29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

# Emerging Education Challenges for Resilient Cyber Physical Systems

Tom McDermott (Stevens Institute of Technology)

www.incose.org/symp2019

# Agenda

- Background & Motivation
- CPS Security Taxonomy
- State of Security Education in Engineering
- Challenges and Recommendations

# Acknowledgement – SERC and Sponsors

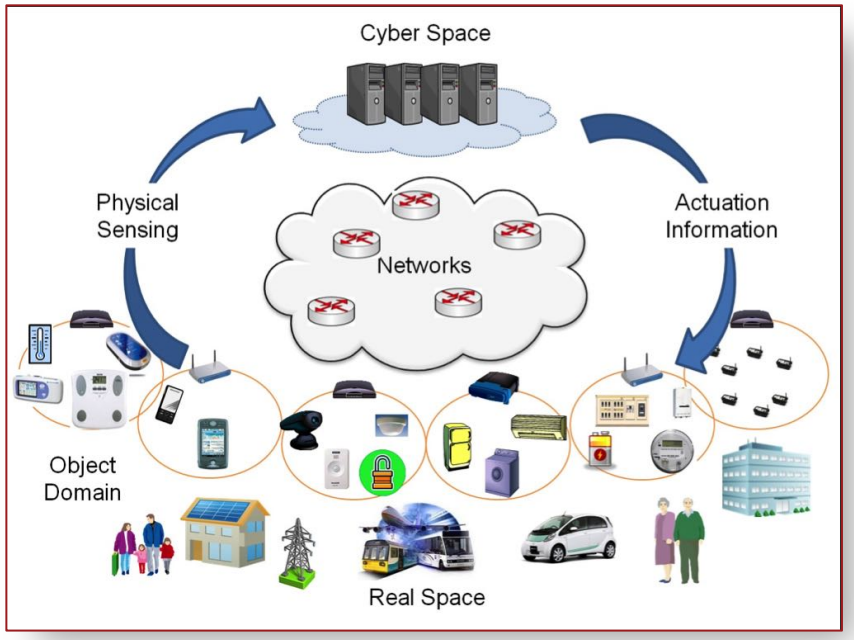


Thanks to:

- ***Melinda Reed and Mike McEvilley***
  - SecDef Research & Engineering
- ***Barry Horowitz, Peter Beling, Cody Fleming***
  - University of Virginia
- ***Val Sitterle, Molly Nadolski, Raheem Beyah***
  - Georgia Institute of Technology

# Background: Securing Physical Systems

- Standard cybersecurity approaches are infrastructural in nature
- There is little emphasis on protecting the applications within specific information systems:
  **Cyber-physical processes are apps**
- The cybersecurity community has limited experience in securing system application functions, especially physical system control functions
- And system application designers, in general, do not have experience with designing for better cybersecurity, especially physical system designers



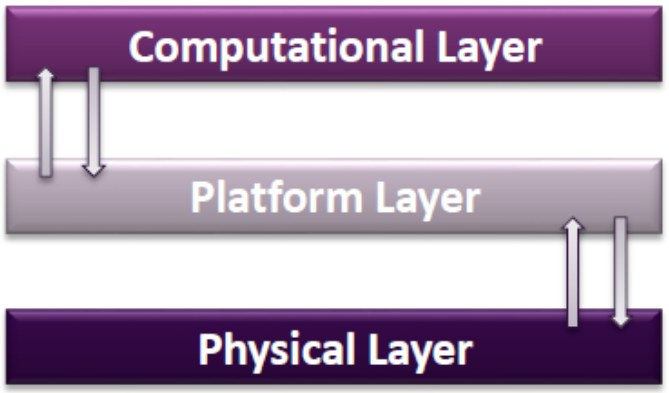
# Agenda

- Background & Motivation
- CPS Security Taxonomy
- State of Security Education in Engineering
- Challenges and Recommendations

# What are Cyber-Physical Systems?

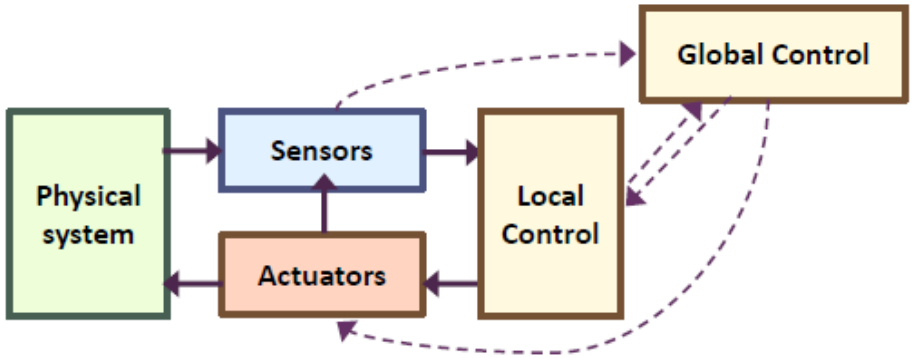
Engineered systems that…

Are comprised of heterogeneous sensing, computational, and actuating components to collect, process, and physically act on information



