Introducing Cyber Resiliency Concerns Into Engineering Education

Mr. Tom McDermott
Georgia Tech Research Institute

Mr. Barry Horowitz
University of Virginia

NDIA 20th Annual Systems Engineering Conference
26 October 2017

Springfield, Virginia

SERC RT 175: Human Capital Development – Resilient Cyber-Physical Systems

- Principal Investigators: Tom McDermott (GT) and Barry Horowitz (UVA)
  01 March – 30 September 2017

- Scope
  - Characterize the existing undergraduate and graduate engineering and computer science education programs in the U.S. as related to emerging needs of large scale cyber-physical systems
  - Develop a taxonomy of related attributes for dependable and secure computing, and
  - conduct a survey of related undergraduate and graduate education programs and lab facilities in the fields of information security, computer science, computer engineering, and electrical engineering
  - identify the challenges for:
    - Developing a body of knowledge for resilient cyber-physical systems,
    - Developing a reference curriculum for SE of resilient cyber-physical systems and resilient computing systems, and
    - Needs and opportunities for developing potential lab facilities.

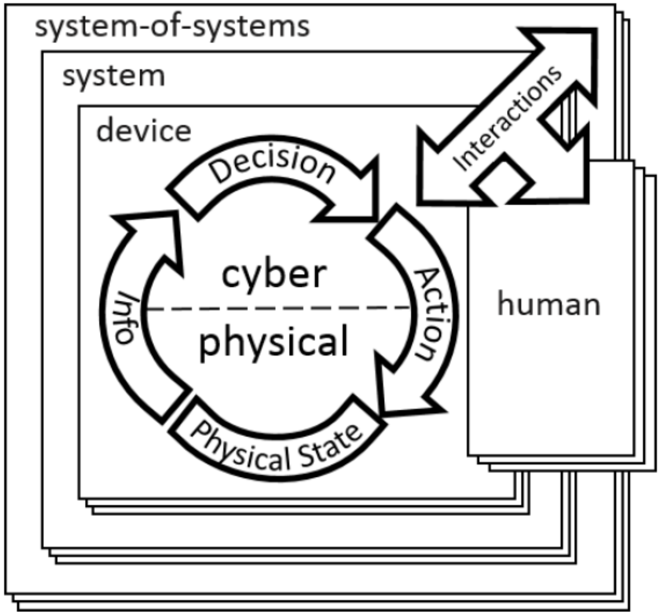
RT 175: Human Capital Development – Resilient Cyber-Physical Systems

- Within the context of military cyber operations and threats, CPS resilience can be interpreted as “the ability of a system to maintain its operational mission effectiveness while under adversary offensive cyber operations, and to manage the risk of adversary exploitation of the system for intelligence purposes.” (Holtzman, 2017)

- “…considering large, networked, evolving, systems either fixed or mobile, with demanding requirements driven by their domain of application...these emerging systems suffer from a significant drop in dependability and security in comparison with the former systems” (EU-ReSIST project)

- “Core CPS knowledge involves not only an understanding of the basics of physical engineering and cyber design and implementation, but understanding how the physical and cyber aspects influence and affect each other…Because CPS engineering centers on the interaction of physical and cyber aspects of systems, it will often not be sufficient to create CPS curricula by simply combining material from existing courses.” (NAP 2016)

What is a CPS?



