Cyber Security

Cyber Physical Systems

Systems Engineering Perspective

June 2014

Honeywell

Cyber Security Problem Statement

- **Attack vectors are applied to vulnerabilities in electronic parts[*] associated with tampering (as defined by the SAE organization). These threats in hardware assurance and security enables a broad range of attack vectors in cyber physical systems supporting the U.S. critical infrastructure and national security.**

- **In response to growing cyber threats, President Obama in 2013 signed Executive Order 13636 - *"Improving Critical Infrastructure Cybersecurity"*. It 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*

G-19A - AS6171 Draft - Definition of Tampered

- ***Tampered:*** A part which has been intentionally and maliciously modified from its intended design to enable a disruption in performance or an unauthorized function.
  - *Tampering can occur at any phase of a part's life cycle, which begins at design, continues through fabrication (manufacturing), all the way to its active usage in the field and disposition.*
  - *Parts that are tampered can have dangerous consequences for the systems that incorporate them. For example:*
    - *A tampered part can act as a time bomb where its functionality is unexpectedly "killed'' at a critical moment.*
    - *Tampered parts may also contain backdoors that give access to critical system functionality or leak secret information to an adversary.*
    - *Tampered parts may contain maliciously modified embedded firmware and software.*

Tampered Counterfeit Electronic Parts Includes Maliciously Altered Firmware or Software

DoD Cyber Security Regulatory Requirements

Final rule, 79 Fed. Reg. 26001 Detection and Avoidance of Counterfeit Electronic Parts; Effective May 6th, 2014.

Definition of electronic part:

"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."

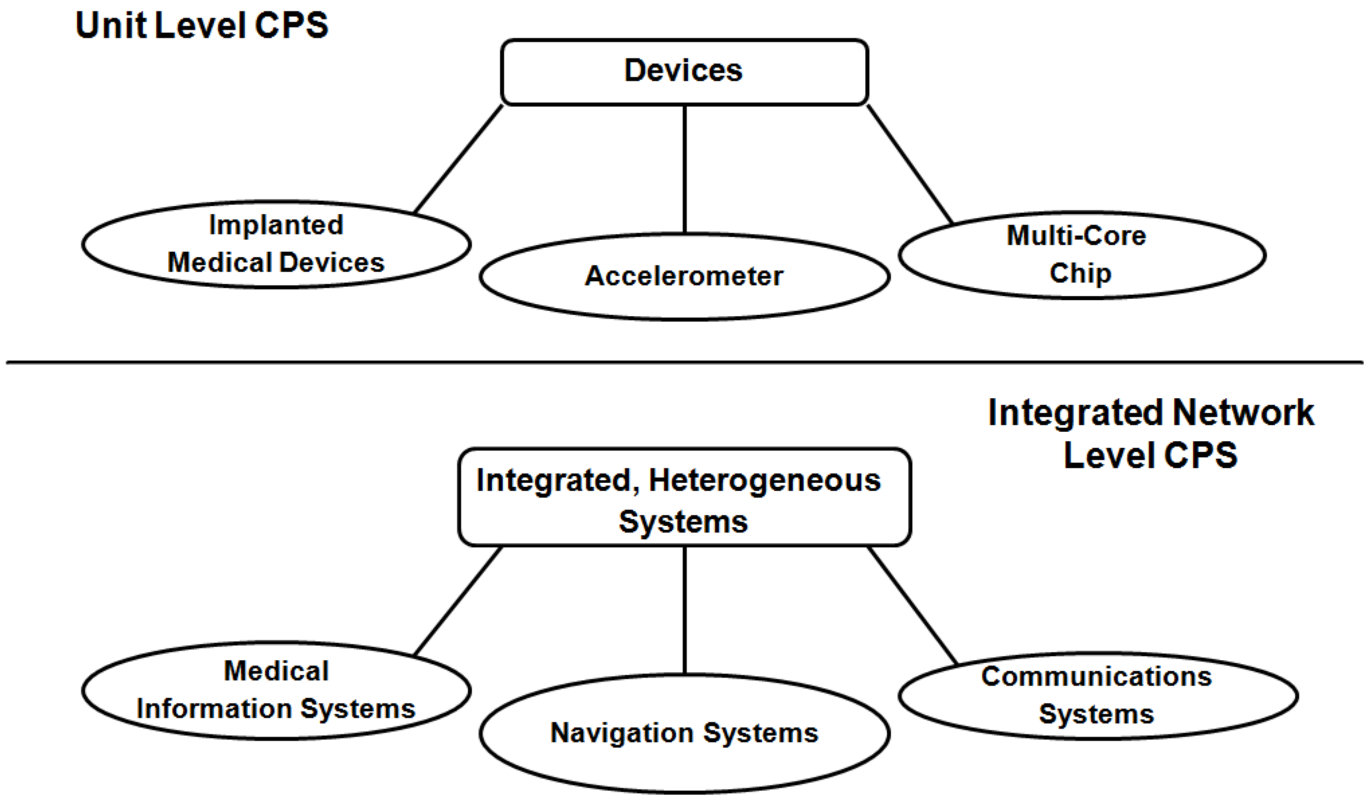
Final rule, 78 Fed. Reg. 69273 Safeguarding Unclassified Controlled Technical Information; Effective November 18th, 2013:

Requires implementing adequate security measures to safeguard unclassified controlled technical information within contractor information systems from unauthorized access and disclosure, and to report cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems.

The Definition Implies Cyber Physical Systems Security Concerns

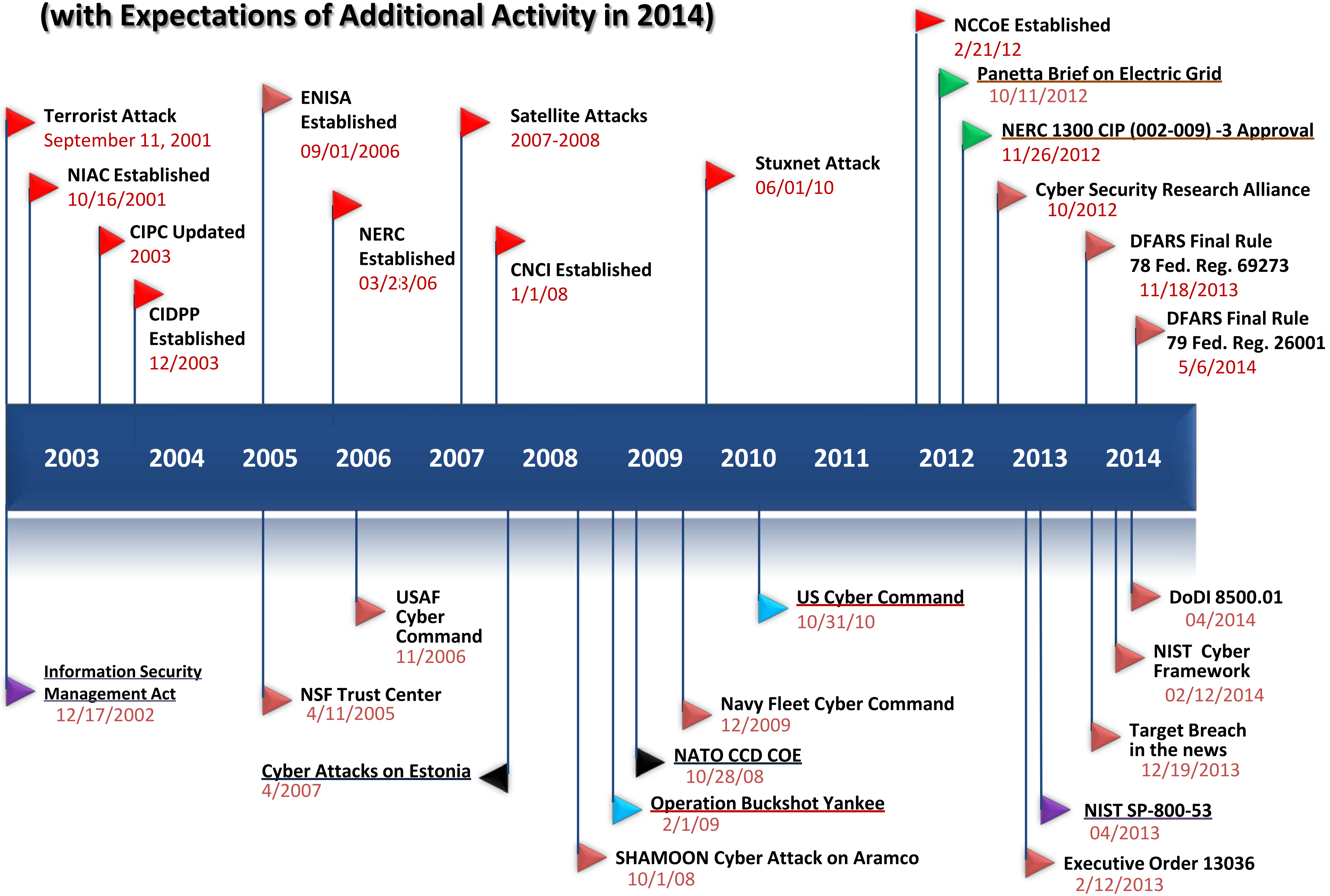
Cyber Physical Systems Definition

- ***Cyber Physical Systems (CPS) are electronics systems that operate as a single, self-contained device or within an interconnected network providing shared operations. An added distinction of this CPS definition is a requirement for affecting a tangible output through command and control electronics embedded in the device or distributed across network nodes.***


Unit Level CPS
Devices
Implanted Medical Devices
Accelerometer
Multi-Core Chip
Integrated Network Level CPS
Integrated, Heterogeneous Systems
Medical Information Systems
Navigation Systems
Communications Systems

Multiple Calls to Action for Cyber Physical Systems

A Partial Listing of Major Cyber Physical Systems Related Milestones (with Expectations of Additional Activity in 2014)



Terrorist Attack
September 11, 2001

NIAC Established
10/16/2001

CIPC Updated
2003

CIDPP Established
12/2003

ENISA Established
09/01/2006

NERC Established
03/28/06

Satellite Attacks
2007-2008

CNCI Established
1/1/08

Stuxnet Attack
06/01/10

NCCoE Established
2/21/12

Panetta Brief on Electric Grid
10/11/2012

NERC 1300 CIP (002-009) -3 Approval
11/26/2012

Cyber Security Research Alliance
10/2012

DFARS Final Rule
78 Fed. Reg. 69273