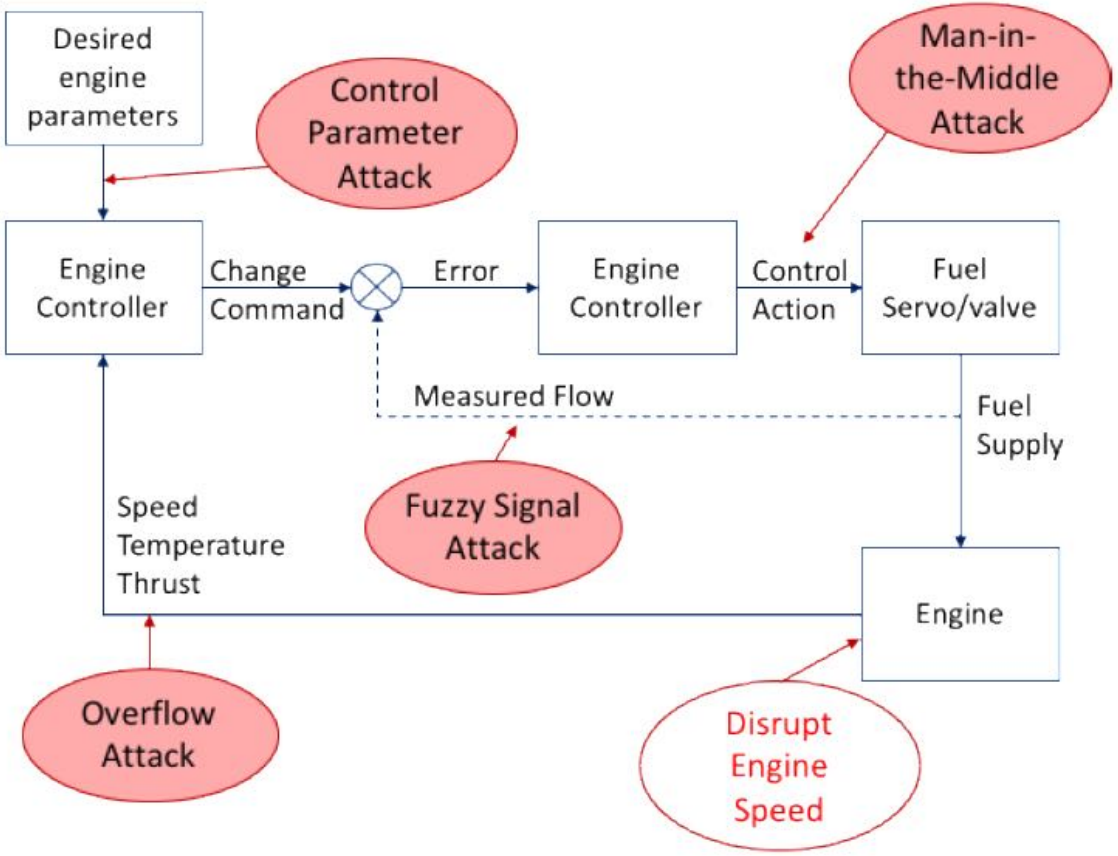

SW models, platform models, physical models

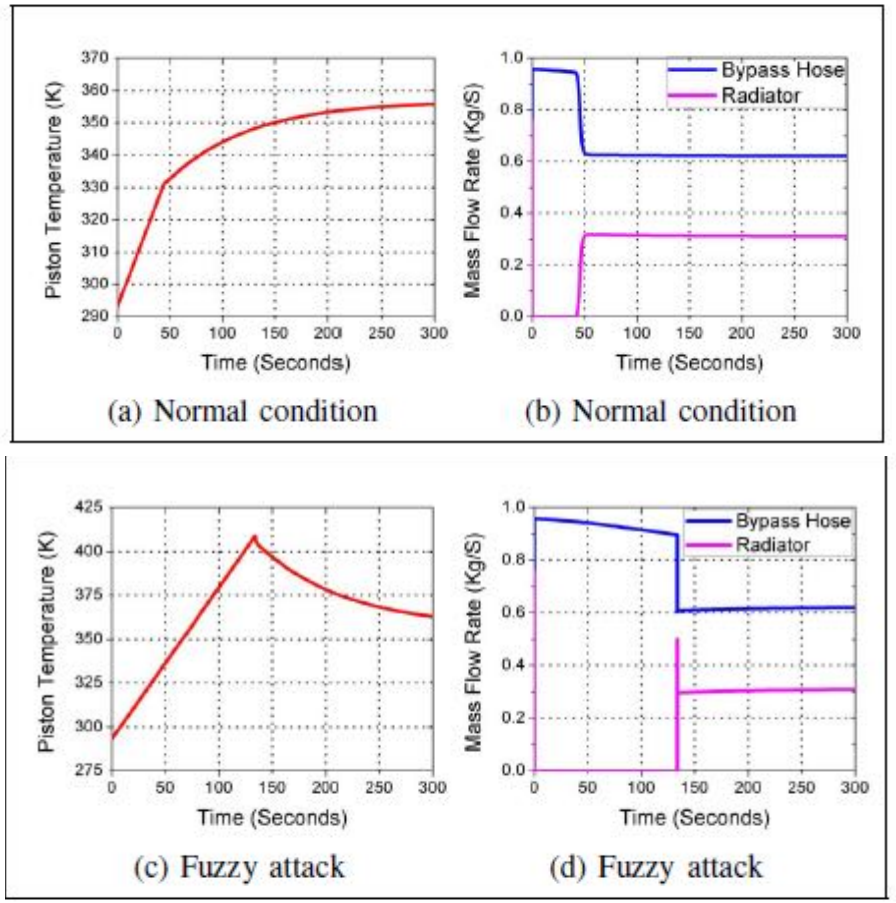
Integrate physical and cyber components where ***relevant functions are realized through interactions*** between the physical and cyber parts