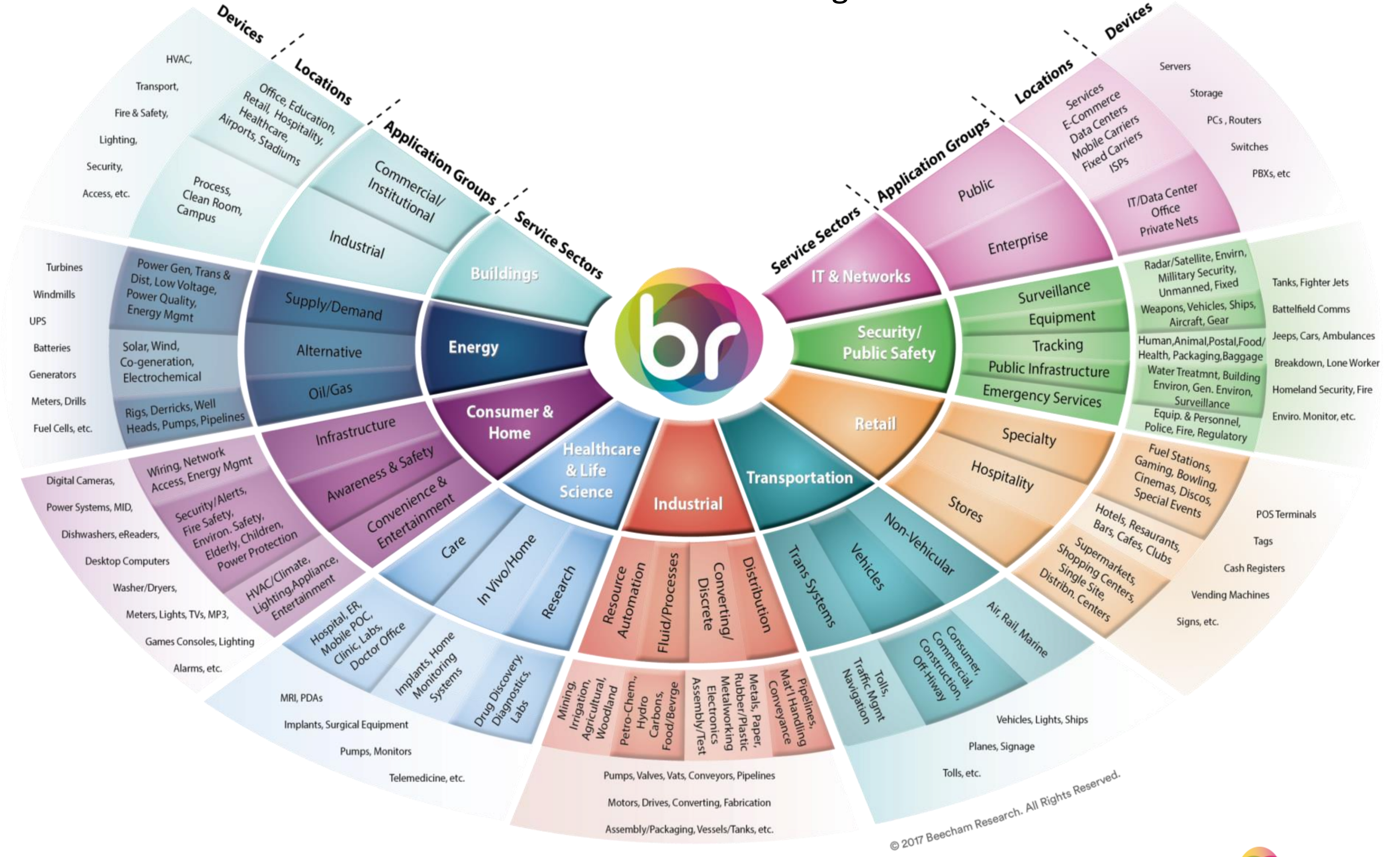
NIST CPS Conceptual Model

- “engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components” (NSF)
- “computers and networks which control physical processes, using feedback loops that affect computations and vice versa” (UC Berkeley)

NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview Version 1.0

M2M World of Connected Services

The Internet of Things



Devices
Locations
Application Groups
Service Sectors

Buildings
Commercial/ Institutional
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Industrial
Process, Clean Room, Campus
HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.

Energy
Supply/Demand
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Alternative
Solar, Wind, Co-generation, Electrochemical
Oil/Gas
Rigs, Derricks, Well Heads, Pumps, Pipelines
Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.

Consumer & Home
Infrastructure
Wiring, Network Access, Energy Mgmt
Awareness & Safety
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
Convenience & Entertainment
HVAC/Climate, Lighting,Appliance, Entertainment
Digital Cameras, Power Systems, MID, Dishwashers, eReaders, Desktop Computers, Washer/Dryers, Meters, Lights, TVs, MP3, Games Consoles, Lighting, Alarms, etc.

Healthcare & Life Science
Care
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
In Vivo/Home
Implants, Home Monitoring Systems
Research
Drug Discovery, Diagnostics, Labs
MRI, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.

Industrial
Resource Automation
Mining, Irrigation, Agricultural, Woodland
Fluid/Processes
Petro-Chem., Hydro Carbons, Food/Bevrge
Converting/ Discrete
Metals, Paper, Rubber/Plastic Metalworking Electronics Assembly/Test
Distribution
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.

Transportation
Trans Systems
Tolls, Traffic Mgmt Navigation
Vehicles
Consumer, Commercial, Construction, Off-Hiway
Non-Vehicular
Air, Rail, Marine
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.

Retail
Specialty
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hospitality
Hotels, Resaurants, Bars, Cafes, Clubs
Stores
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.

