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

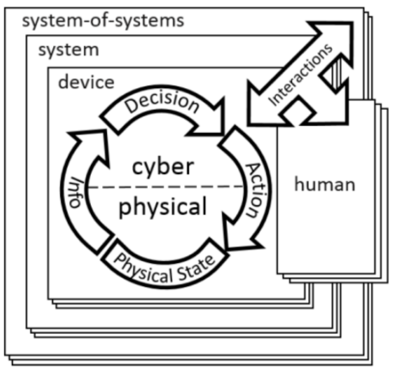
Tom McDermott, Molly Nadolski, Paige Meierhofer (GT)
Barry Horowitz, Nicola Bezzo, Jack Davidson, Ron Williams (UVA)

Research Task / Overview

The DoD has undertaken a number of initiatives to better understand the vulnerability of their systems to a cyber-equipped adversary, and to address engineering processes that would help ensure DoD systems can complete their missions in the presence of such adversaries. There has been an intensive focus on securing computer networks and IT systems, and a great deal of investment in perimeter oriented defenses. Although this remains important, there is an increasing focus on the vulnerabilities of DoD weapon systems, and the general category of cyber-physical systems (CPS).

The DoD has focused investment for some time now on developing and sustaining a cyber-ready workforce. The objective of this research is to assess the ability and current state of U.S. university education to produce a workforce that can design, protect, and sustain secure and resilient CPS. This research is intended as an initial characterization of the educational landscape in order to plan further initiatives in workforce development.

What is a CPS?



NIST CPS Conceptual Model [1]

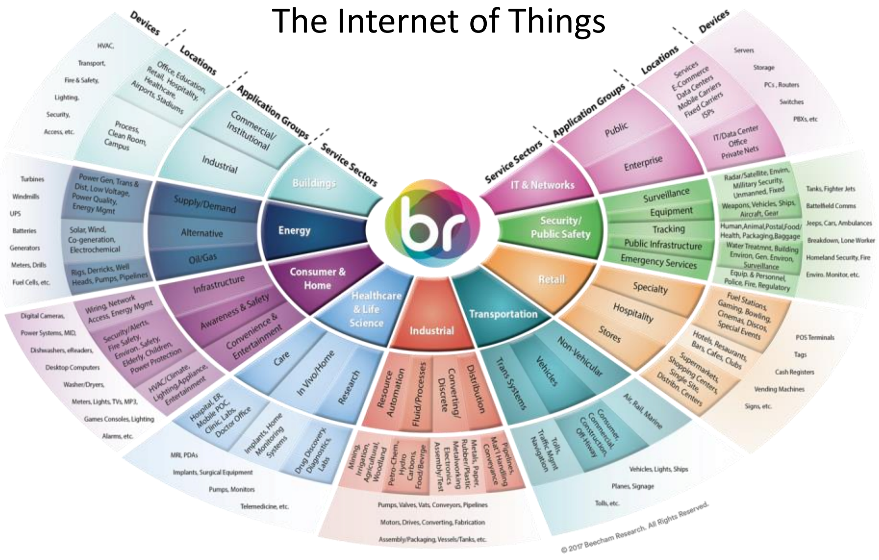
CPS are "engineered systems that are built from, and depend upon, the **seamless integration of computational algorithms and physical components**" (National Science Foundation)

CPS are "computers and networks which control physical processes, using feedback loops that affect computations and vice versa" (UC Berkeley web)

Where are CPS?

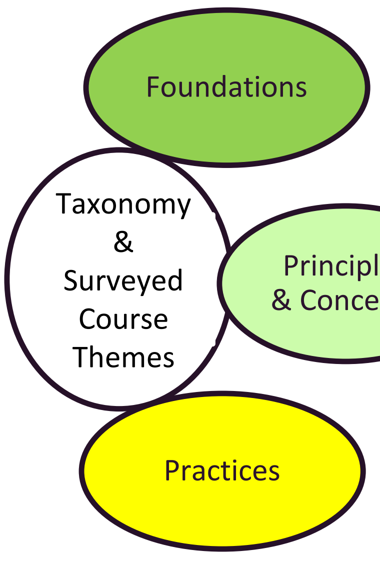
M2M World of Connected Services

The Internet of Things


Devices
Locations
Application Groups
Service Sectors
br
Buildings
Commercial/ Institutional
Industrial
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
Energy
Supply/Demand
Alternative
Oil/Gas
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
Consumer & Home
Infrastructure
Awareness & Safety
Convenience & Entertainment
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
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
In Vivo/Home
Research
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
MRI, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
Industrial
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Mining, Irrigation, Agricultural, Woodland
Petro-Chem, Hydro Carbons, Food/Bevrge
Metals, Paper, Rubber/Plastic, Metalworking, Electronics, Assembly/Test
Pipelines, Mat'l Handling, Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines, Motors, Drives, Converting, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
Transportation
Trans Systems
Vehicles
Non-Vehicular
Tolls, Traffic Mgmt, Navigation
Consumer, Commercial, Construction, Off-Highway
Air, Rail, Marine
Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
Retail
Specialty
Hospitality
Stores
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distrib. Centers
POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
Security/ Public Safety
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Radar/Satellite, Envirn. Military Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human, Animal, Postal, Food/ Health, Packaging, Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets, Battlefield Comms, Jeeps, Cars, Ambulances, Breakdown, Lone Worker, Homeland Security, Fire, Enviro. Monitor, etc.
IT & Networks
Public
Enterprise
Services, E-Commerce, Data Centers, Mobile Carriers, Fixed Carriers, ISPs
IT/Data Center, Office, Private Nets
Servers, Storage, PCs, Routers, Switches, PBXs, etc
© 2017 Beecham Research. All Rights Reserved.

http://www.beechamresearch.com/

CPS Security Education Themes



Foundations

Taxonomy & Surveyed Course Themes

Principles & Concepts

Practices

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

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

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

Goals & Objectives

- 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.

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
- Additional funding and attention must be delegated to research and projects in CPS
- New educational-focused laboratories need to be developed

A Sharable CPS Security Lab

- Inspired by GT/NSF Robotarium model, sharing addresses cost of CPS equipment
- 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

robotarium.gatech.edu

Contacts/References

Tom McDermott, Georgia Tech, tom.mcdermott@gtri.gatech.edu
Barry Horowitz, Univ of Virginia, bh8e@virginia.edu

[1] "NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview Version 1.0
[2] National Academies of Sciences, Engineering, and Medicine (2016). A 21st Century Cyber-Physical Systems Education. Washington, DC: The National Academies Press.
[3] Software Engineering Institute. Software Competency Model. CMU/SEI-2013-TN-004. Carnegie Mellon Univ.

SERC Doctoral Students Forum and SERC Sponsor Research Review, November 7 - 8, 2017