Integration is key to system behavioral abstraction

# Example CPS Threat Pattern



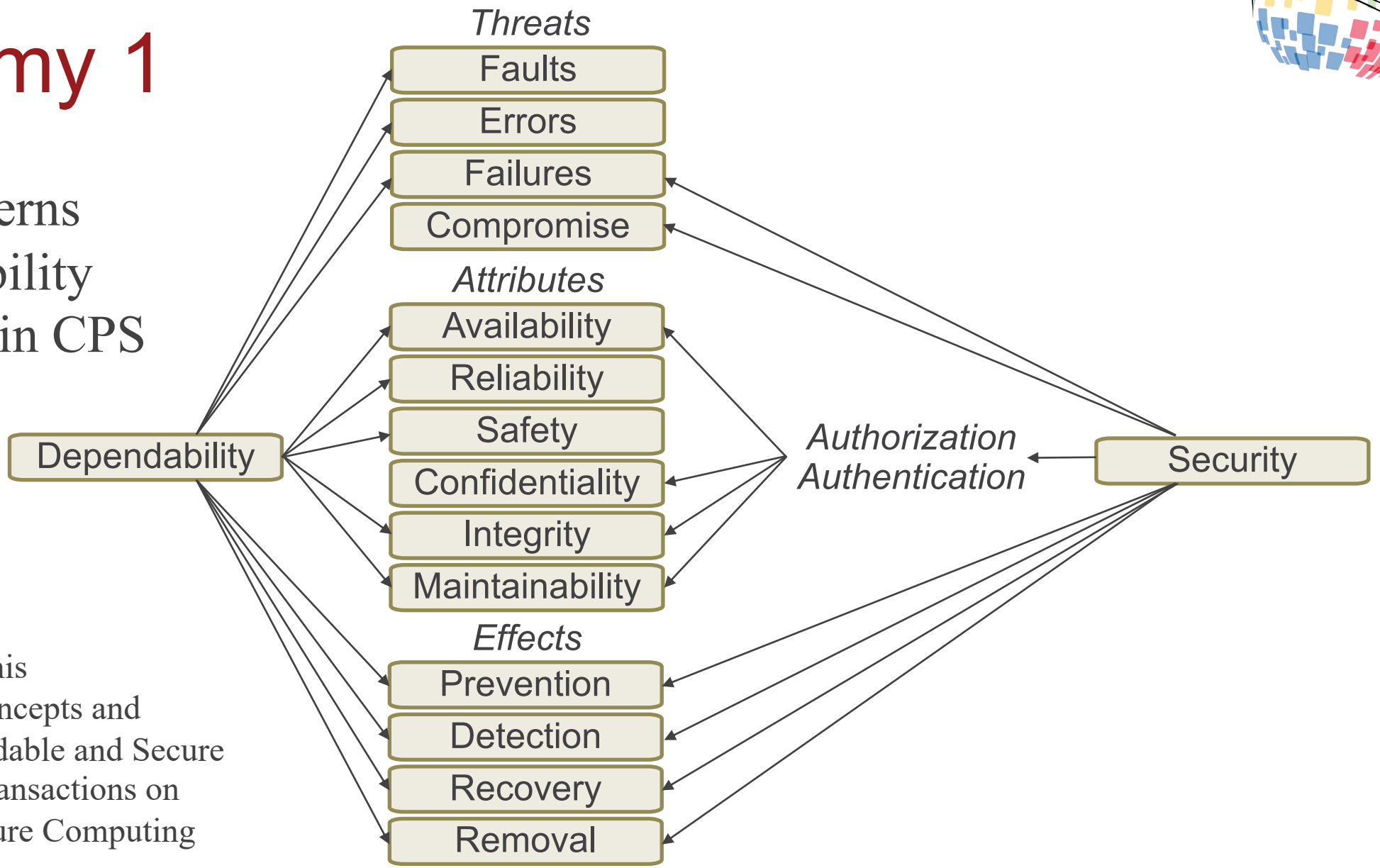




Rashid, Wan, Quiros,Canedo, Al Faruque; Modeling and Simulation of Cyberattacks for Resilient Cyber-Physical Systems

