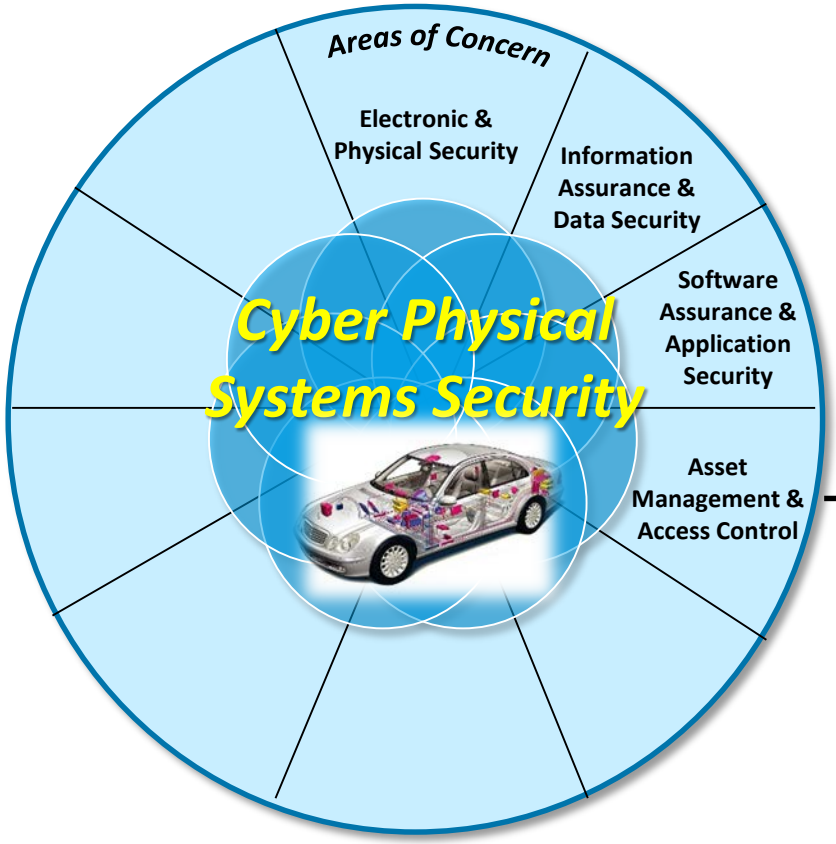


Prevent unauthorized software modifications or viruses

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

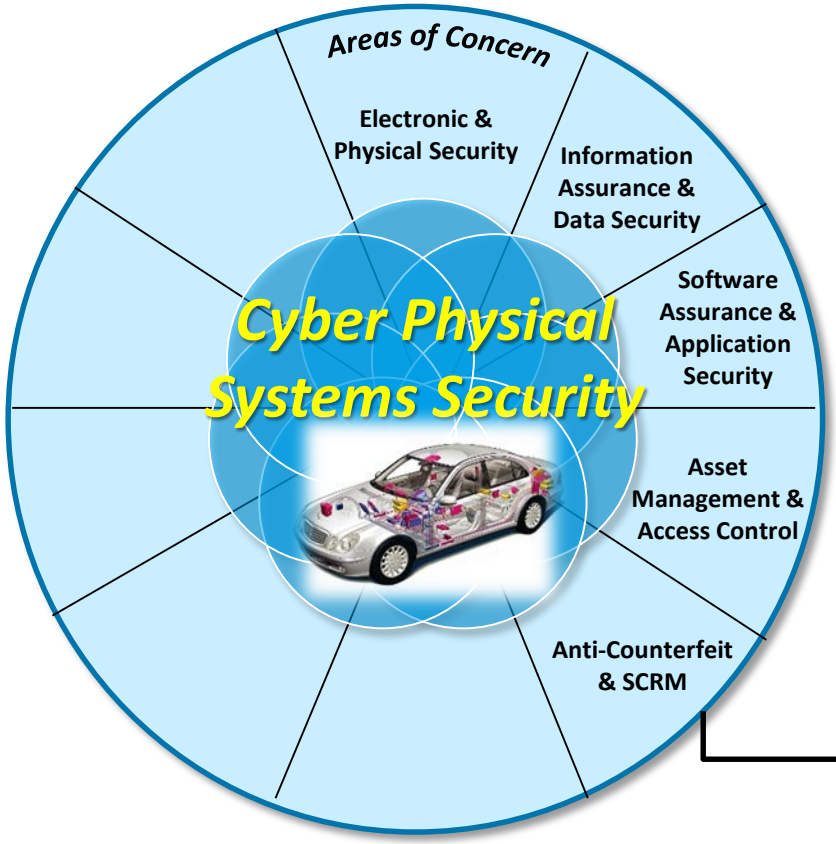


Manage Critical Assets and Verification Credentials in the Cyber Physical System

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

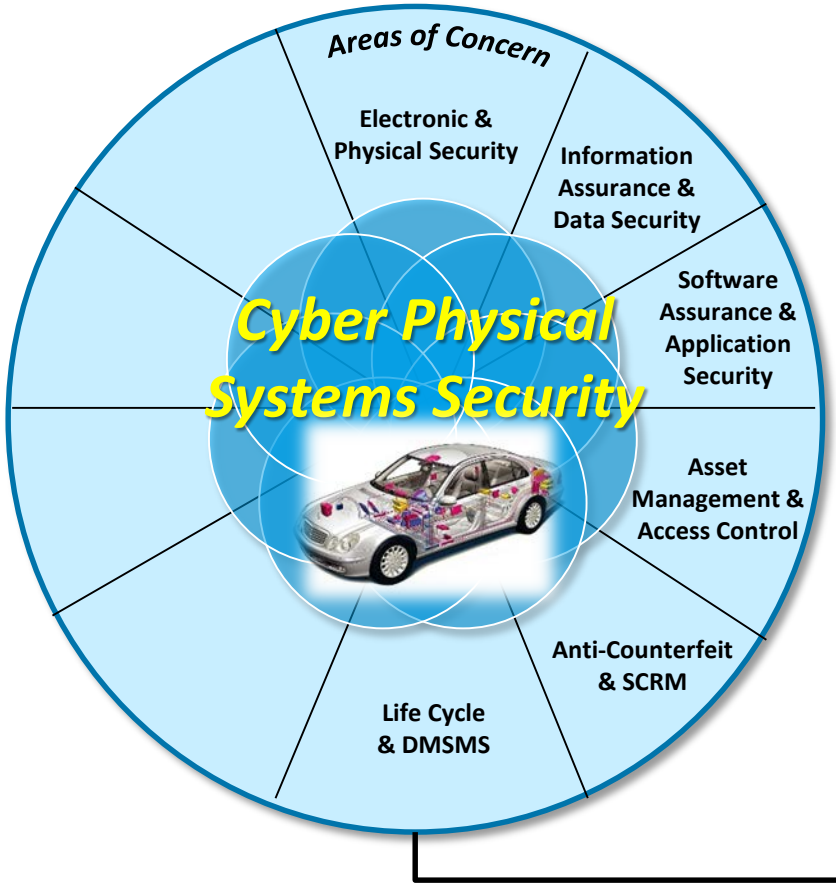