11/18/2013

DFARS Final Rule
79 Fed. Reg. 26001
5/6/2014

2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

Information Security Management Act
12/17/2002

NSF Trust Center
4/11/2005

USAF Cyber Command
11/2006

Cyber Attacks on Estonia
4/2007

SHAMOON Cyber Attack on Aramco
10/1/08

Operation Buckshot Yankee
2/1/09

NATO CCD COE
10/28/08

Navy Fleet Cyber Command
12/2009

US Cyber Command
10/31/10

Executive Order 13036
2/12/2013

NIST SP-800-53
04/2013

Target Breach in the news
12/19/2013

NIST Cyber Framework
02/12/2014

DoDI 8500.01
04/2014

Industry data breaches/cyber attacks increased this year to date by 18.3% from 614 reported 2013 breaches exposing 91,982,172 records.

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

Business Case – Cost of Security

Cost/impact of security breaches:

- **Average cost of data theft in 2012 was $188 per customer account* (i.e. exposed record).**
- **Average cost per security breach in 2012 totaling over $5.4 million*.**
- **Analysts are forecasting $1 billion in losses for the Target breach. Since the breach was discovered, the company has incurred $88 million in breach-related expenses, its filings say.****

*Ponemon Institute, 2013

**New York Times, June 8, 2014

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 CPS-S
- 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

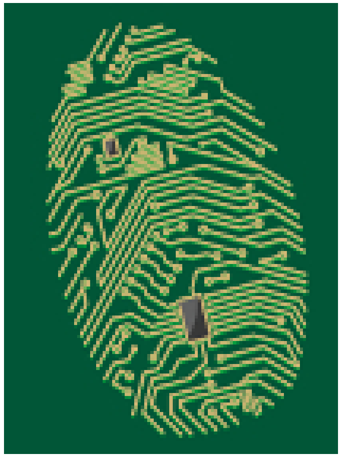
Problem Definition and Approach

- Cyber Physical Security is a complex topic with a number of areas of concern that need to be addressed to ensure robust, 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.