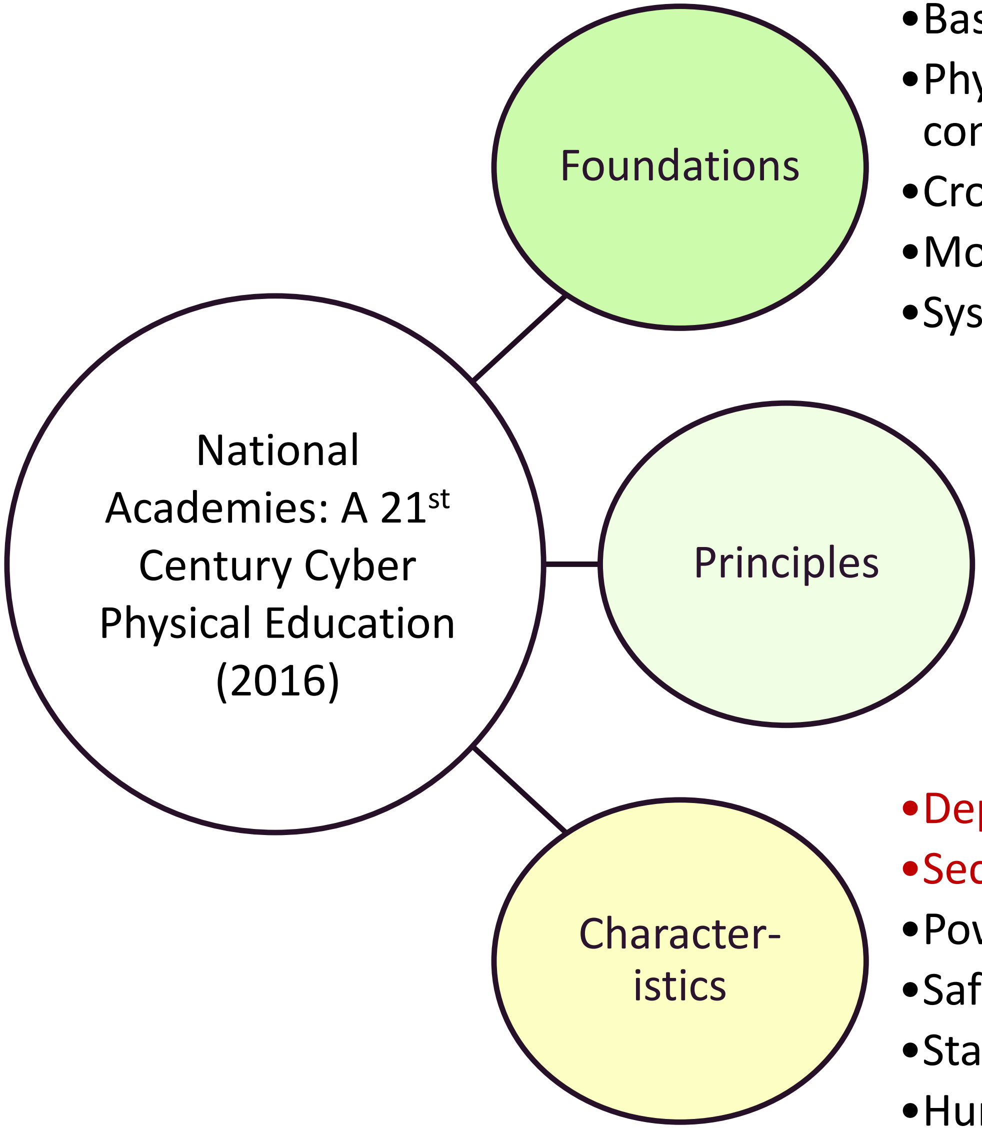
Security/ Public Safety
Surveillance
Radar/Satellite, Envirn, Millitary Security, Unmanned, Fixed
Equipment
Weapons, Vehicles, Ships, Aircraft, Gear
Tracking
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Public Infrastructure
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Emergency Services
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets, Battelfield Comms, Jeeps, Cars, Ambulances, Breakdown, Lone Worker, Homeland Security, Fire, Enviro. Monitor, etc.