Prevent and Detect Counterfeit Parts and Implement Strategy for Supply Chain Risk Management

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

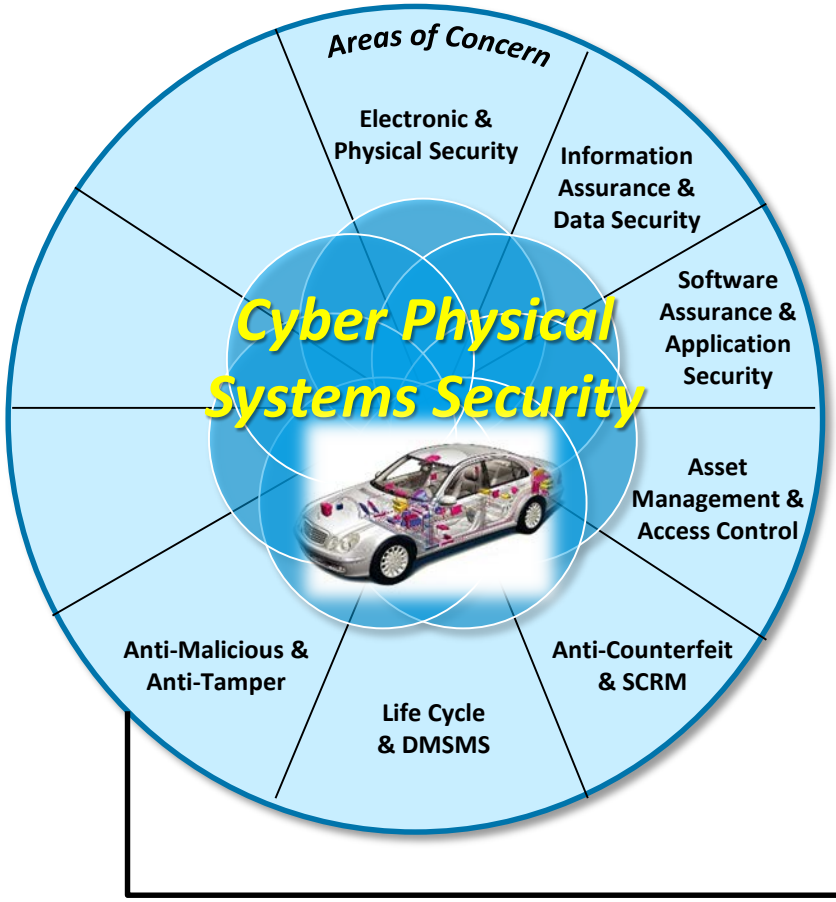


Manage Obsolescence Issues Throughout System Lifecycle

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

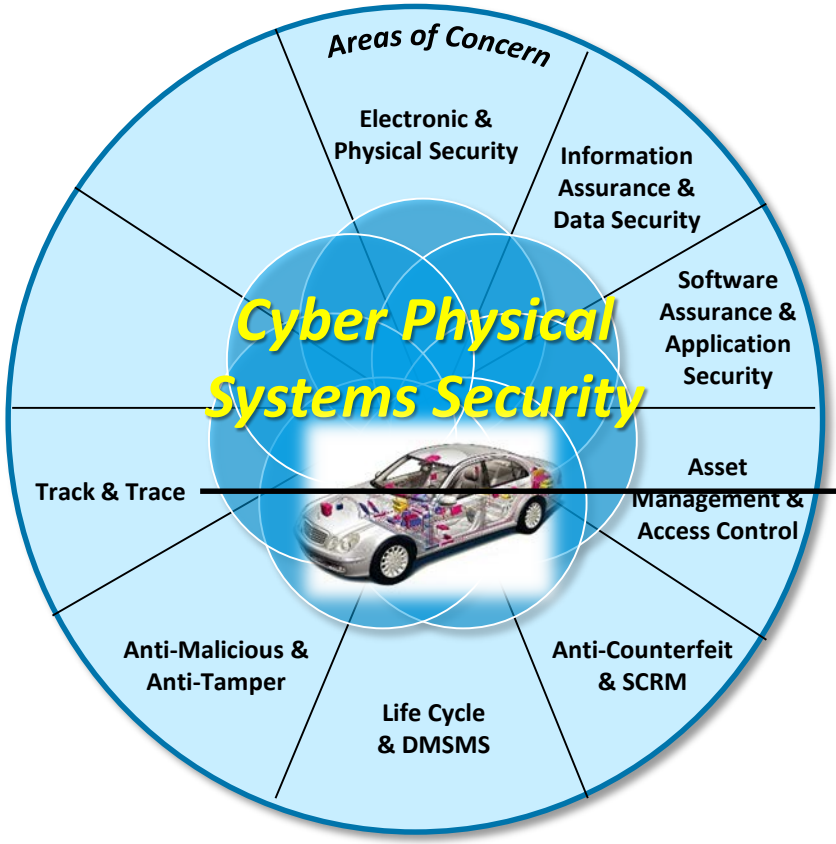


Prevent Reverse Engineering and Detect and Avoid Malicious Trojans, Attacks, and Tampering