Industry and Government Needs

Honeywell

- Systems based view that interweaves the various areas of concern that need to be addressed
- Identify weaknesses and gaps in policy, services, and high-fidelity technology roadmaps to help govern future policy and allocate research resources
- Framework that is robust based on the knowledge we know today, yet resilient enough to address the persistent, dynamic threat
- Incorporates the strictly technological perspective with *social and decision making aspects* in the construct



Cyber Physical Security

Electronic Piece Parts

Industry Efforts to Address Concerns

- For the first release of AS6171, SAE G-19A is proposing 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 Efforts will be Limited to Electronics Piece Parts.

Tampered Subgroup will not Address Assemblies and Subsystems.

Cyber Physical Security

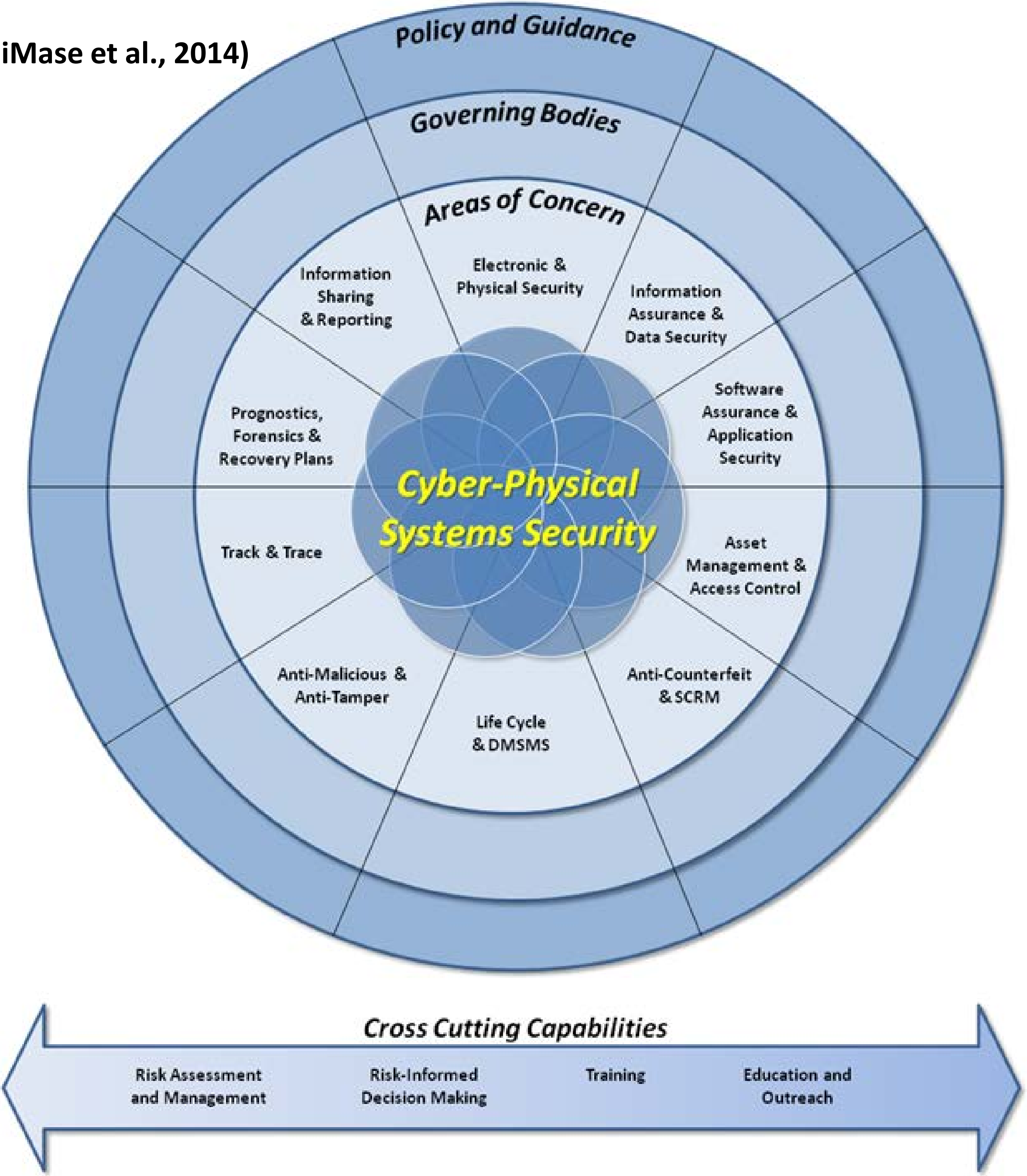
Honeywell

Assemblies & Subsystems

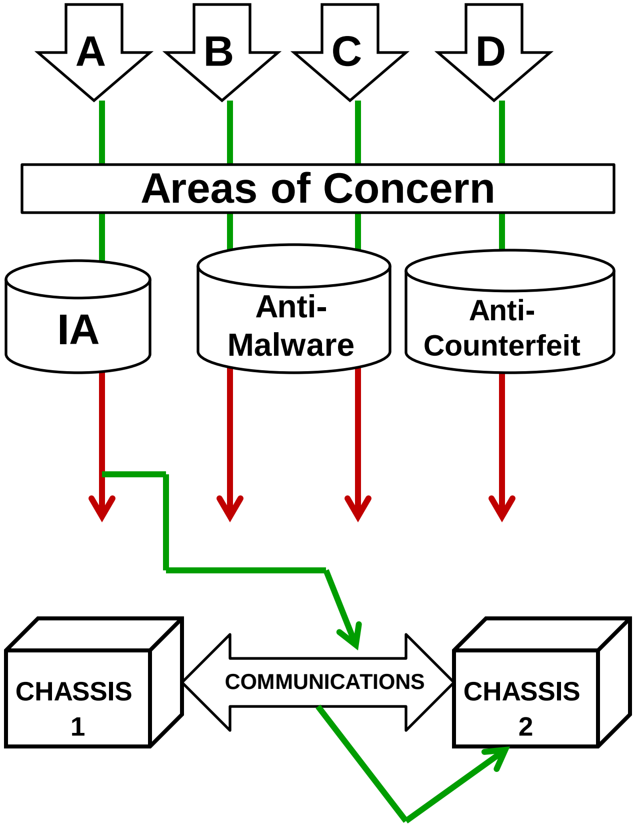
Systems Engineering Perspective (SEP) for CPS-Security

Honeywell

(DiMase et al., 2014)


Policy and Guidance
Governing Bodies
Areas of Concern
Electronic & Physical Security
Information Assurance & Data Security
Software Assurance & Application Security
Asset Management & Access Control
Anti-Counterfeit & SCRM
Life Cycle & DMSMS
Anti-Malicious & Anti-Tamper
Track & Trace
Prognostics, Forensics & Recovery Plans
Information Sharing & Reporting
Cyber-Physical Systems Security
Cross Cutting Capabilities
Risk Assessment and Management
Risk-Informed Decision Making
Training
Education and Outreach