The key is to create “safe” designs, not respond to known threats.

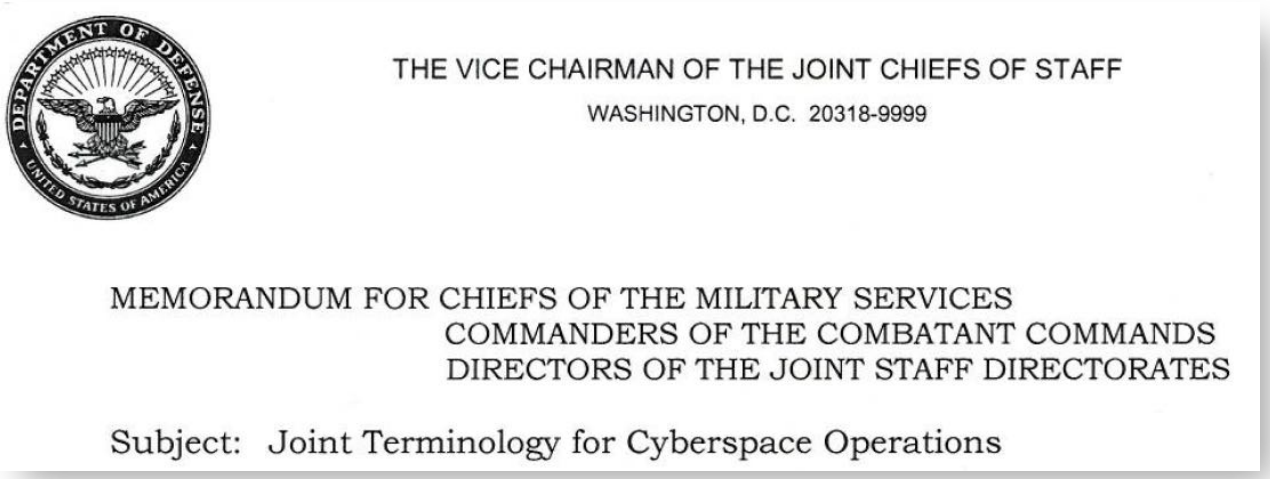
# Taxonomy 1

Related concerns for Dependability and Security in CPS




adapted from Avižienis et al, 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing

