



Perspectives on CPS Security and Resilience



David Corman
CISE Directorate
National Science Foundation

Outline

- What are Cyber-physical systems?
- What do we mean by CPS security and why is it different? How does resilience enter into the discussion?
- What is NSF perspective on CPS security and resilience, and some recent examples





What are Cyber-Physical Systems?





In a few words...

Cyber-physical systems are smart, complete systems of tomorrow;

Cyber-physical systems will enable ubiquitous technologies and applications for the future.

Cyber-physical systems consider the user and the environment in which the system operates



Smart Infrastructure

Imagine a day when...

static infrastructure is adaptable and safe

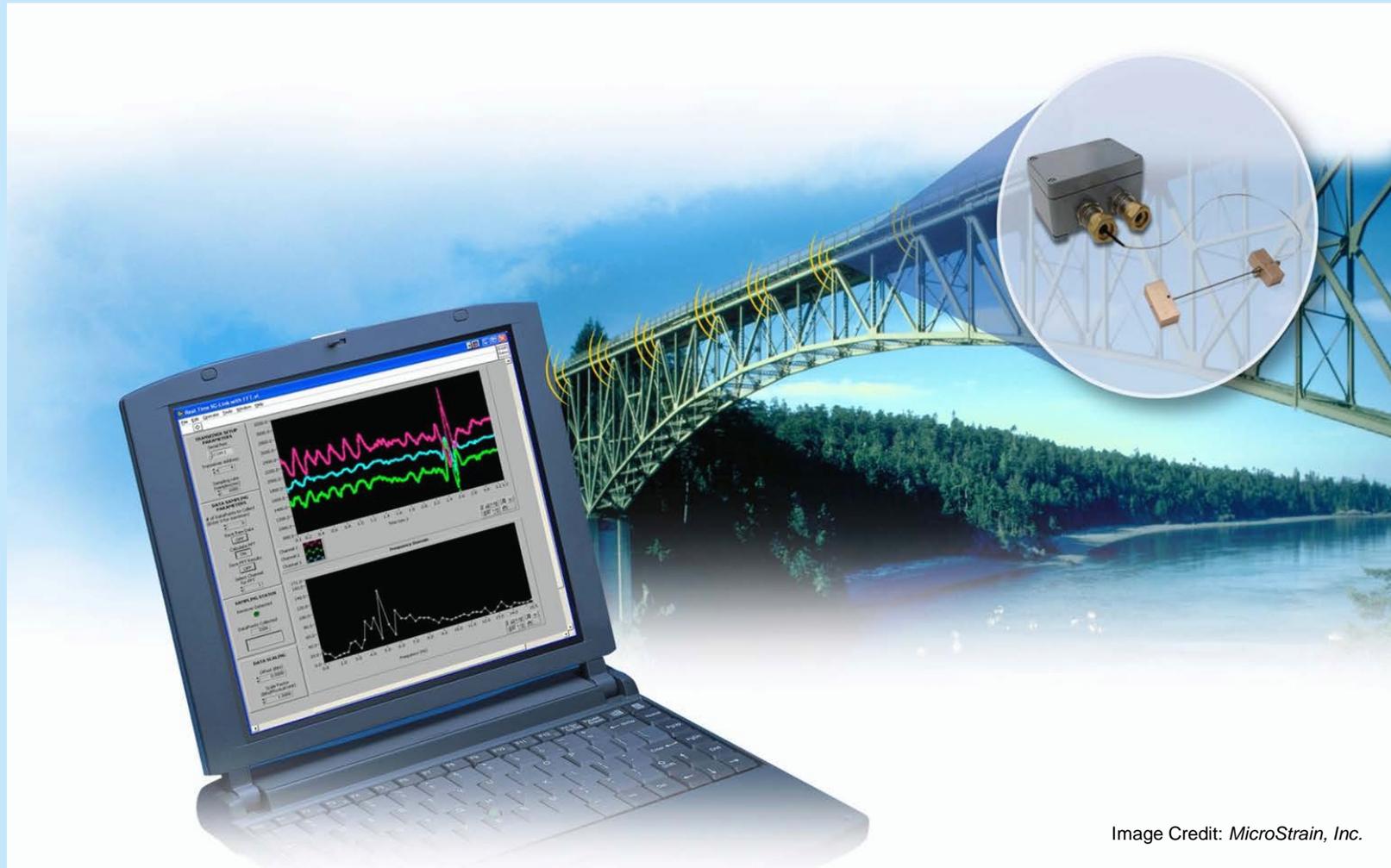


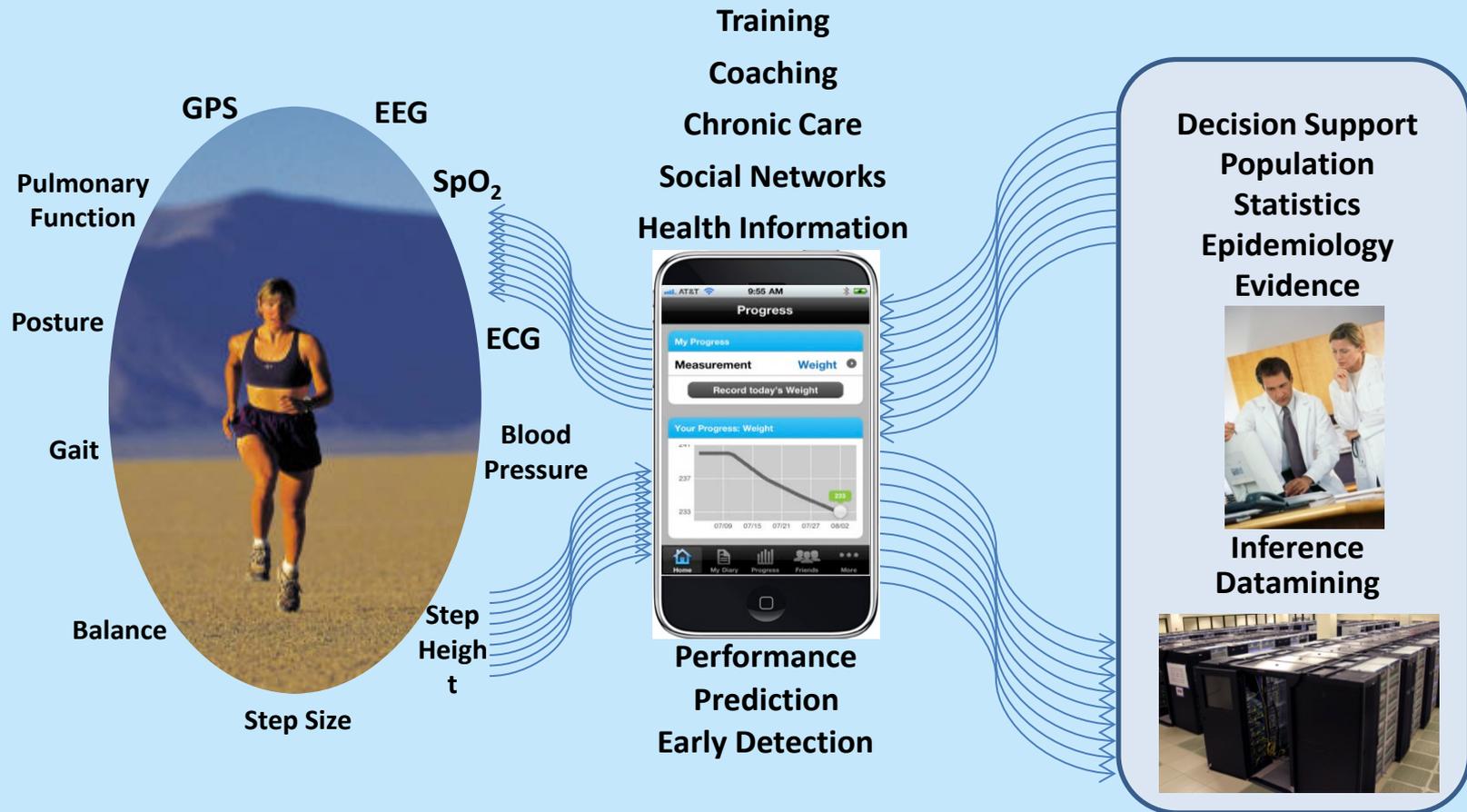
Image Credit: *MicroStrain, Inc.*



Health and Wellbeing

Imagine a day when...

