DHS Science and Technology Directorate
Cyber Physical Systems Security (CPSSEC)

Cyber Physical Systems: A Core Opportunity

Automobiles, medical devices, building controls and the smart grid all are examples of cyber physical systems (CPS). Each includes smart networked systems with embedded sensors, processors and actuators that sense and interact with the physical world and support real-time, guaranteed performance in safety-critical applications. Whether referencing the forward collision prevention capability of a car or a medical device's ability to adapt to circumstances in real-time, these systems are a source of competitive advantage in today's innovation economy.

The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment. Proactive and coordinated efforts are needed to strengthen and maintain secure and resilient cyber physical systems.

A Critical Time for CPS Design & Deployment

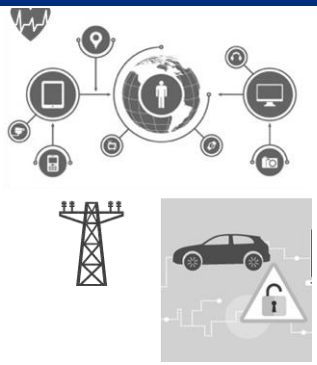
Advances in networking, computing, sensing and control systems have enabled a broad range of new devices. These systems are being designed and deployed now, however, security often is forgotten or added later. While some Internet of Things (IoT) devices have limited lifespans, many being deployed today will have lifespans measured in decades. Current design choices will impact the next several decades in transportation, health care, building control systems, manufacturing, energy, and other sectors.

CPS Space Spans Multiple Sectors

The Cyber Physical Systems vision statement from the Networking Information Technology Research and Development Program identifies nine areas of critical importance to government: agriculture, building controls, defense, energy, emergency response, health care, manufacturing and industry, society and transportation. These areas have shared issues of cybersecurity, economics, interoperability, privacy, safety and reliability, and social aspects. No single agency can tackle all these areas alone.

CPSSEC Project Purpose

The CPSSEC project is working to develop cybersecurity technical guidance for critical infrastructure sectors facing CPS challenges. It is conducting this effort in collaboration with key government, infrastructure and industry partners with the goal to transition guidance in a sustainable way.



The project is developing solutions for automotive, medical device, building controls, smart manufacturing and the smart grid security with an increasing focus on IoT security. DHS S&T also engages through coordination with the sector-specific agency, government research agencies, industry engagement and support for sector-focused innovation, small business efforts and technology transition.

Accomplishments to Date

- A design document for securely updating automobiles
- A model Medical Device Risk Assessment Platform
- A testbed for smart grid security developed in collaboration with the National Science Foundation

Upcoming Milestones

- Automotive telematics cyber security assessment and application for the federal government vehicle fleet
- Industry-endorsed reference implementation for securely updating automobiles
- Vulnerability assessment for building controls in key sites (airports, federal buildings, etc.)

Performers

- New York University, New York
- University of Michigan, Ann Arbor, Michigan
- Hughes Research Laboratories, Malibu, California
- Medical Device Innovation, Safety and Security Consortium, New York
- Adventium Labs, Minneapolis
- Kansas State University, Manhattan, Kansas
- Arizona State University, Tempe, AZ
- Iowa State University, Ames, IA
- Vanderbilt University, Nashville, TN
- Virginia Tech, Blacksburg, VA
- Volpe Center, Boston, MA

Homeland Security
Science and Technology

To learn more about Cyber Physical Systems Security, contact Dan Massey, program manager, at sandt-cyber-liaison@hq.dhs.gov

2016-11-15