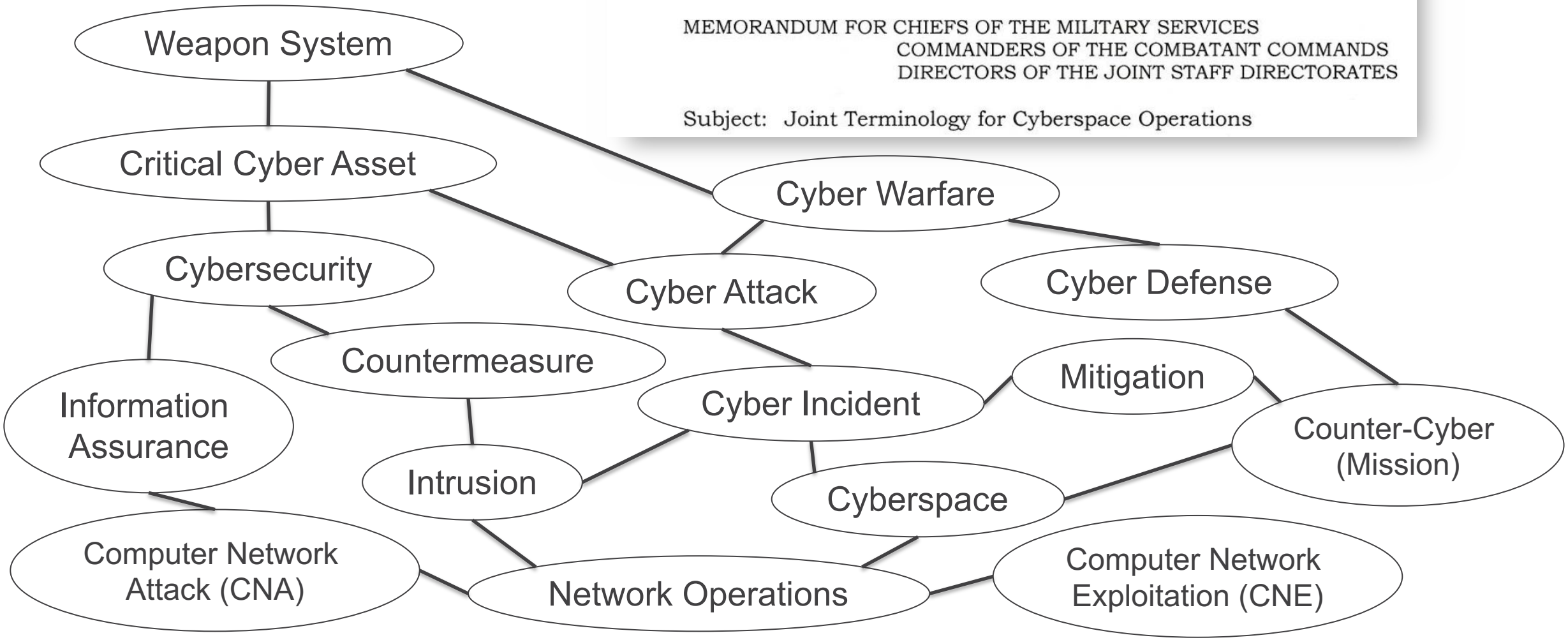
# Taxonomy 2



THE VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-9999

MEMORANDUM FOR CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTORS OF THE JOINT STAFF DIRECTORATES

Subject: Joint Terminology for Cyberspace Operations



# A CPS Systems Engineer must master:

- Concepts of secure access control to and use of the system and system resources (domain of system security engineering)
- Understanding of design attributes that minimize exposure of vulnerabilities to external threats (systems security engineering and dependable computing)
- Understanding of design patterns to produce effects that protect and preserve system functions or resources (dependable computing)
- Approaches to monitor, detect and respond to threats and security anomalies (cybersecurity)
- Understanding of network operations and external security services (information systems)
- Approaches to maintain system availability under adverse conditions (all of the above)

# Agenda

- Background & Motivation
- CPS Security Taxonomy
- State of Security Education in Engineering
- Challenges and Recommendations

# National Academies recommendations on CPS education

| CPS principles | CPS foundations | CPS characteristics |
|---|---|---|
| Communication and Networking | Basic computing concepts, including software engineering | **Security and privacy** |
| Real time systems | Physical world computing, including sensors, actuators, and real-time control | Interoperability |
| Embedded systems, both hardware and software | Discrete and continuous mathematics | Discrete and continuous mathematics |
| Physical world computing, including safety, reliability, security, performance, and risk management | Cross-cutting application of sensing, actuation, control, communication, and computing | **Reliability and dependability** |
| **Human interaction with CPS, including ease of use** | Modeling of heterogeneous and dynamic systems integrating control, computing, and communication | Power and energy management |
| | **CPS system development (emphasizing concepts of resilience and safety, test and verification)** | Stability and performance |
| | | Human factors and usability |
| | | Safety |

# Knowledge Areas and Competencies (ACM & SEI)

Table 2. Computer Engineering Knowledge Areas and Bodies of Knowledge.

| Knowledge Areas | Resilient CPS Selected Bodies of Knowledge |
|---|---|
| CE-CAO Computer Architecture and Organization | Instruction set architecture; Measuring performance; Computer arithmetic; Processor organization; Memory system organization and architectures; Input/Output interfacing and communication; Peripheral subsyste system architectures |
| CE-ESY Embedded Systems | Characteristics of embedded systems; Ba tions; Parallel input and output; Asynchr Periodic interrupts, waveform generation sensors, actuators; Implementation strate for low-power operation; Mobile and net put/output topics; Computing platforms f |
| CE-NWK Computer Networks | Network architecture; Local and wide ar Network protocols; Network application Performance evaluation; Wireless sensor |
| CE-SEC Information Security | Data security and integrity; Vulnerabiliti Secret and public key cryptography; Mes security; Authentication; Trusted comput |
| CE-SPE Systems and Project Engineering | Project management principles; Human- and fault tolerance; Hardware and softwa tation; System specifications; System arc hardware and software design; System int sustainability, manufacturability |
| [illegible] Re- | Managing system reso [illegible] |

Table 3 (cont.). Computer Science Knowledge Areas and Bodies of Knowledge.