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

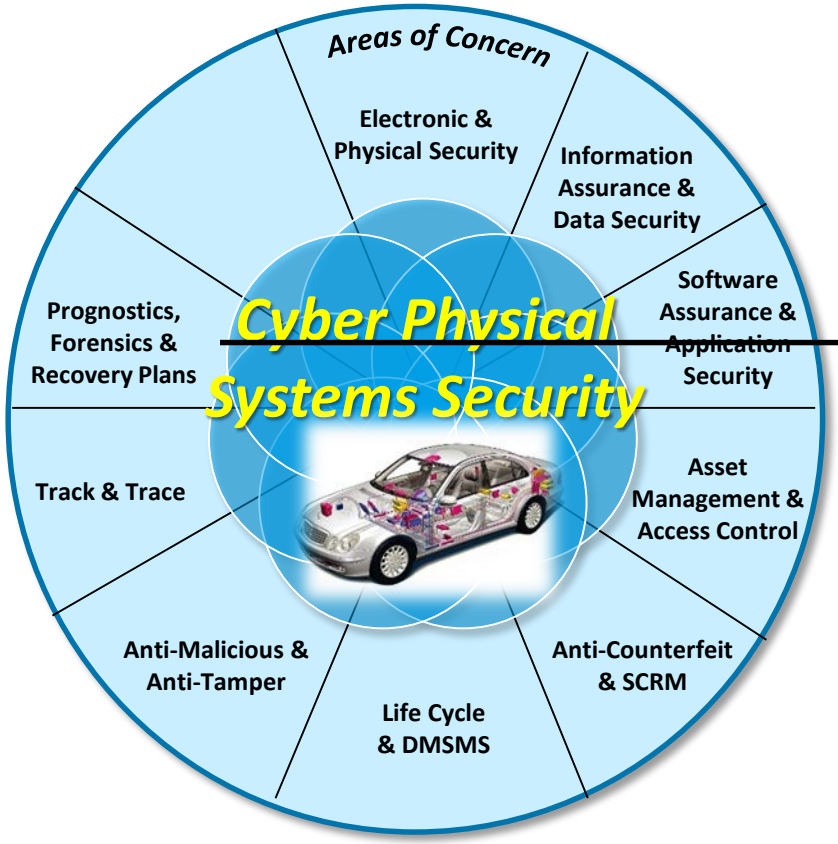


Track Piece Parts Throughout Fabrication, Assembly, and Lifecycle

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)

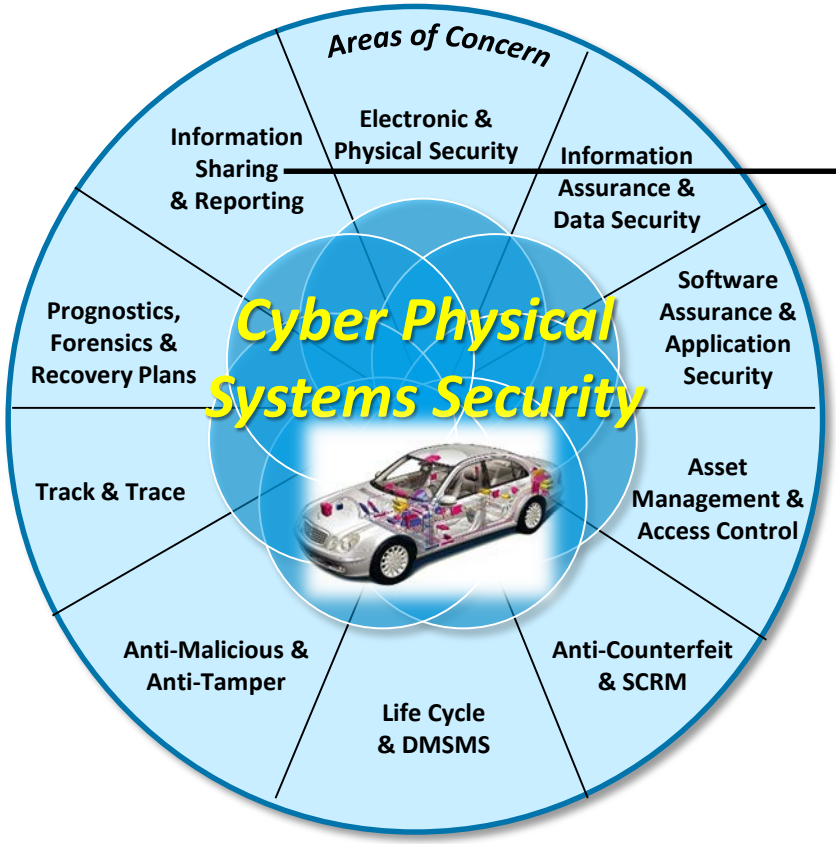


Rapidly Diagnose Security Issues, Design for Resiliency, and Rapidly Recover from Attacks

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

(DiMase et al., 2015)



Acquire Industry Bulletins, Report Lessons Learned, and Engage with Standards Organizations

SAE International

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM GIDEP

DEFENSE CYBER CRIME CENTER AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