IT & Networks
Public
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
Enterprise
IT/Data Center Office Private Nets
Servers, Storage, PCs , Routers, Switches, PBXs, etc

http://www.beechamresearch.com/

beecham research

Taxonomy of CPS Competencies



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

Foundations

- Basic computing concepts
- Physical world computing properties & constraints
- Cross-cutting applications
- Modeling Dynamic Control processes
- System lifecycle development

Principles

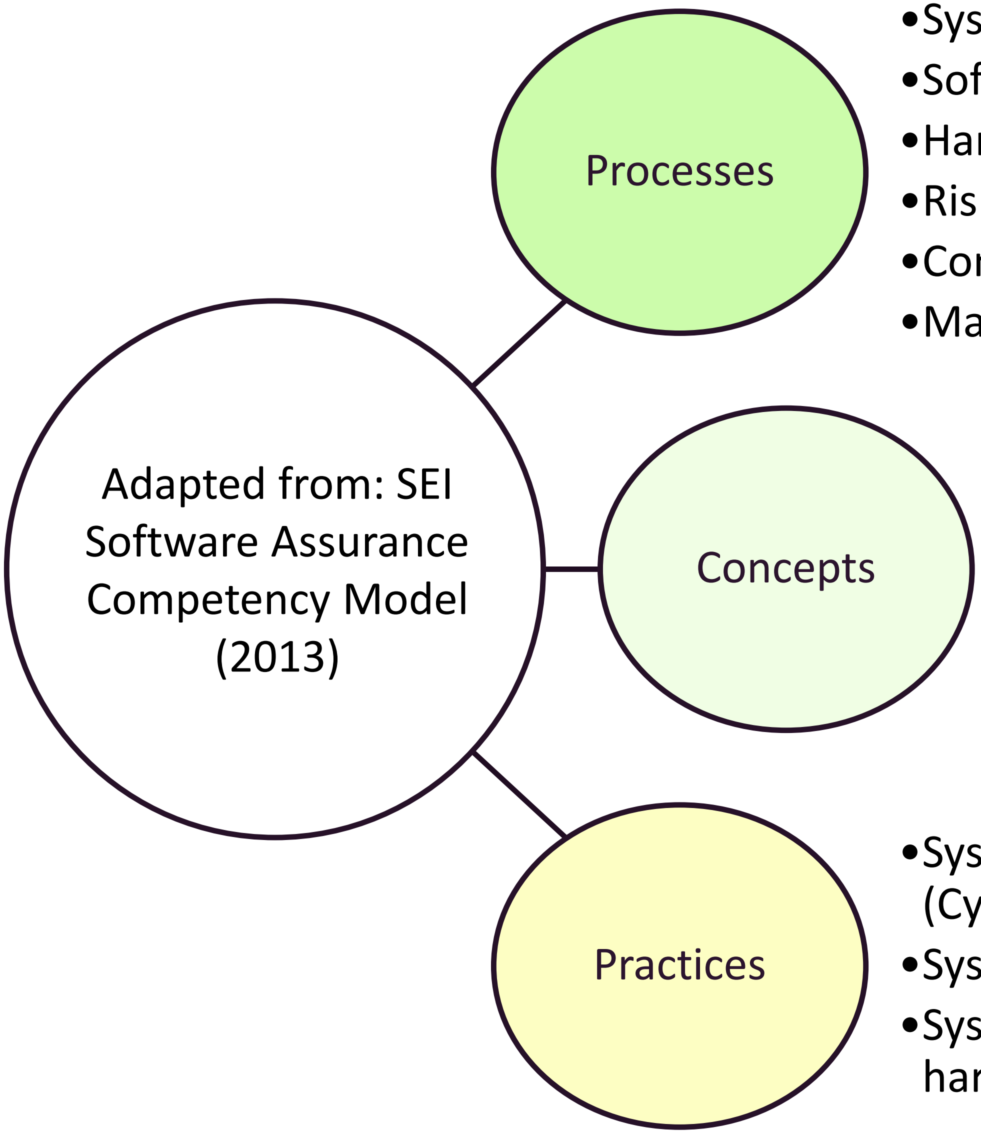
- Communications and networking
- Real-time operation
- Distributed & embedded systems
- Physical properties
- Human interaction

Character-istics

- Dependability
- Security and privacy
- Power and energy
- Safety
- Stability and performance
- Human factors and usability

SYSTEMS ENGINEERING RESEARCH CENTER

Taxonomy of Assurance Competencies



Adapted from: SEI Software Assurance Competency Model (2013)

Processes

- System/software lifecycle
- Software assurance
- Hardware assurance
- Risk management
- Compliance
- Management