Hardware Attack Vectors

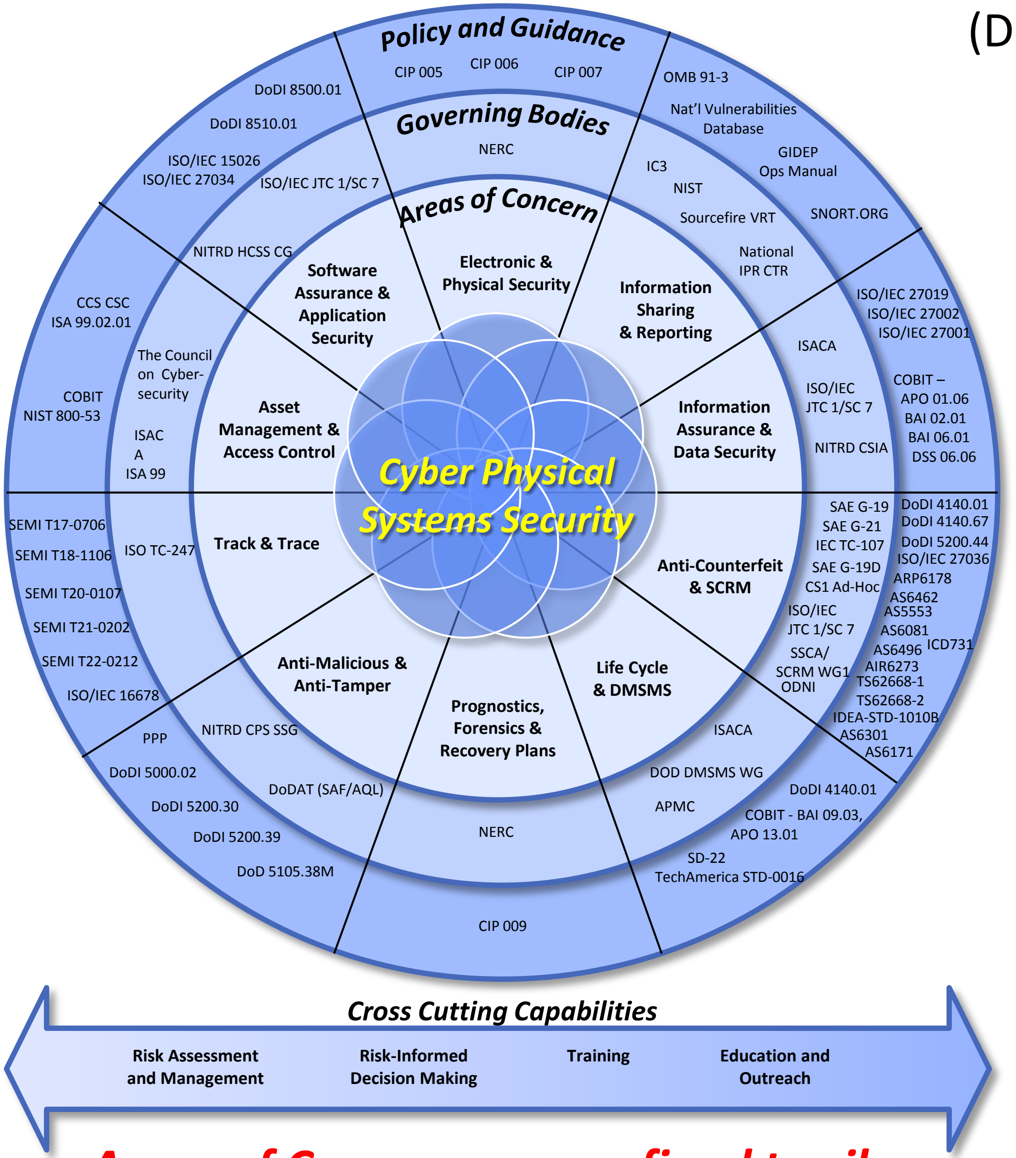


Communications Unit has vulnerabilities permitting penetration in Chassis 2.

Implementing Cyber Physical Systems Security
A Systems Engineering Perspective

Honeywell

(DiMase et al., 2014)



Policy and Guidance

Governing Bodies

Areas of Concern

Cyber Physical Systems Security

CIP 005 CIP 006 CIP 007

NERC

Electronic & Physical Security

OMB 91-3

Nat'l Vulnerabilities Database

GIDEP Ops Manual

SNORT.ORG

IC3

NIST

Sourcefire VRT

National IPR CTR

Information Sharing & Reporting

ISO/IEC 27019
ISO/IEC 27002
ISO/IEC 27001

COBIT –
APO 01.06
BAI 02.01
BAI 06.01
DSS 06.06

ISACA

ISO/IEC JTC 1/SC 7

NITRD CSIA

Information Assurance & Data Security

DoDI 4140.01
DoDI 4140.67
DoDI 5200.44
ISO/IEC 27036
ARP6178
AS6462
AS5553
AS6081
AS6496
ICD731
AIR6273
TS62668-1
TS62668-2
IDEA-STD-1010B
AS6301
AS6171

SAE G-19
SAE G-21
IEC TC-107
SAE G-19D
CS1 Ad-Hoc
ISO/IEC
JTC 1/SC 7
SSCA/
SCRM WG1
ODNI

Anti-Counterfeit & SCRM

DoDI 4140.01

COBIT - BAI 09.03,
APO 13.01

SD-22
TechAmerica STD-0016

ISACA

DOD DMSMS WG

APMC

Life Cycle & DMSMS

CIP 009

NERC

Prognostics, Forensics & Recovery Plans

DoDI 5000.02
DoDI 5200.30
DoDI 5200.39
DoD 5105.38M

PPP

NITRD CPS SSG

DoDAT (SAF/AQL)

