Answering the Secure Cyber-Resilient Engineering Workforce Challenge

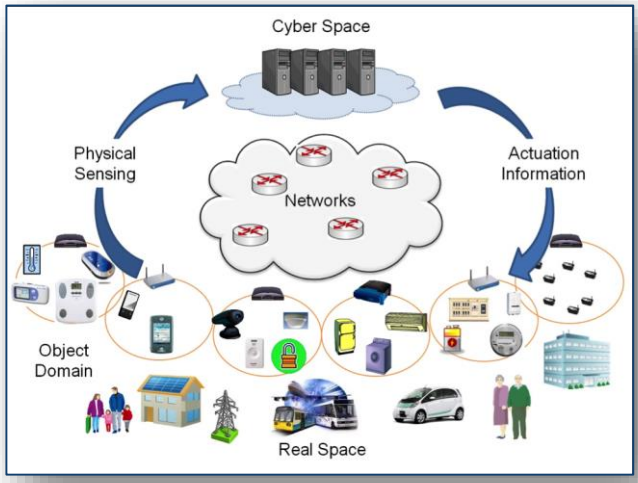
Tom McDermott, Deputy Executive Director, SERC

Stevens Institute of Technology – November 2019

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract H98230-08-D-0171. The SERC is a federally funded University Affiliated Research Center (UARC) managed by Stevens Institute of Technology consisting of a collaborative network of over 20 universities. More information is available at www.SERCuarc.org

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

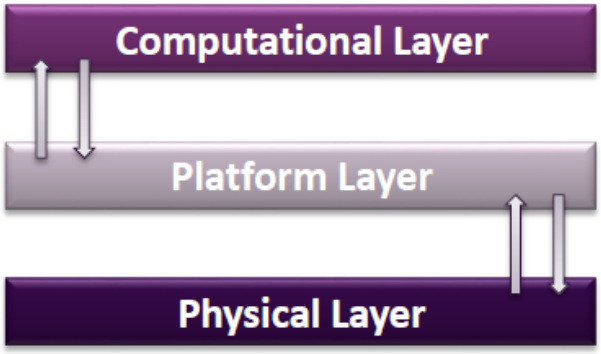


What are Cyber-Physical Systems?

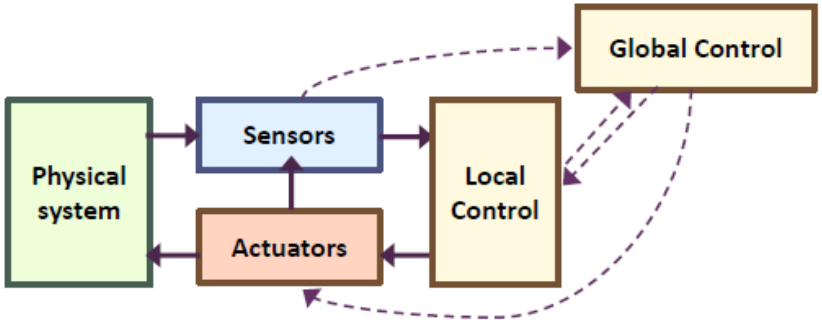
Engineered systems that…

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

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



SW models, platform models, physical models



Integration is key to system behavioral abstraction

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)

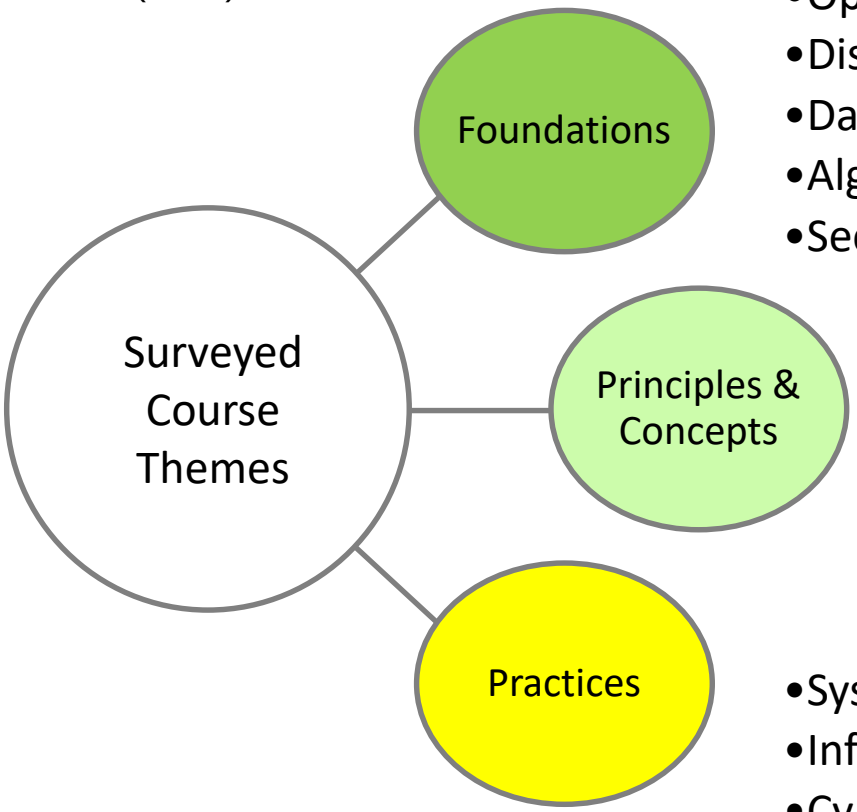
SYSTEMS ENGINEERING RESEARCH CENTER

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

Derived CPS Security Education Themes

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



Adapted from: SEI Software Assurance Competency Model (2013)