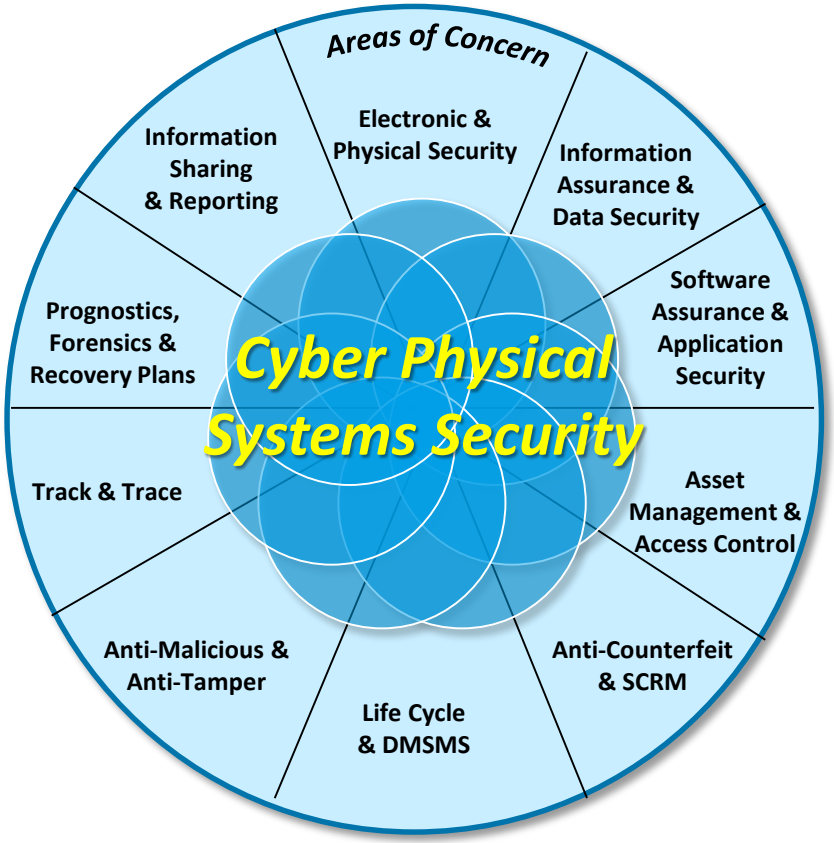
erai

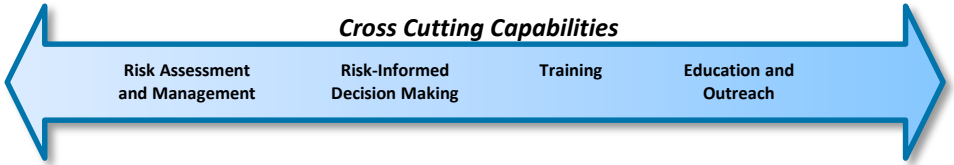
ESCO

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

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

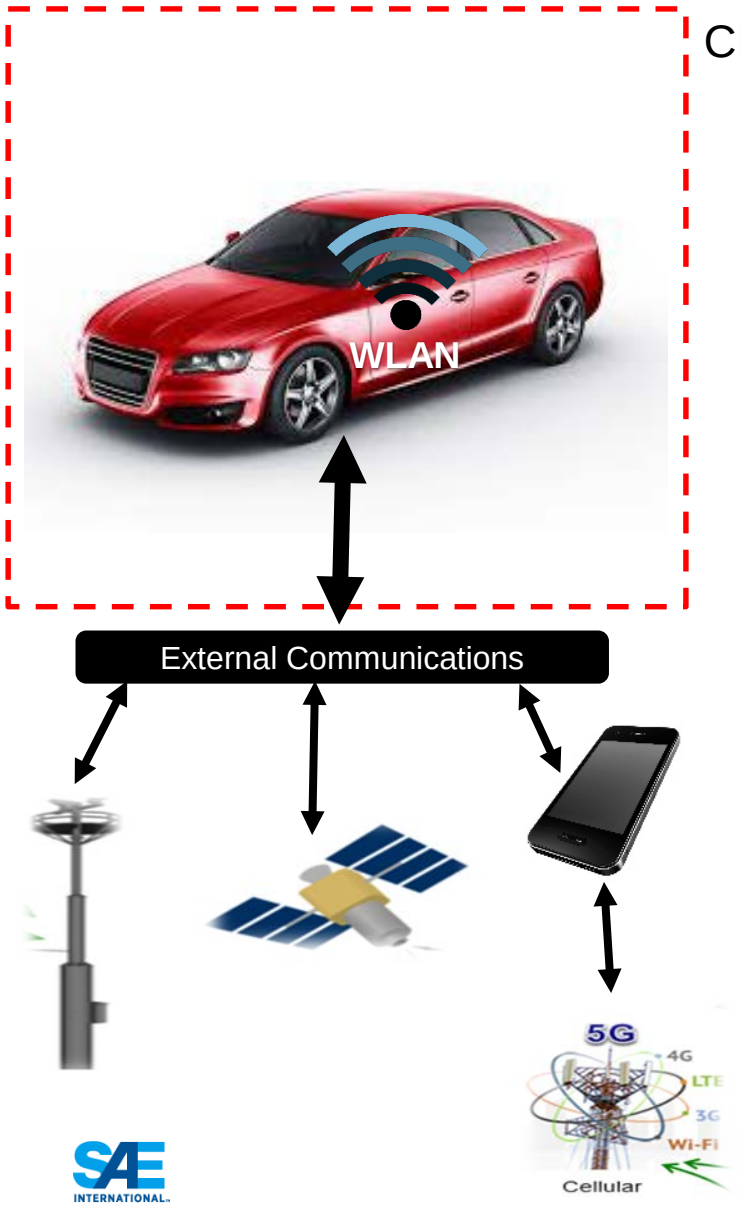
(DiMase et al., 2015)