wellbeing is pervasive and healthcare is personalized



Smart Grids

Imagine a day when...

energy is efficiently used and intelligently managed



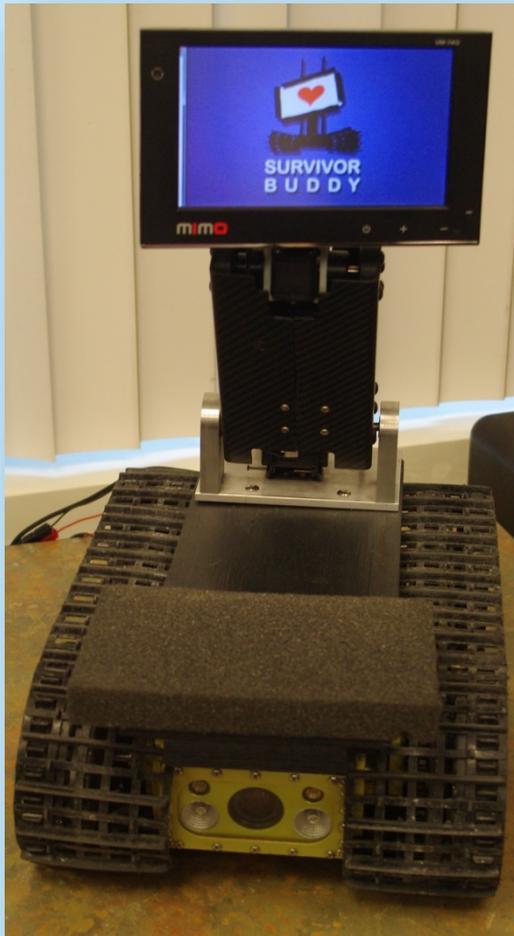
Image Credit: Cisco, Inc.



Emergency Response

Imagine a day when...

we can prevent, mitigate, and recover from disasters



Transportation: Safety and Energy

Imagine a day when...

traffic fatalities no longer exist



Image Credit: PaulStamatiou.com





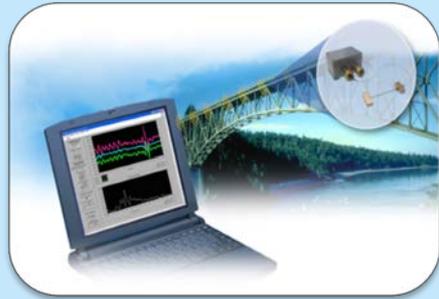
The Promise

Advances in *cyber-physical systems* hold the potential to reshape our world with more responsive, secure, and efficient systems that:

- transform the way we live
- drive economic prosperity
- underpin national security
- enhance societal well-being
- users can bet their life on



CPS and National Priorities



**Manufacturing,
Robotics, & Smart
Systems**



**Environment &
Sustainability**



**Emergency Response
& Disaster Resiliency**



Health & Wellbeing



**Transportation &
Energy**



**Broadband &
Universal Connectivity**



Secure Cyberspace



**Education and
Workforce
Development**



NSF Vision for Cyber Physical Systems



Cyber-Physical Systems

Deeply integrating computation, communication, and control into physical systems

- Pervasive computation, sensing and control
- Networked at multi- and extreme scales
- Dynamically reorganizing/reconfiguring
- High degrees of automation
- Dependable operation with high assurance of reliability, safety, security and usability



Transportation

- Faster and safer aircraft
- Improved use of airspace
- Safer, more efficient cars



Energy and Industrial Automation

- Homes and offices that are more energy efficient and cheaper to operate
- Distributed micro-generation for the grid



Healthcare and Biomedical

- Increased use of effective in-home care
- More capable devices for diagnosis
- New internal and external prosthetics