- Control Systems
- 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

SYSTEMS ENGINEERING RESEARCH CENTER

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 subsystems; Multi/Many-core architectures; Distributed system architectures
CE-ESY Embedded Systems	Characteristics of embedded systems; Basic software techniques for embedded applications; Parallel input and output; Asynchronous and synchronous serial communication; Periodic interrupts, waveform generation, time measurement; Data acquisition, control, sensors, actuators; Implementation strategies for complex embedded systems; Techniques for low-power operation
CE-NWK Computer Networks	Network architecture; Lo Network protocols; Netw Performance evaluation;
CE-SEC Information Security	Data security and integri Secret and public key cr security; Authentication;
CE-SPE Systems and Project Engineering	Project management prin and fault tolerance; Hard tation; System specificat hardware and software d sustainability, manufactu
	Managing system reso

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; Designing Interaction
IAS - Information Assurance and Security	Foundational Concepts; Principles of Secure Design; Defensive Programming; Threats and Attacks; Network Security; Cryptography; Web Security; Platform Security; Security Policy & Governance; Secure Software Engineering
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;
	Mobile Pl

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
	Understand

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 Body of Knowledge
- 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**

Workshop Recommendations

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

NIST Example

- Category: Securely Provision (SP)
- Definition — Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development.
- Specialty Areas:
  - Risk Management (SP-RSK), Software Development (SP-DEV), Systems Architecture (SP-ARC), Systems Development (SP-SYS), Systems Requirements Planning (SP-SRP), Technology R&D (SP-TRD), Test and Evaluation (SP-TST)
- Work Roles:
  - Authorizing Official (SP-RSK-001)
  - Security Control Assessor (SP-RSK-002)
  - Software Developer (SP-DEV-001)
  - Secure Software Assessor (SP-DEV-002)
  - Enterprise Architect (SP-ARC-001)
  - Security Architect (SP-ARC-002)
  - Research and Development Specialist (SP-TRD-001)
  - Systems Requirements Planner (SP-SRP-001)
  - System Test & Evaluation Specialist (SP-TST-001)
  - Information Systems Security Developer (SP-SYS-001)
  - Systems Developer (SP-SYS-002)
- Primary Competencies
  - 1. Information Assurance
  - 2. Vulnerabilities Assessment
  - 3. Infrastructure Design
  - 4. Information Systems/ Network Security
  - 5. Systems Testing and Evaluation
  - 6. Enterprise Architecture
  - 7. Data Privacy and Protection
  - 8. Risk Management
  - 9. Systems Integration
  - 10. Software Development

NIST Example

- Category: Securely Provision (SP)
- Definition — Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development.
- Specialty Areas:
  - Risk Management (SP-RSK), Software Development (SP-DEV), Systems Architecture (SP-ARC), Systems Development (SP-SYS), Systems Requirements Planning (SP-SRP), Technology R&D (SP-TRD), Test and Evaluation (SP-TST)

Real World Control Systems, Reliability, Dependability, Power mgmt., etc.
Hardware vulnerabilities and supply chain mgmt.

- Work Roles:
  - Authorizing Official (SP-RSK-001)
  - Security Control Assessor (SP-RSK-002)
  - Software Developer (SP-DEV-001)
  - Secure Software Assessor (SP-DEV-002)
  - Enterprise Architect (SP-ARC-001)
  - Security Architect (SP-ARC-002)
  - Research and Development Specialist (SP-TRD-001)
  - Systems Requirements Planner (SP-SRP-001)
  - System Test & Evaluation Specialist (SP-TST-001)
  - Information Systems Security Developer (SP-SYS-001)
  - Systems Developer (SP-SYS-002)

- Computer architect
- Control systems developer
- Embedded SW developer
- Security engineering
- System reliability and safety
- Secure HW assessor

- Primary Competencies
  - 1. Information Assurance
  - 2. Vulnerabilities Assessment
  - 3. Infrastructure Design
  - 4. Information Systems/ Network Security
  - 5. Systems Testing and Evaluation
  - 6. Enterprise Architecture
  - 7. Data Privacy and Protection
  - 8. Risk Management
  - 9. Systems Integration
  - 10. Software Development

- Computer engineering
- Physical world computing
- Control systems
- Distributed & embedded systems
- Real-time SW & operations
- Dependable computing
- System reliability and safety
- Power & energy
- Microelectronics

Questions and Discussion