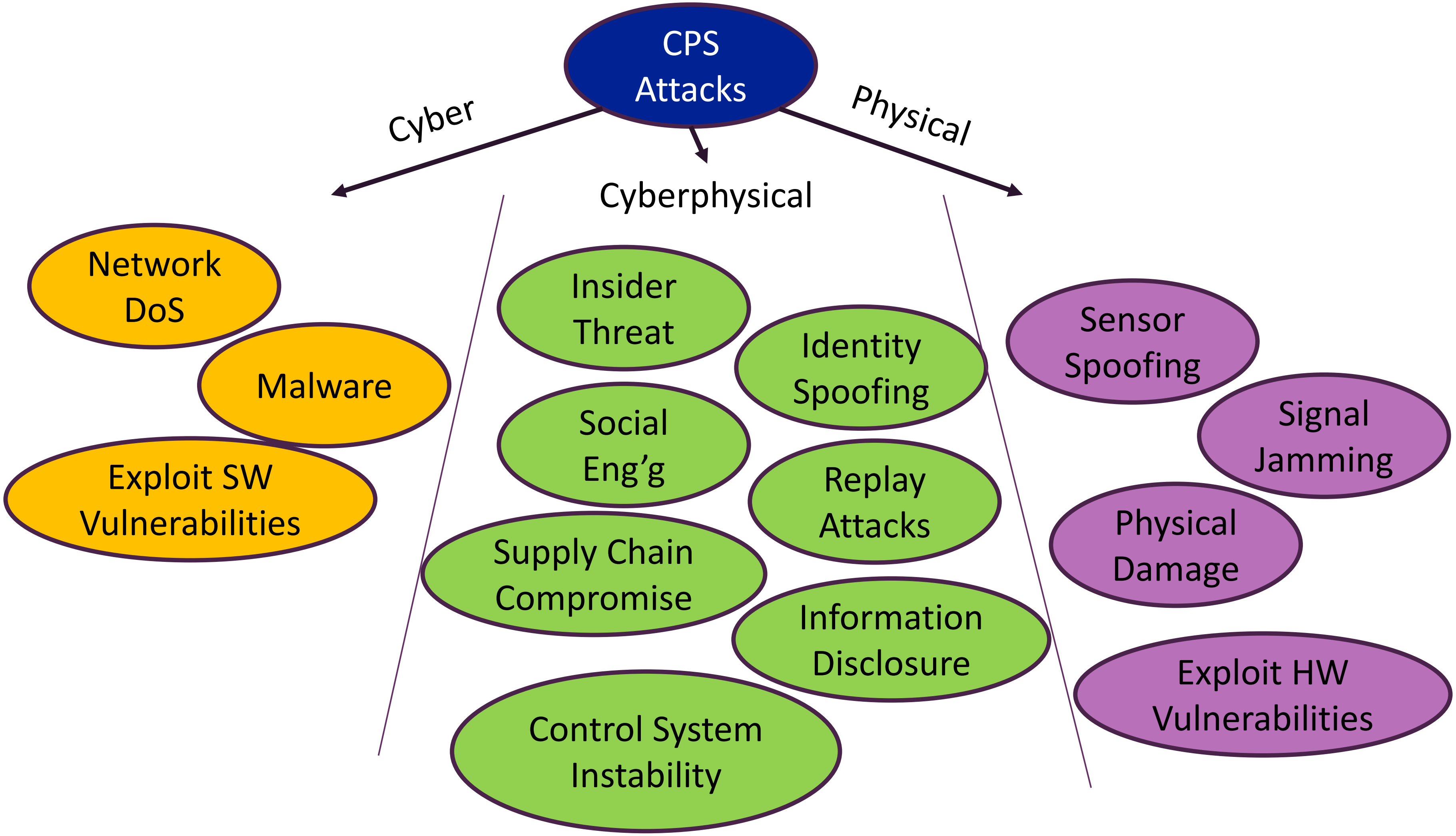
Concepts

- Risk management & threat modeling
- Assurance assessment
- Assurance measurement
- Business case