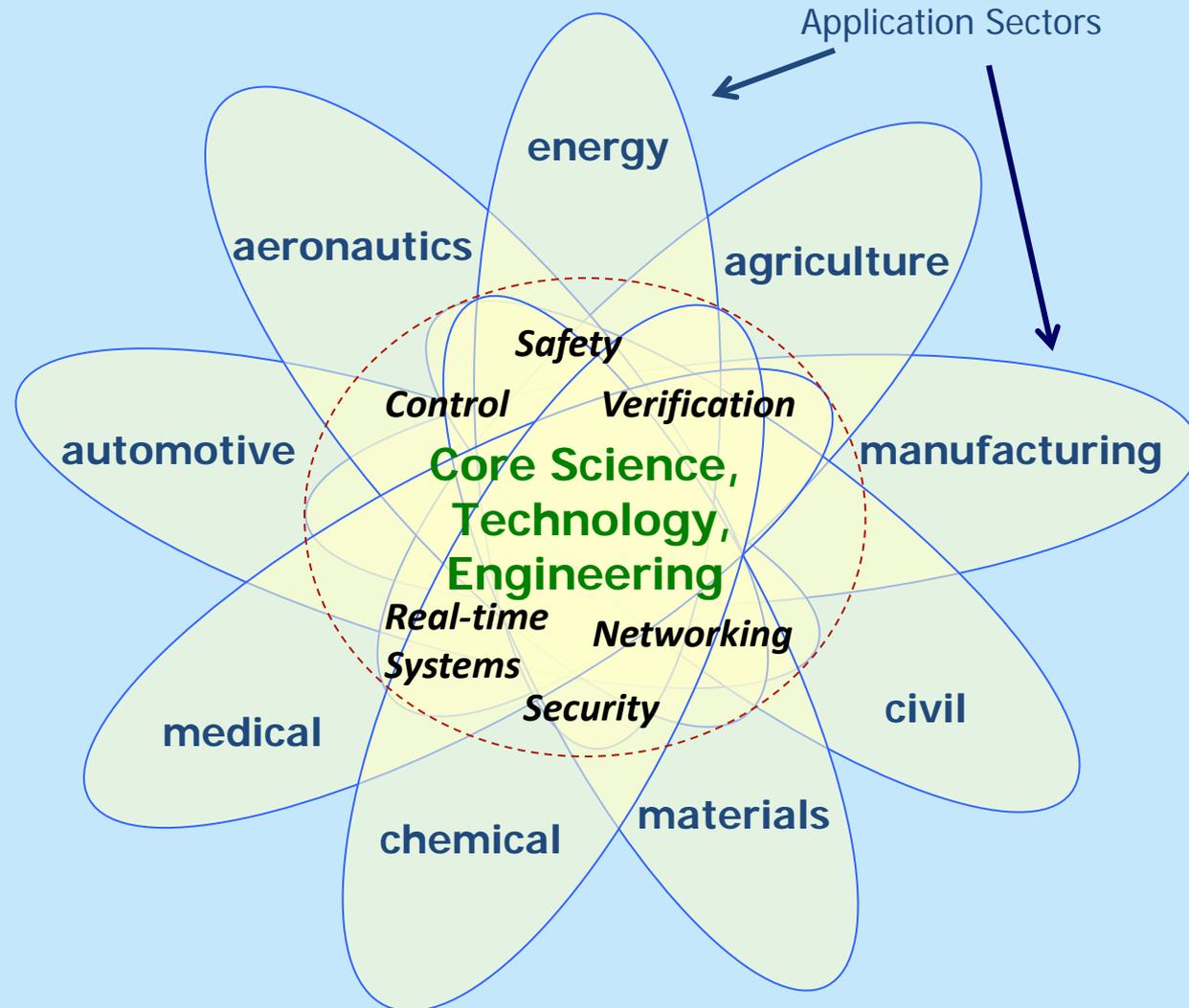


Critical Infrastructure

- More reliable power grid
- Highways that allow denser traffic with increased safety

NSF model for expediting progress

- Abstract from sectors to more general principles
- Apply these to problems in new sectors
- Build a new CPS community
- Encourage other communities to join



Some CPS Program Info

- Foundation-wide initiative including Directorate for Computer and Information Science and Engineering (CISE) and Directorate of Engineering
- Since CPS Launch in 2009:
 - Over \$200M investment
 - 250 awards
 - 350+ PIs and Co-PIs in 35 states
 - 60 new awards in FY13 (35 projects)
 - Over \$35M investment in FY13, over \$40M in FY14
 - Three Classes of awards (Breakthrough, Synergy, and Frontier)
 - Three on-going Frontier awards
 - CAREER awards