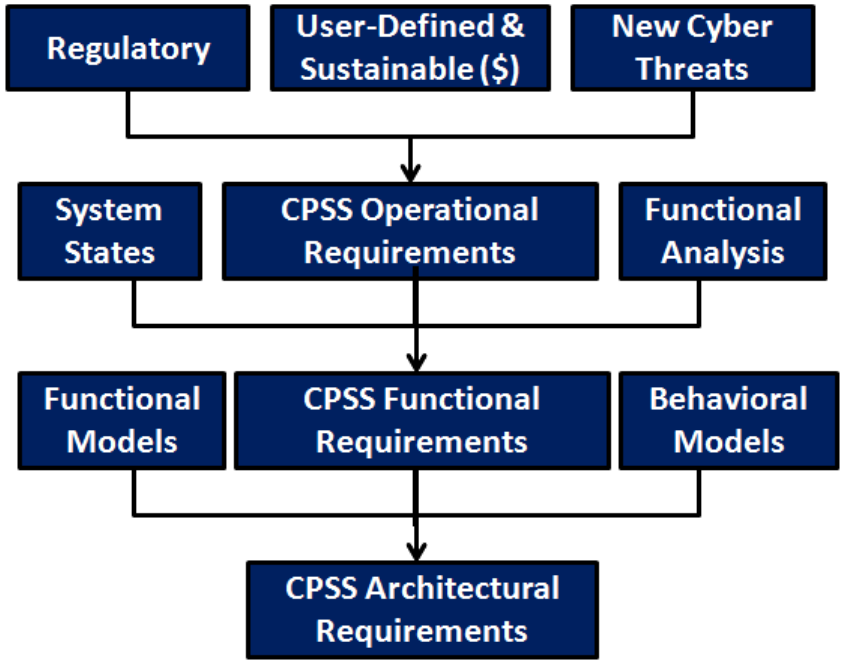


Introduces an Integrated Approach to the Problem that Includes Assemblies and Subsystems

CPSS SEP Notional Electronics Security Perimeter



CPSS Systems Engineering Requirements Flowdown



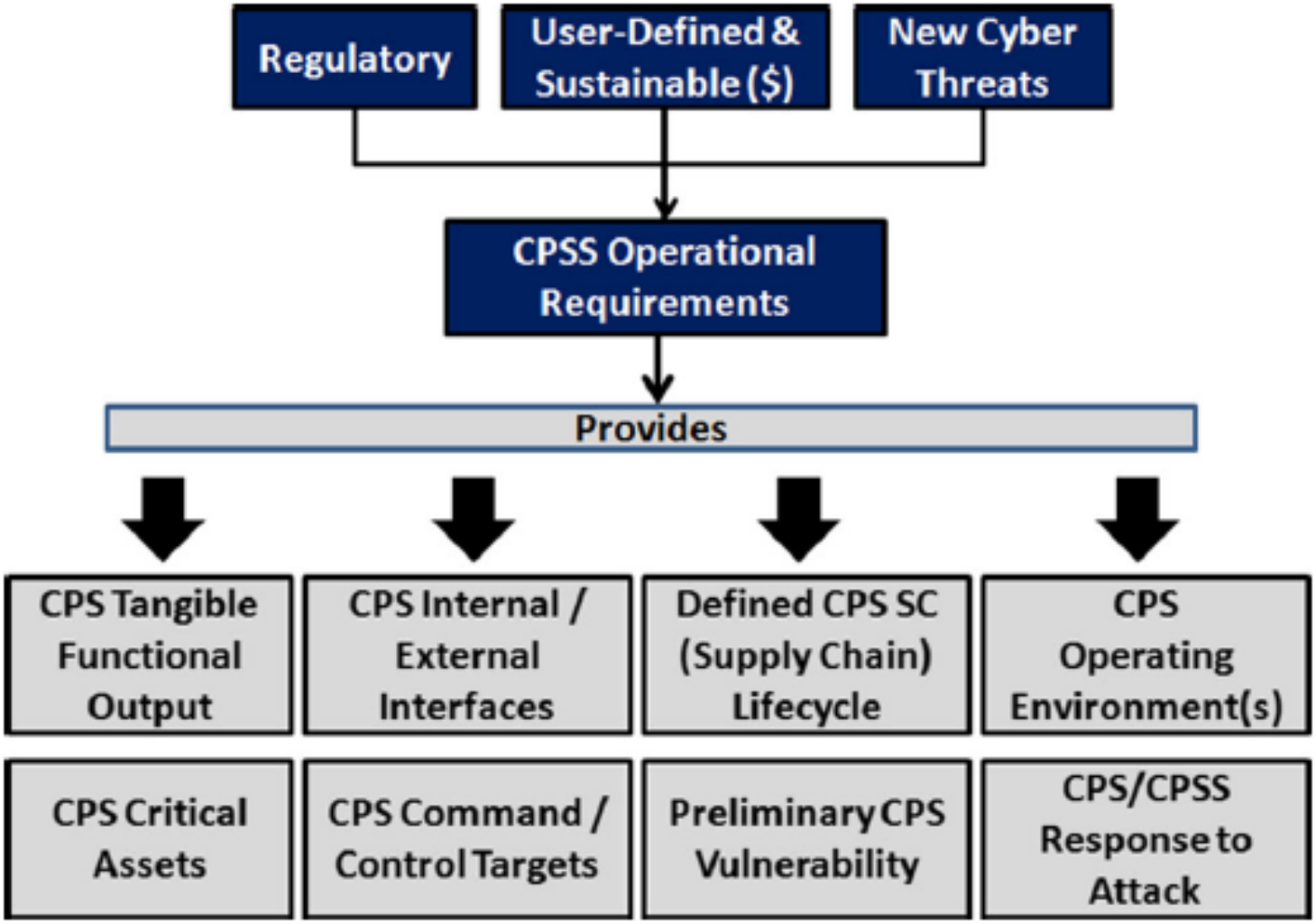
CPS Summary Assessment

CPS Systems Engineering Tiers	CRITICAL ASSETS AND COMMAND/CONTROL TARGETS					
	Weighting Factor	Critical Asset A	Critical Asset B	Critical Asset C	C&C Function A	C&C Function B
Operational Requirements	4	3	5	1	3	1
Functional Requirements	3	7	3	7	9	7
Architectural Requirements	5	1	7	3	5	7
Totals		11	15	11	17	15
Weighted Totals		38	64	40	64	60
Required Minimum Score		40	50	40	60	45