Practices

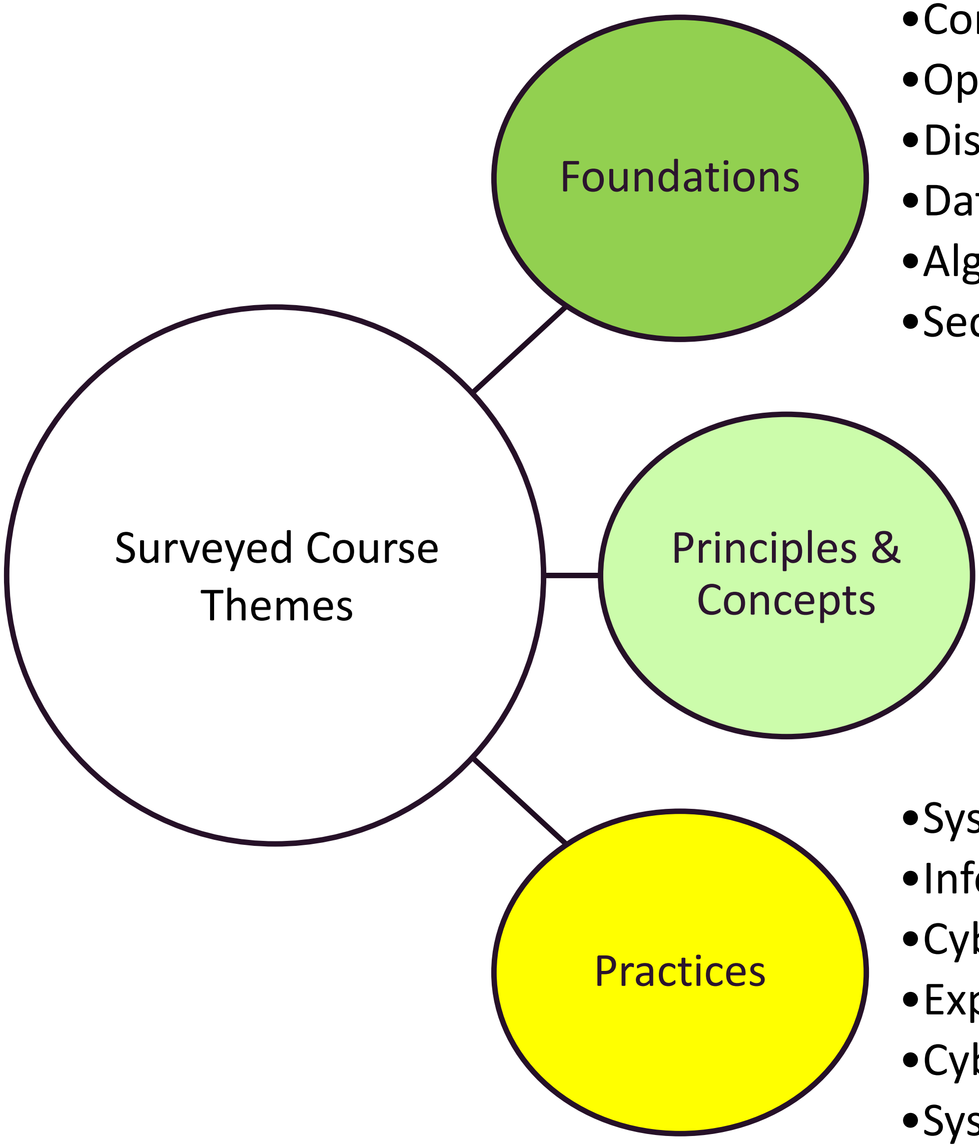
- System functional assurance (Cybersecurity)
- System operational assurance
- System security assurance (software & hardware

CPS Attack Taxonomy



Because cyber-physical systems consist of both cyber and physical systems, the attack surface, when compared, to either cyber or physical systems solely, is much larger

Derived CPS Security Education Themes



Surveyed Course Themes

Foundations

- Computer Architecture
- Operating Systems
- Discrete Structures
- Data structures
- Algorithms & Programming
- Security & Privacy Concepts