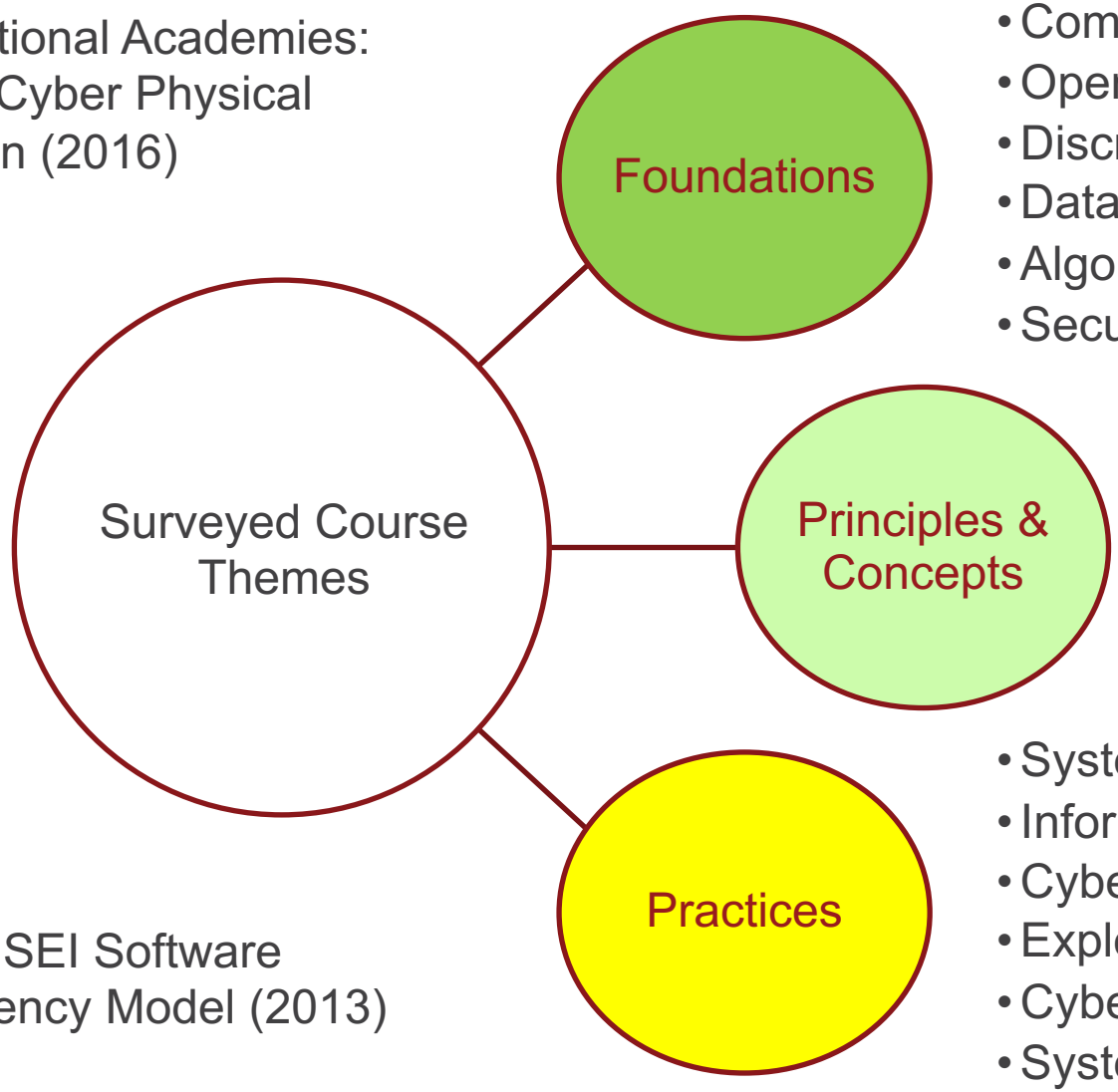
| Knowledge Areas | Resilient CPS Selected Bodies of Knowledge |
|---|---|
| GV - Graphics and Visualization | Fundamental Concepts |
| HCI - Human-Computer Interaction | HCI Foundations; Desig |
| IAS - Information Assurance and Security | Foundational Concepts; Threats and Attacks; Net Security; Security Policy |
| IM - Information Management | IM Concepts; Database I |
| IS - Intelligent Systems | IS Fundamentals; Basic soning; Basic Machine L |
| NC - Networking and Communications | NC Introduction; Netwo Forwarding; Local Area working |
| OS - Operating Systems | Introduction; OS Princip Management; Security a and Embedded Systems; |
| [illegible] based Devel- | Mobile Plat |

Table 4. Entry Level Competencies for a Career Dealing with Assurance.

| Competency | Description |
|---|---|
| System/software lifecycle processes | Able to manage the application of a defined lifecycle software process for a small project |
| Software Assurance Processes | Able to apply methods, processes, and tools to asses assurance |
| Risk Management Concepts | Understanding of risk analysis and risk management, including threat modeling |
| Risk Management Processes | Able to identify and describe risks in a project; able to analyze likelihood and severity; understanding of risks; understanding of risks in the acquisition of contracted software; employment of mitigation tasks |
| Assurance Assessment Concepts | Basic understanding of assurance assessment methods |
| Measurement for Assessing Assurance | Able to apply tools and documentation support for assessment processes |
| Business Case for Assurance | Able to apply a business case tradeoff a |
| [illegible] | Understandi |