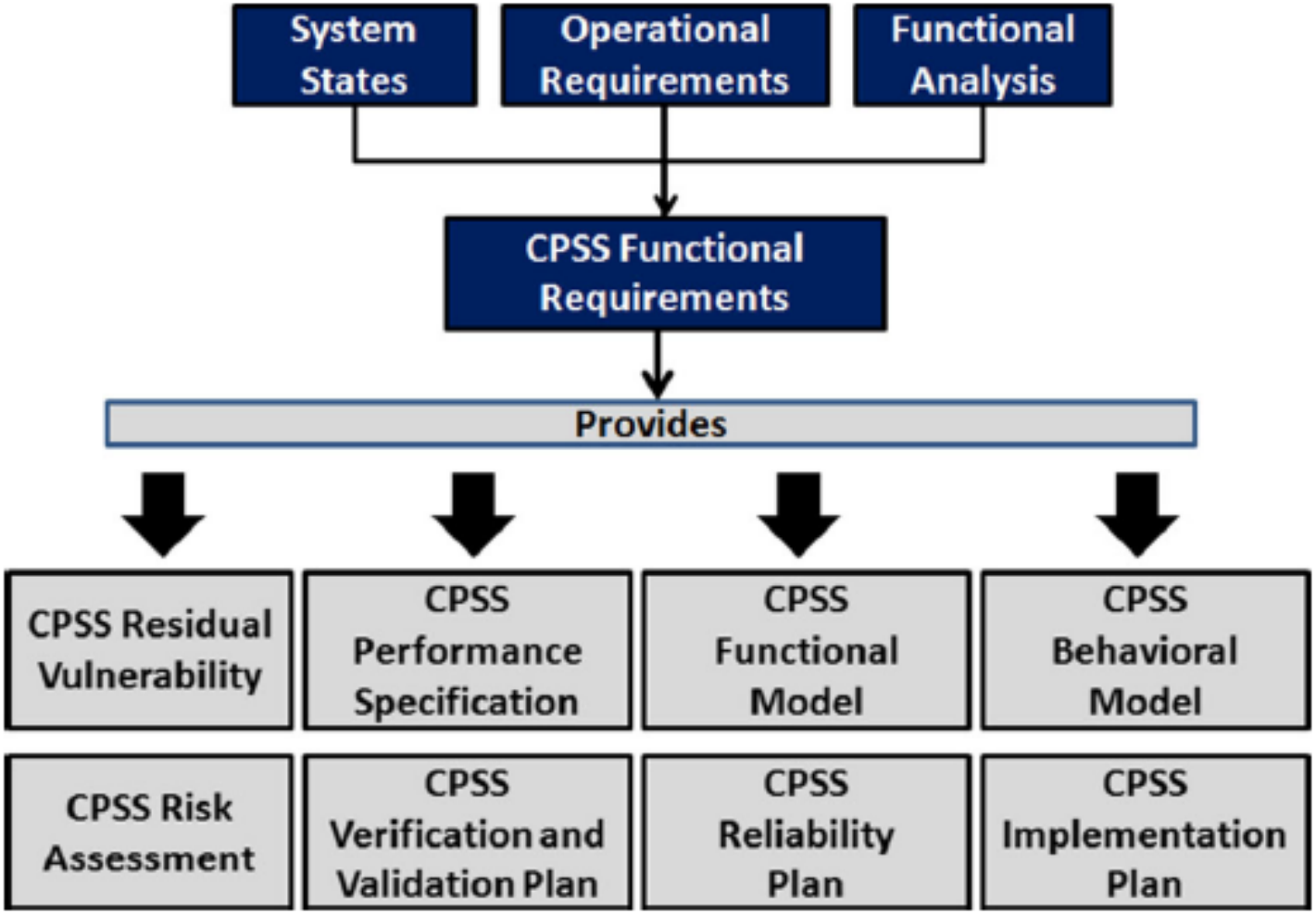
	Actual CPSS Score	Required Minimum CPSS Score
Total Score	266	235

(DiMase et al., 2015)