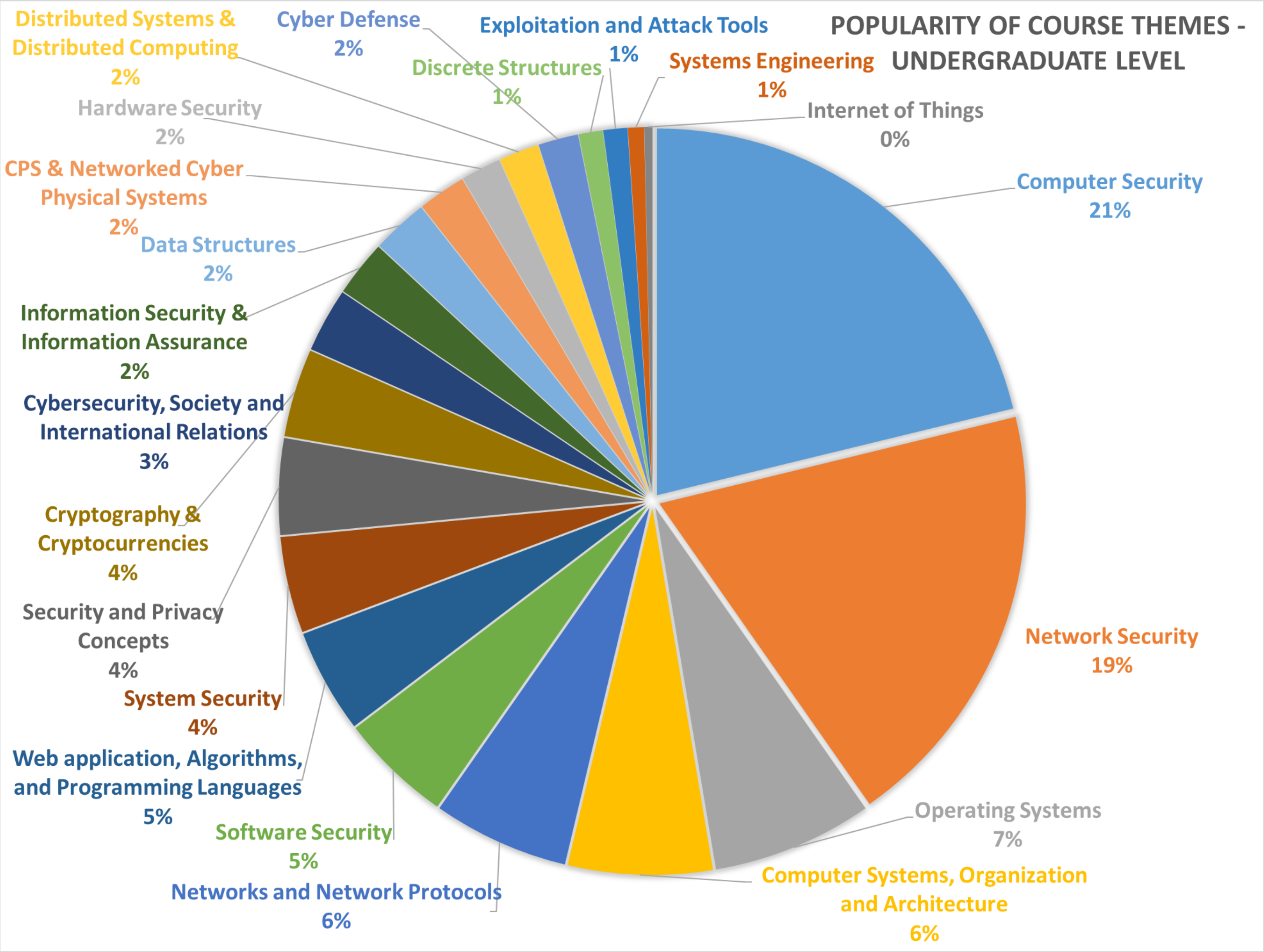
Principles & Concepts

- Computer Security
- Network Security
- Networks & Network Protocols
- Cryptography
- Distributed Systems & Computing
- Cyberphysical Systems