Smart Systems: Sensing, Computation, and Control

Environment Sensing

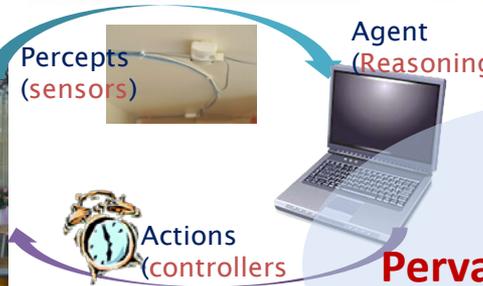


Percepts (sensors)

Agent (Reasoning)

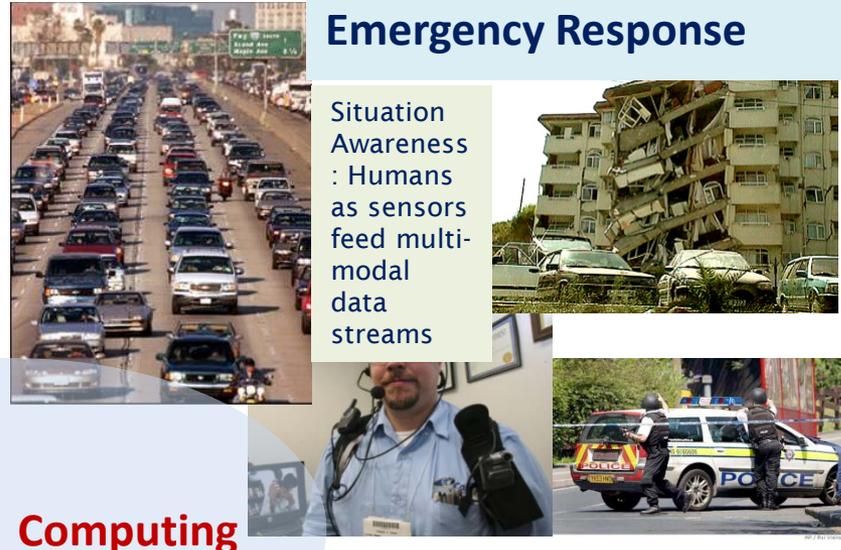
Actions (controllers)

Pervasive Computing



Emergency Response

Situation Awareness : Humans as sensors feed multi-modal data streams



Computing

People-Centric Sensing

Social

Personal Sensing

Public Sensing

Social Sensing



Informatics

Temperature, light, microphone

ECG

Blood pressure

SpO₂, GSR

Accelerometer

Smart Health Care

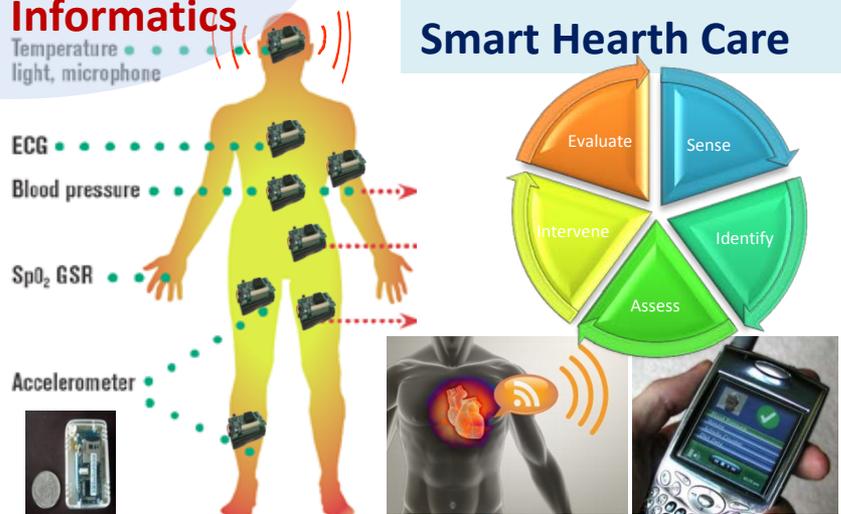
Evaluate

Sense

Intervene

Identify

Assess



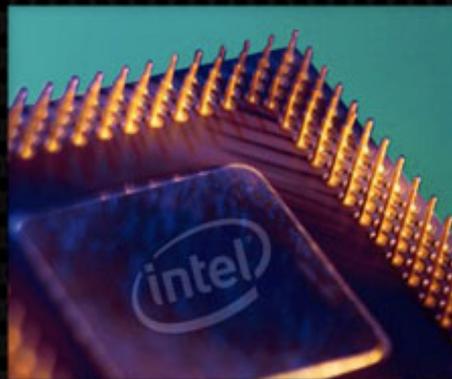



However...