Anti-Malicious & Anti-Tamper

SEMI T17-0706
SEMI T18-1106
SEMI T20-0107
SEMI T21-0202
SEMI T22-0212
ISO/IEC 16678

ISO TC-247

Track & Trace

CCS CSC
ISA 99.02.01

COBIT
NIST 800-53

The Council on Cyber-security

ISAC
A
ISA 99

Asset Management & Access Control

DoDI 8500.01
DoDI 8510.01
ISO/IEC 15026
ISO/IEC 27034

ISO/IEC JTC 1/SC 7

NITRD HCSS CG

Software Assurance & Application Security

Cross Cutting Capabilities

Risk Assessment and Management

Risk-Informed Decision Making

Training

Education and Outreach

Areas of Concern are confined to silos.

There is Currently no Unified Approach that Interweaves All Areas of Concern.

Recommend forming new SAE committee to codify construct into industry standard work.

Challenges in Cyber Risk Assessment

Challenges:

- Difficulty in quantification of Threat, Vulnerability, Impact & Consequence
- High uncertainty and variability associated with predicting emerging threats
- Disconnect between risk assessment and risk management
- Dynamic application of threats and attack strategy

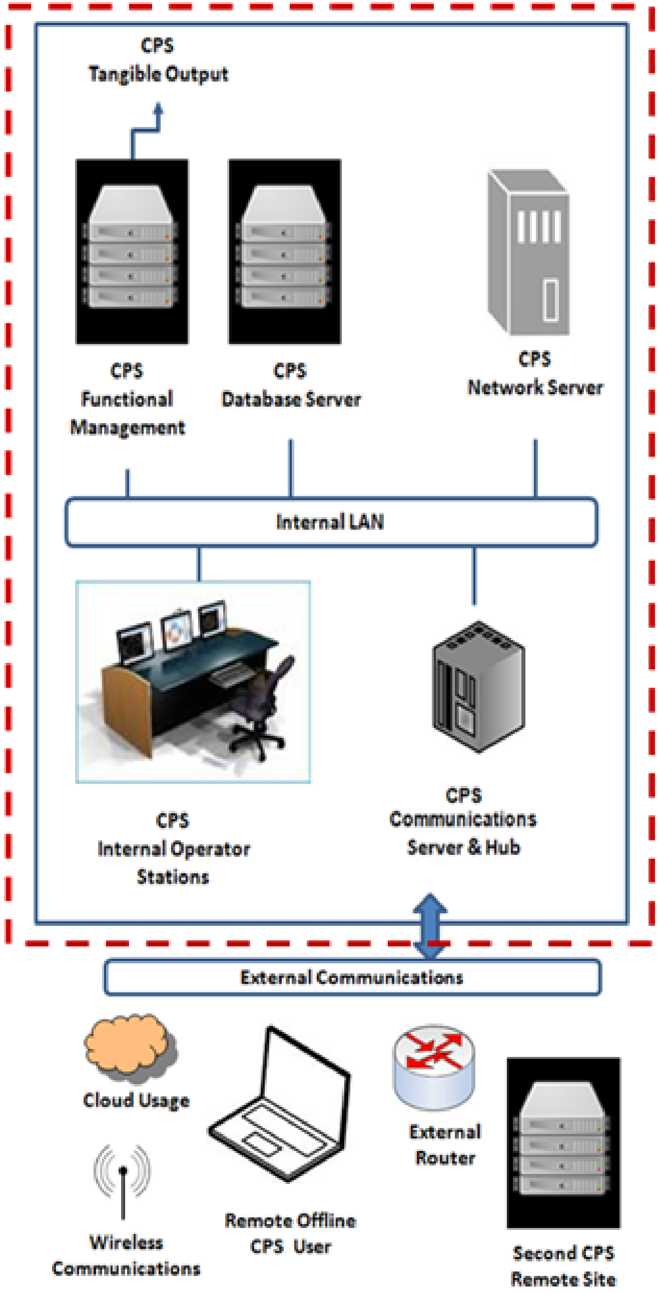
Perspective for improvement:

- Semi-quantitative approach
- Evolve the guidance on actionable mitigation efforts
- Physical information and preferences/value for judgment by stakeholders
- Drive collaboration between areas of concern through integration of the Cyber Physical Security framework