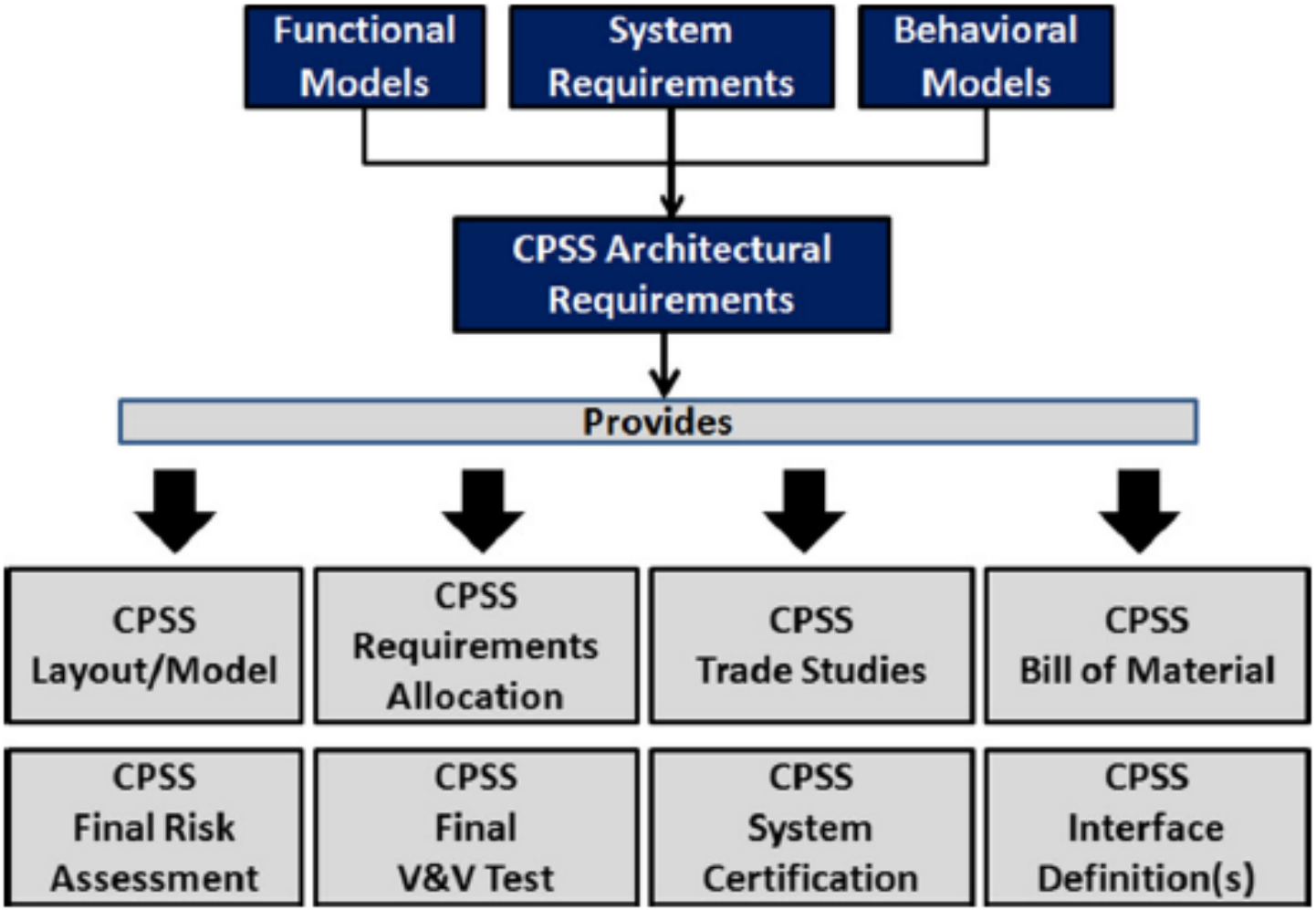
Operational Requirements



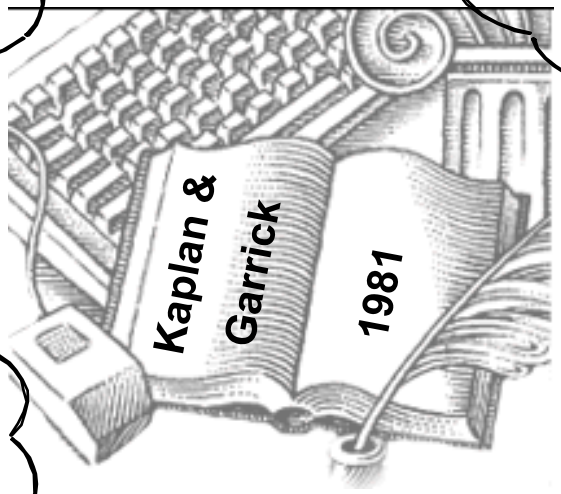
Functional Requirements



Architectural Requirements



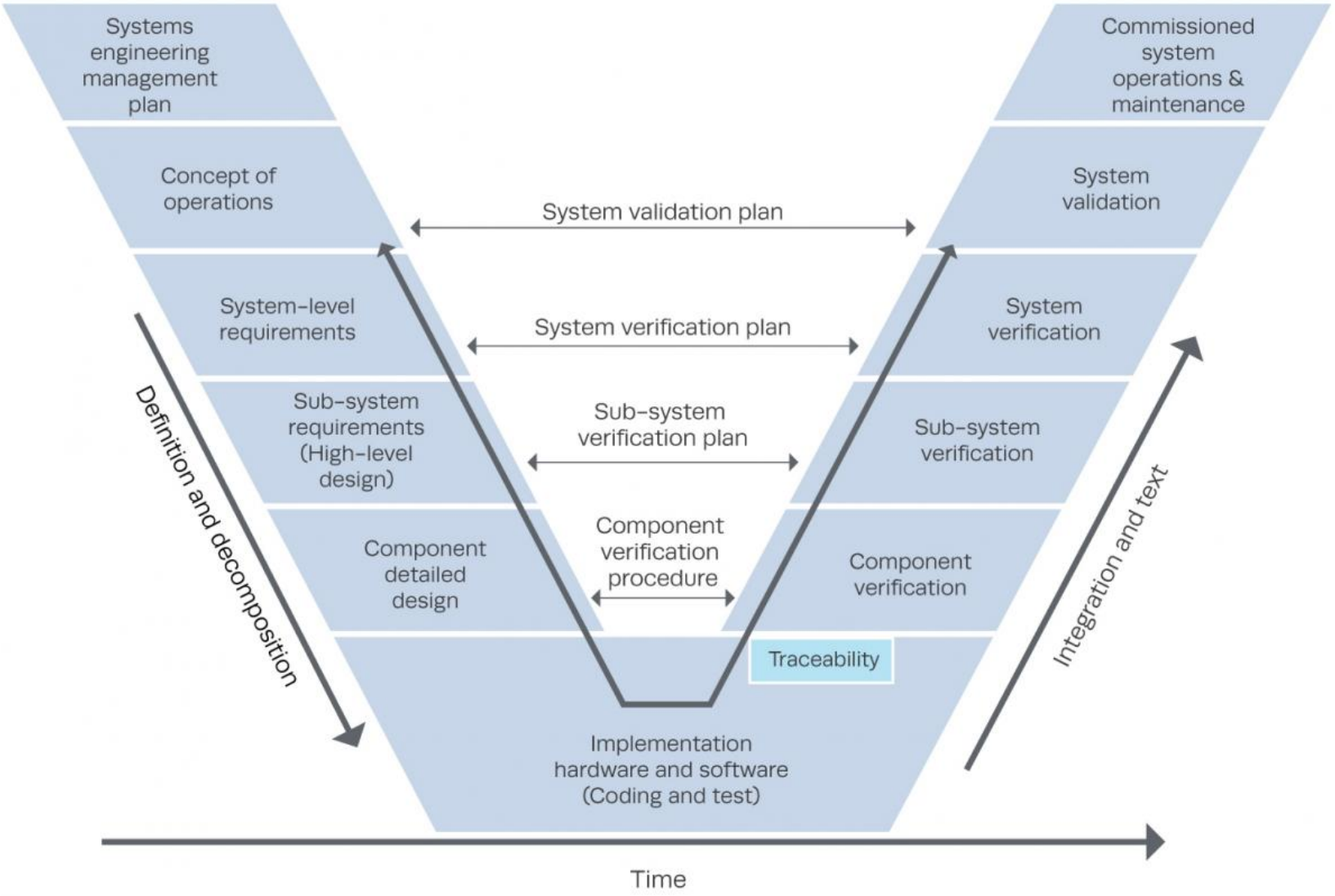
Systems Engineering Challenges: Risk Identification and Threat Modeling