A CPS-enabled vision of the future is only possible if we can first (fundamentally) assure **security** and **safety**.



How can we design, build and verify reliable, predictable, safe and **secure** cyber-physical systems upon which people can - and will - bet their lives?



A World of Cyber Threats

- DDoS attacks
- Worms
- Trojan Horses
- Spyware
- Botnets
- Phishing
- Insider misuse
- Data theft



How do these impact behaviors of cyber physical systems? What are trust boundaries?



Why is the Cyber Security Challenge so Difficult?

- **Attacks and defenses co-evolve:** a system that was secure yesterday might no longer be secure tomorrow.
- The technology base of our systems is frequently updated to improve functionality, availability, and/or performance. **New systems introduce new vulnerabilities** that need new defenses.
- The **environments** in which our computing systems are deployed and the functionality they provide are **dynamic**, e.g. cloud computing, mobile platforms.
- The **sophistication** of attackers is increasing as well as their sheer **number** and the **specificity** of their targets.
- As **automation pervades new platforms**, vulnerabilities will be found in critical infrastructure, automotive systems, medical devices.
- Cyber security is a **multi-dimensional** problem requiring expertise from CS, mathematics, economics, behavioral and social sciences.





Physical systems are increasingly complex and cyber-enabled.

As our dependency on cyber-physical systems grows, so does the need to secure those systems – as well as develop strategies and technologies to respond to security threats.