# Derived CPS Security Education Themes

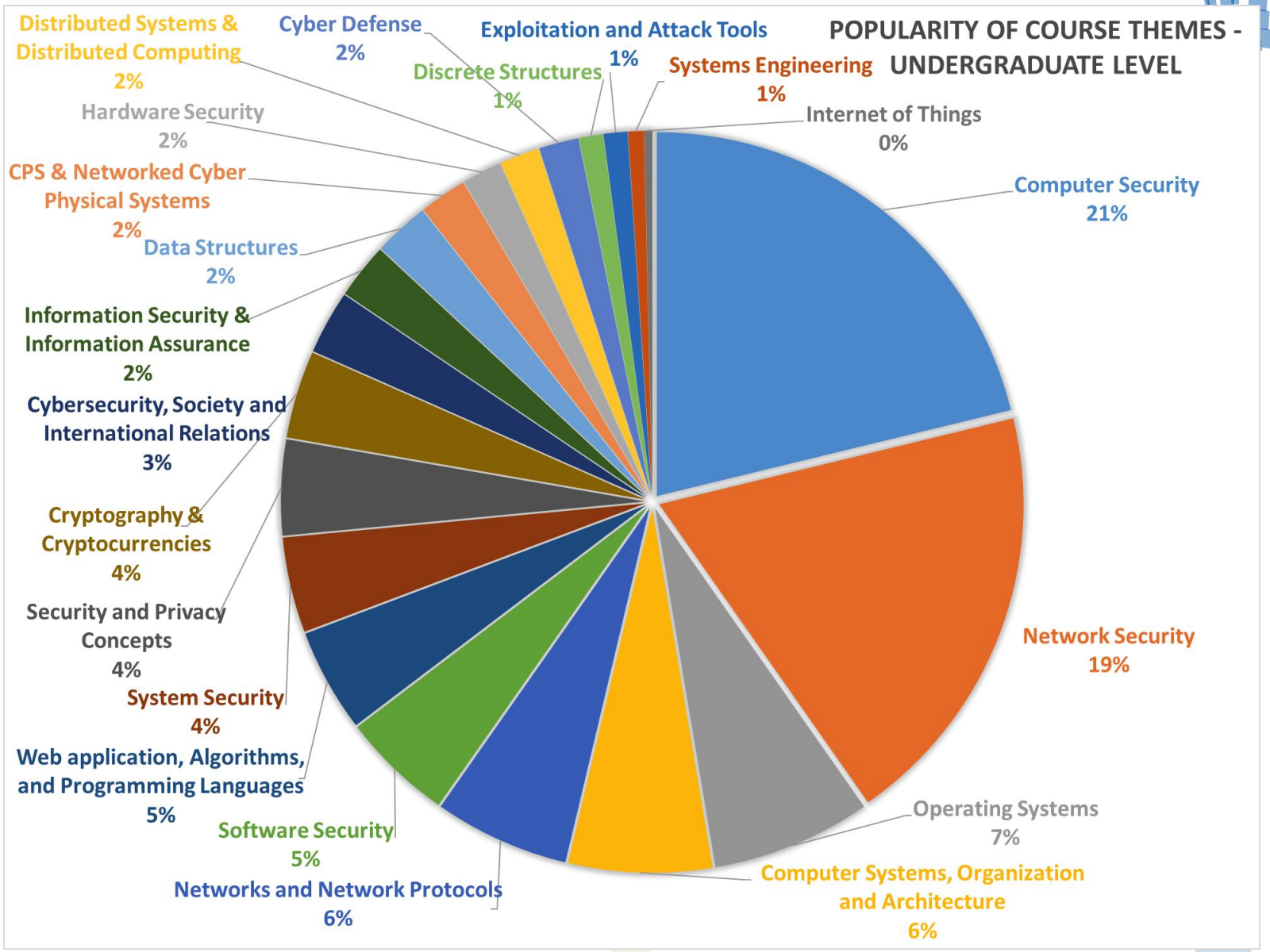
Adapted from: National Academies: A 21st Century Cyber Physical Education (2016)




- Computer Architecture
- Operating Systems
- Discrete Structures
- Data structures
- Algorithms & Programming
- Security & Privacy Concepts
  - Computer Security
  - Network Security
  - Networks & Network Protocols
  - Cryptography
  - Distributed Systems & Computing
  - Cyberphysical Systems
- System, HW & SW Security
- Information Security & Assurance
- Cybersecurity & Society
- Exploitation & Attack Tools
- Cyber Defense
- Systems Engineering