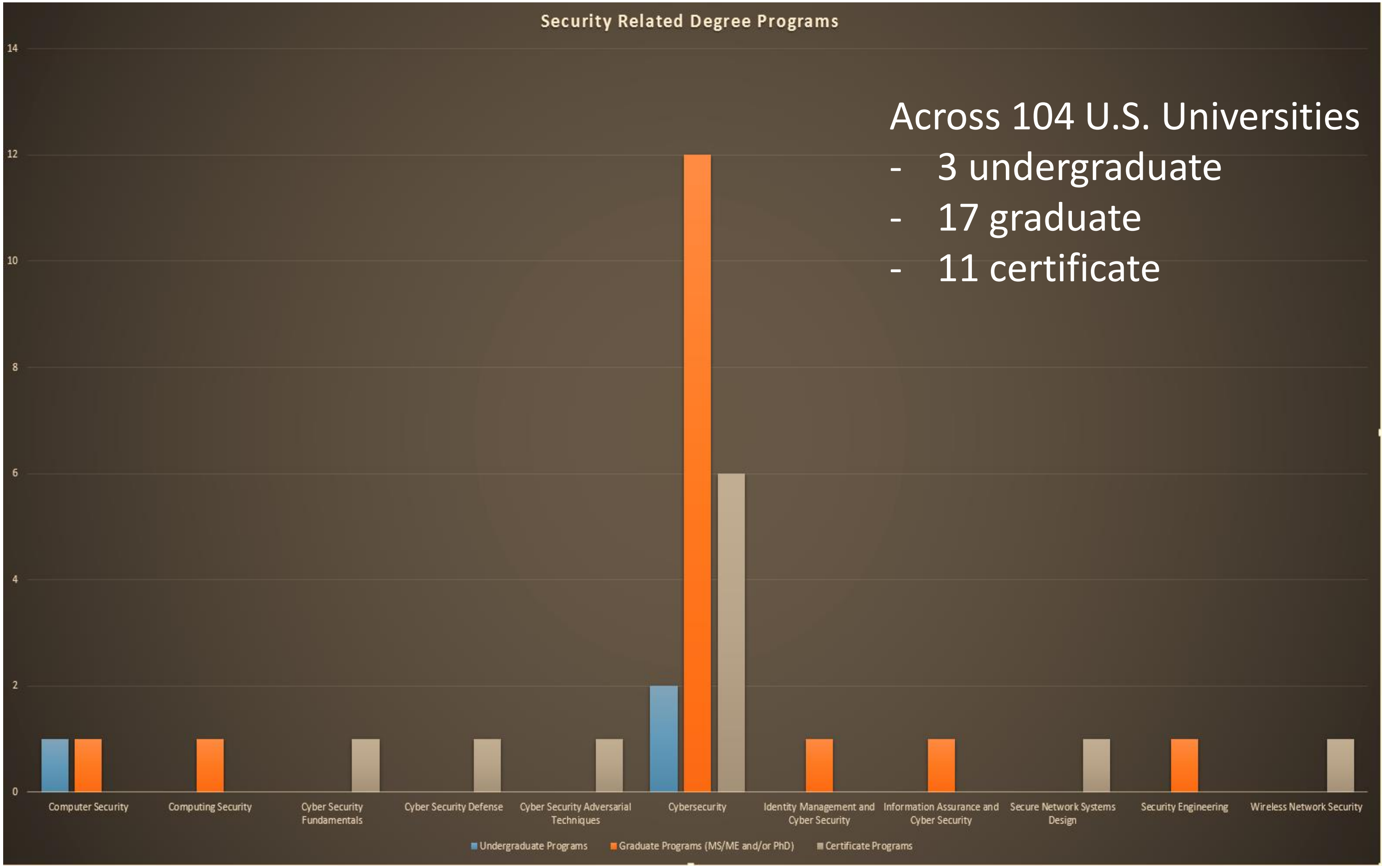
Practices

- System, HW & SW Security
- Information Security & Assurance
- Cybersecurity & Society
- Exploitation & Attack Tools
- Cyber Defense
- Systems Engineering

Survey of 104 Universities by Course Themes



Degree & Certificate Programs with Security Themes



Across 104 U.S. Universities

- 3 undergraduate
- 17 graduate
- 11 certificate

A Prototype Professional Education Course

- Underlying concepts for applying resilience-based solutions to cyber security defense
- System-Aware Cybersecurity & Experiments with Technology Prototypes
- Fault Tolerant Systems Design Principles
- Attack Trees
- Attack Taxonomy
- Cybersecurity-related Human Factors Issues
- Project Plan - Hands-on laboratory exercise
- Hands-on attack laboratory activity
- Hands-on decision support tool laboratory activity
- Presentations of Individual Team Exercise Results and Class Evaluation of Results
- Summary and Discussion

Inspiration for a Sharable CPS Security Laboratory

- CPS platforms remotely interfaced and accessible via web browsers or a cloud-based environment
- a software simulator to run first operations in a virtual environment and then transition to hardware experiments
- A framework to overwrite any unsafe situation and reset the system needs to be in place

Recommendations

- The future CPS workforce needs to include a combination of
  - engineers trained in foundational fields (such as electrical and computing engineering, mechanical engineering, systems engineering, and computer science),
  - engineers trained in specific applied engineering fields (such as aerospace and civil engineering),
  - and CPS engineers, who focus on the knowledge and skills spanning cyber technology and physical systems that operate in the physical world
- Consider establishing one or two new cyber physical system resilience education efforts that build upon the study outcomes
- Model-based engineering techniques combined with physical labs would provide students with a greater understanding of the engineering efforts required to both derive and evaluate possible CPS security solutions

Recommendations

- Additional funding and attention must be delegated to research and projects in CPS
    - —More research into CPS security and dependability must occur in university lab environments
    - —Appropriate use cases for new educational-focused laboratories will need to be developed
- Due to issues associated with DoD information security sensitivities and industry proprietary solution sensitivities, appropriate use cases for new educational-focused laboratories will need to be developed
- A network of CPS Labs accessible to all is a worthy model