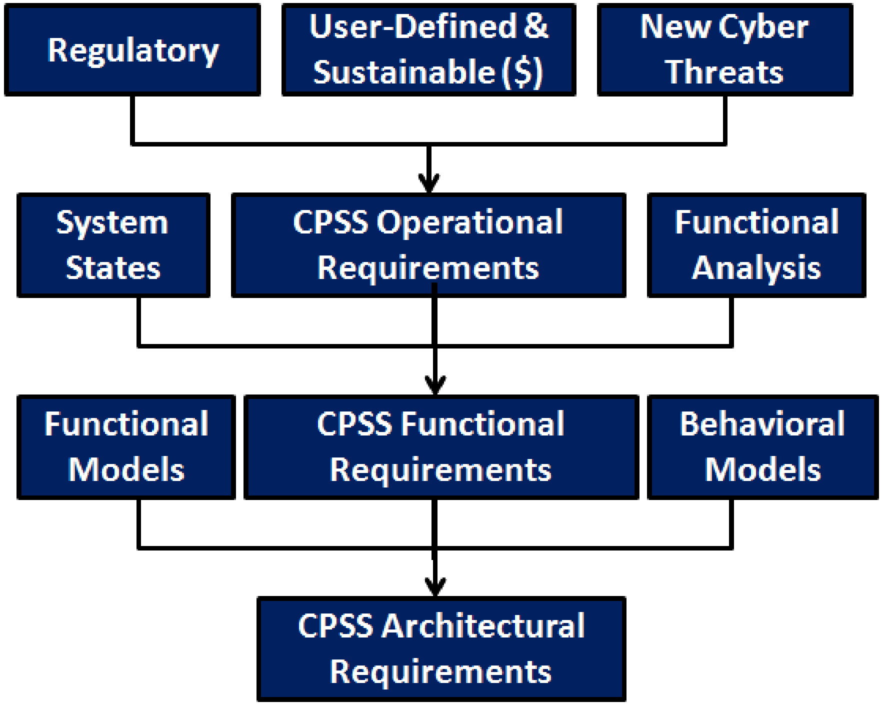
Systems Engineering Perspective [SEP] - SE

- The defense of an integrated, network-level CPS is a very large undertaking that is encumbered by the extensive threat environment.
- Today's solutions are *ad hoc* at best leaving gaps in the network.
- The SEP proposes a path through a formal systems engineering process.
  - Organizational Requirements
  - Functional Requirements
  - Architectural Requirements
- There is the need for measures of effectiveness for the SEP – based CPS-security design.

CPSS SEP Notional Electronics Security Perimeter



CPSS Systems Engineering Requirements Flowdown


Regulatory
User-Defined & Sustainable ($)
New Cyber Threats
System States
CPSS Operational Requirements
Functional Analysis
Functional Models
CPSS Functional Requirements
Behavioral Models
CPSS Architectural Requirements

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., 2014)

Discussion Points

- The systems engineering perspective (SEP) provides the concept of how to integrate and evaluate multiple areas of concern for Cyber Physical Security.

- The SEP serves as the framework for applying vulnerability analysis and resolutions to those ad-hoc attacks that find gaps in the traditionally stove-piped areas of concern.

- As we overlay the attack vectors, defense mechanisms and technologies that counter the attacks, we can:
  - Create roadmaps that can assess the current state of the art
  - Identify the gaps that introduce vulnerabilities that will help prioritize our resources
  - Build the future integrated state needed to address the issue

Recommended Next Steps

- Support and expedite (if possible) G-19A efforts to develop cost effective test methods capable of detecting defects associated with tampered parts. SAE group could use additional engineering SMEs.
- Support and expedite (if possible) 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 the development of an industry standard to codify the cyber physical systems security, systems engineering perspective and provide support as needed.
- Further research that include steps to enable systems resilience, with actions commensurate with risk.
- Other ?

Summary

- **Semi-quantitative framework could be used to assess well-being of CPS Security with the help of a Systems Engineering Perspective (SEP).**
- **Lexicon of terms specific to Cyber Physical Security enables stakeholders to holistically assess the health status for all CPS areas of concern.**
- **The SEP could provide a roadmap to assess the current state of the art and identify the gaps that introduce vulnerabilities .**
- **The approach could assist in prioritizing resources in building resilient CPS- security designs.**