Challenges:

- Adversaries are adaptive and intelligent, threat identification difficult
- Quantification of risk (likelihood of occurrence, severity of impact)
- High uncertainty and variability associated with predicting emerging threats, vulnerabilities, consequences
- Field is evolving fast and risk benchmarks do not exist (i.e.: How much risk is acceptable or too much?)
- Disconnect between risk assessment and risk management

Systems Engineering Challenges: Validation and Verification



https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/test-and-evaluation/verification-and-validation

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.
- Call for action for standard work to codify cyber physical systems security from a systems engineering perspective.

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

Future Work and Research Needs[7]

- 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 embedded malware and hardware Trojans
- 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.
- IT industry's use of penetration testing and code reviews should be adopted.
- Domain separation for in-system networks and safety critical systems.
- Implement a layered approach to security.
- Develop 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.

Summary

- **Awareness and Understanding of the Threat**
- **Impact and Consequences**
- **Terms, Definitions and Taxonomy**
- **Introduction to Cyber Physical Systems Security (CPSS)**
- **CPSS Challenges and Business Impact**
- **Industry Efforts**
  - SAE G-19A Tampered Subgroup
  - CPSS and the Systems Engineering Approach
- **Recommended Next Steps**
- **Future Work and Research Needs**

References

[1]Ponemon Institute (2013) 2013 Cost of data breach study: global anaylsis. Ponemon Institute, Traverse City.

[2]Perlroth N, Harris EA (2014) Cyberattack insurance a challenge for business. New York Times, Originally published 8 June 2014.

http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html

[3]Reed, John (2011) China May Have Hacked U.S. Satellites. D*efenceTech.Org,* Originally published 28 October 2011.

http://defensetech.org/2011/10/28/china-may-have-hacked-u-s-satellites/

[4]Langner, Ralph (2013) To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve.

http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[5]McAfee (2014) Net losses: estimating the global cost of cybercrime.

http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf

[6]DiMase, et. all (2015) Environment Systems and Decisions. Systems engineering framework for cyber physical security and resilience. Originally published 8 February 2015.

http://rd.springer.com/article/10.1007%2Fs10669-015-9540-y

References

[7]Collier, et. all (2015) Building a Trusted and Agile Supply Chain Network for Electronic Hardware. 20th International Command and Control Research and Technology Symposium.

[8]Privacy Rights Clearing House – Chronology of Data Breaches Security Breaches 2005 – Present

http://www.privacyrights.org/data-breach

[9]Joseph Menn, Reuters (2015) Russian researchers expose breakthrough U.S. spying program.

http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216

[10]Samy Kamkar – Keysweeper (Sigint // Samy.pl // Rel to All // Applied Hacking)

http://samy.pl/keysweeper/

[11]CBS News, 60 Minutes (2015) Car Hacked on 60 Minutes

http://www.cbsnews.com/news/car-hacked-on-60-minutes/

[12]Mike Snider, et al, USA TODAY (2015) Banking hack heist yields up to $1 billion

http://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913/

References

[13]Sara Peters, InformationWeek Dark Reading (2014) As Stuxnet Anniversary Approaches, New SCADA Attack is Discovered

http://www.darkreading.com/as-stuxnet-anniversary-approaches-new-scada-attack-is-discovered/d/d-id/1278881?_mc=RSS_DR_EDT&templatemsg=Your+email+was+sent%2E

[14]Georg T. Becker, et al (2014) Stealthy Dopant-Level Hardware Trojans

http://sharps.org/wp-content/uploads/BECKER-CHES.pdf

[15]Agence France Presse (2008) Worst cyber attack on US military came via flash drive: US

http://www.alternet.org/rss/breaking_news/271139/worst_cyber_attack_on_us_military_came_via_flash_drive%3A_us

[16]Sergei Skorobogatov, et al (2012) In the blink of an eye: There goes your AES key

http://eprint.iacr.org/2012/296.pdf

[17]NERC (2009) Cyber security—electronic security perimeter(s). NERC Standard CIP–005–3

[18]NIST. https://www.nist.gov/programs-projects/cyber-physical-systems-program

References

[19] "Cyber Security Dictionary". 2 Jan 2012. Retrieved 23 March 2014.

[20] Boys, Walt (18 August 2009). "Back to Basics: SCADA". Automation TV: Control Global - Control Design.

[21] https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/test-and-evaluation/verification-and-validation

[22] http://www.trustedfoundryprogram.org/