Cyber-Physical Security Risks

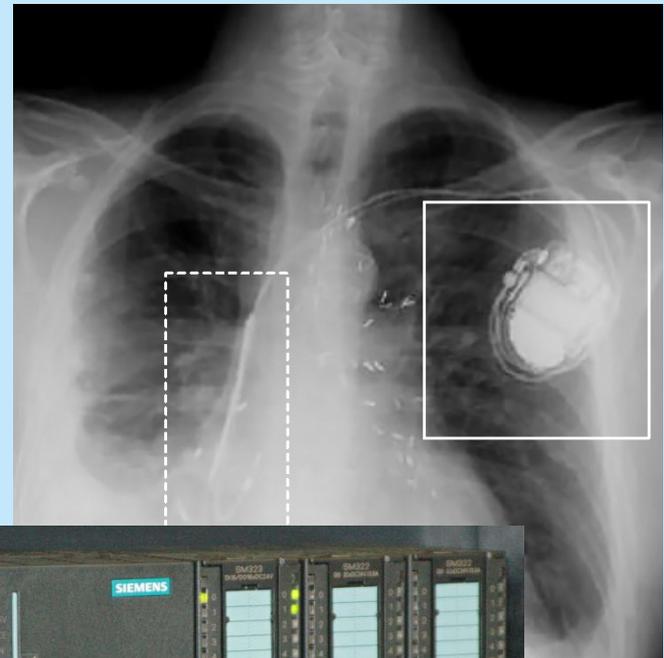


Law Enforcement Communications



Automobiles

Embedded Medical Devices

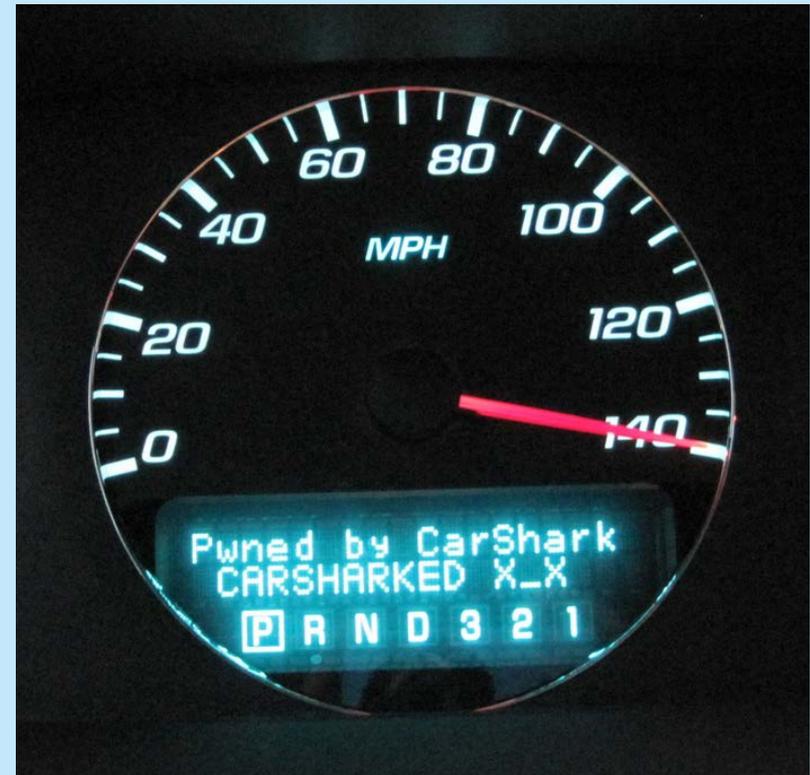


Control Systems



Security Risks in Automotive Computers and Networks

- Computer scientists and engineers have demonstrated ability to remotely take over automotive control systems
- In one case, by connecting to a standard diagnostic computer port included in late-model cars, caused disruption to brakes, speedometer reading, and vehicle telematics
- They are now working with the automotive industry to develop new methods for assuring the security as well as safety of automotive electronics



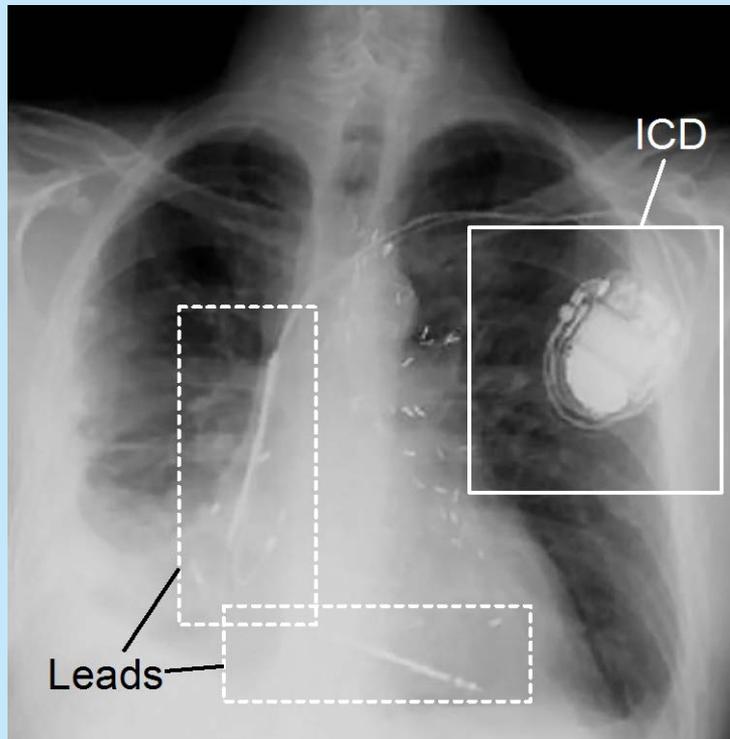
This car was not moving

Stefan Savage (UC San Diego) and Tadayoshi Kohno (U Washington)

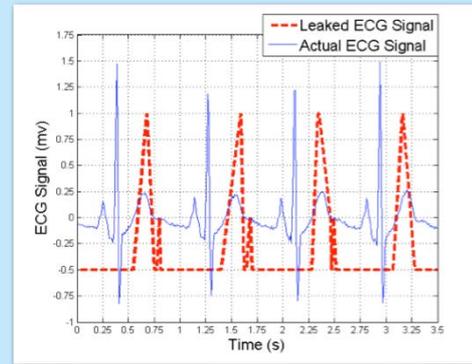


Medical Device Security

As of 2006, more than half of medical devices on the US market now contain and trust software.