Adapted from: SEI Software Assurance Competency Model (2013)

# Survey of 104 Universities Summer 2017 (SERC RT-175)




Reflective of market interest shown across the application area of resilient CPS

# Agenda

- Background & Motivation
- CPS Security Taxonomy
- State of Security Education in Engineering
- Challenges and Recommendations

# Workshop Gap Identification

Engineering education gaps related to cybersecurity

- Security concerns emerging in today's embedded systems and CPS
- Fundamental security practices
- Domain & context knowledge
- Comprehension of tools
- Software assurance
- Security evaluation & test
- Adversary pace of change
- Lack of a BoK
- Sharing of data and use cases
- HW & SW supply chain issues

**Workshop 6 (Jul 31– Aug 2 2018)**
**State of the Engineering Workforce; Cybersecurity Engineering**

**Goal: Identify skill sets and curriculum needs for our current and future engineering workforce**

- **Understand engineering education gaps related to cybersecurity**
- **Develop Need's for today's engineering workforce**
- **Develop Need's for tomorrow's engineering workforce**
- **Identify efforts to meet anticipated EO on America's Workforce**

# Focus Needed

NIST

Search NIST

Information Technology Laboratory / Applied Cybersecurity Division

**NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)**

Knowledge ID: K0030

**Description:** Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).

Work Roles:

**Work Role ID:** SP-ARC-001
**Work Roles:** Enterprise Architect
**Work Role Description:** Develops and maintains business, systems, and information processes to support e develops information technology (IT) rules and requirements that describe baseline and target architectures.
**Category:** Securely Provision
**Specialty Area(s):** Systems Architecture

**Work Role ID:** SP-ARC-002
**Work Roles:** Security Architect
**Work Role Description:** Ensures that the stakeholder security requirements necessary to protect the organi business processes are adequately addressed in all aspects of enterprise architecture including reference mo solution architectures, and the resulting systems supporting those missions and business processes.
**Category:** Securely Provision
**Specialty Area(s):** Systems Architecture

**Work Role ID:** SP-SYS-001
**Work Roles:** Information Systems Security Developer
**Work Role Description:** Designs, develops, tests, and evaluates information system security throughout the cycle.
**Category:** Securely Provision
**Specialty Area(s):** Systems Development

**Work Role ID:** SP-SYS-002
Systems Developer

## NICE Cybersecurity Workforce Framework

**Table 1 - NICE Framework Workforce Categories**

| Categories | Descriptions |
|---|---|
| Securely Provision (SP) | Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development. |
| Operate and Maintain (OM) | Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security. |
| Oversee and Govern (OV) | Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work. |
| Protect and Defend (PR) | Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks. |
| Analyze (AN) | Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. |
| Collect and Operate (CO) | Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. |
| Investigate (IN) | Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence. |

# Primary Outcomes

- Fold cybersecurity education into curriculum at all levels and disciplines
- Foundational principles should start early – security hygiene and safe coding practices
- Fold specialized content into all engineering disciplines – for CPS and security
- Increase PhD's in systems engineering with a cybersecurity focus
- Create opportunities for experiential learning
- Contribute case studies from commercial and defense

# At the Professional level

- best level to introduce different disciplines and domains to the adversarial and subversion characteristics afforded by cyberspace
- need for development of a professional certification tailored to the needs of the CPS domain
- must also include software engineering certifications

# At the University level

- general studies should teach engineers how to produce higher quality secure software, introduce fundamentals, and good coding practices in every discipline
- government standards and guidelines are good case studies
- a core cybersecurity 101 course that is tailored to the discipline of interest, but cybersecurity principles should be embedded into existing curricula

# At the High School level & STEM

- High School would be the best place to introduce cybersecurity hygiene and good early coding practices
- There is a need to foster interest in secure cyber-physical systems in middle and high school level
  - High school challenge programs such as robotics challenges could include security challenges.
  - Organizations could sponsor challenges and develop “kits” for repeatable learning.
- Those with interest in coding should begin practicing safe versus vulnerable coding practices early in education

# Some Recommendations

1. Defense services are leading the way in education and training for cyber-physical security. The services should share best practices, programs, and guidance.
2. Develop a lexicon/taxonomy to adequately describe the CPS security domain, in order to inform the needed competency framework.
3. Sponsor academic Centers of Excellence in CPS security.
4. Develop a formal competency framework (informed by the NICE framework).
5. Address the System Security Engineering (SSE) competency gap in the CPS domain. Develop short application specific interpretation guides for CPS security.
6. Investigate formal CPS security certifications and their value.
7. Pursue a series of STEM activities for secure CPS.
8. Develop education modules in secure and safe coding practices.
9. Prototype a cyberspace-realistic virtual reality simulations for a relevant systems.
10. Standardize assurance case practices spanning safety and security.

29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

www.incose.org/symp2019