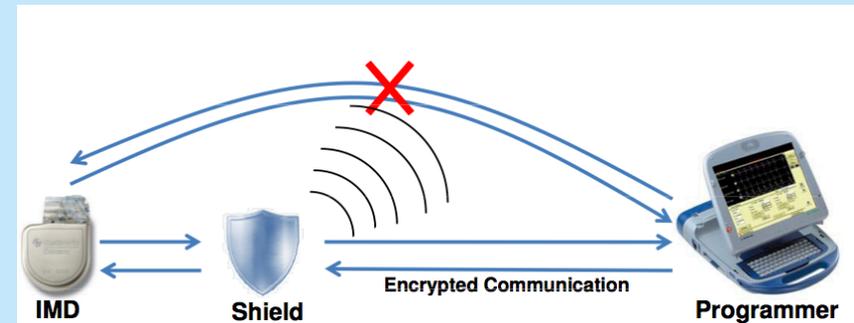
Defibrillator Vulnerabilities,
Zero-Power Defenses
[Halperin et al., IEEE S&P '08]



Telemedicine Privacy
[Salajegheh et al., J. Med. Dev. '09]



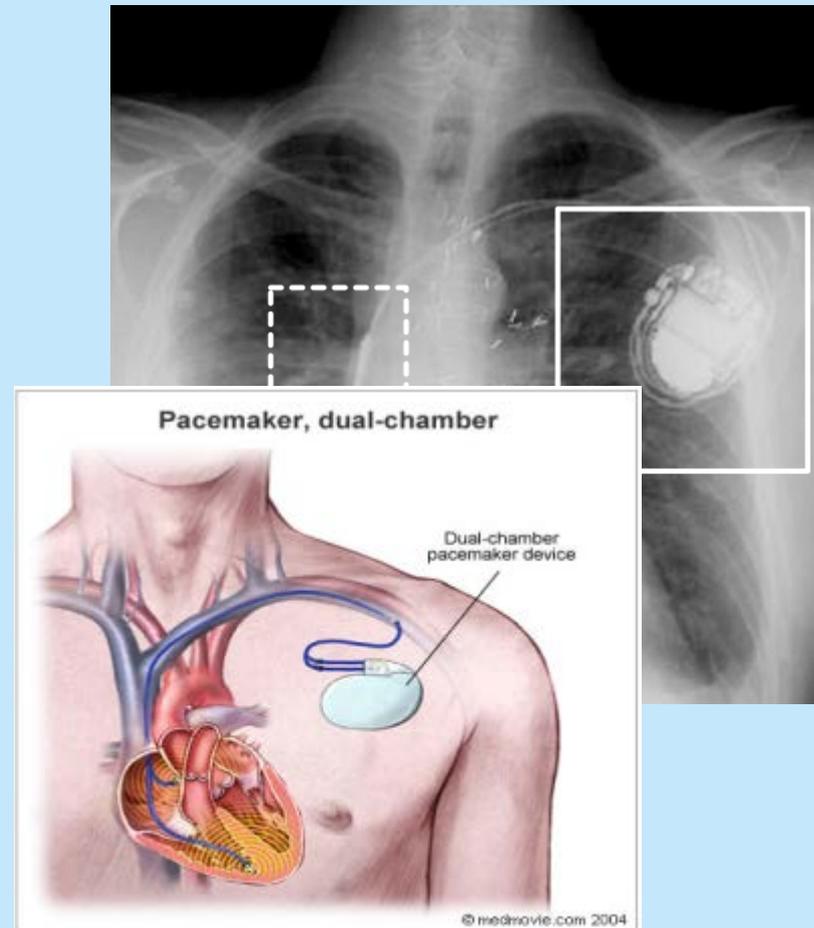
AED Security
[Hanna et al., HealthSec '11]



Radio Shield/Jamming for Implants
[Gollakota et al., ACM SIGCOMM '11]

Implantable Medical Device Security

- Implanted medical devices frequently incorporate wireless control
- By gaining wireless access to a combination heart defibrillator and pacemaker, were able to reprogram it to shut down and to deliver jolts of electricity
- Attack vector: the device test mechanism, wireless communication interface with a control mechanism that was unencrypted
- Computer scientists working with physicians found new ways to secure these devices against extraneous signals and wireless attacks
- Encryption but also “cloakers” – make your implants “invisible” at your discretion



PI: Kevin Fu, UMass – Amherst

[Halperin et al., IEEE Symposium on Security & Privacy 2008]

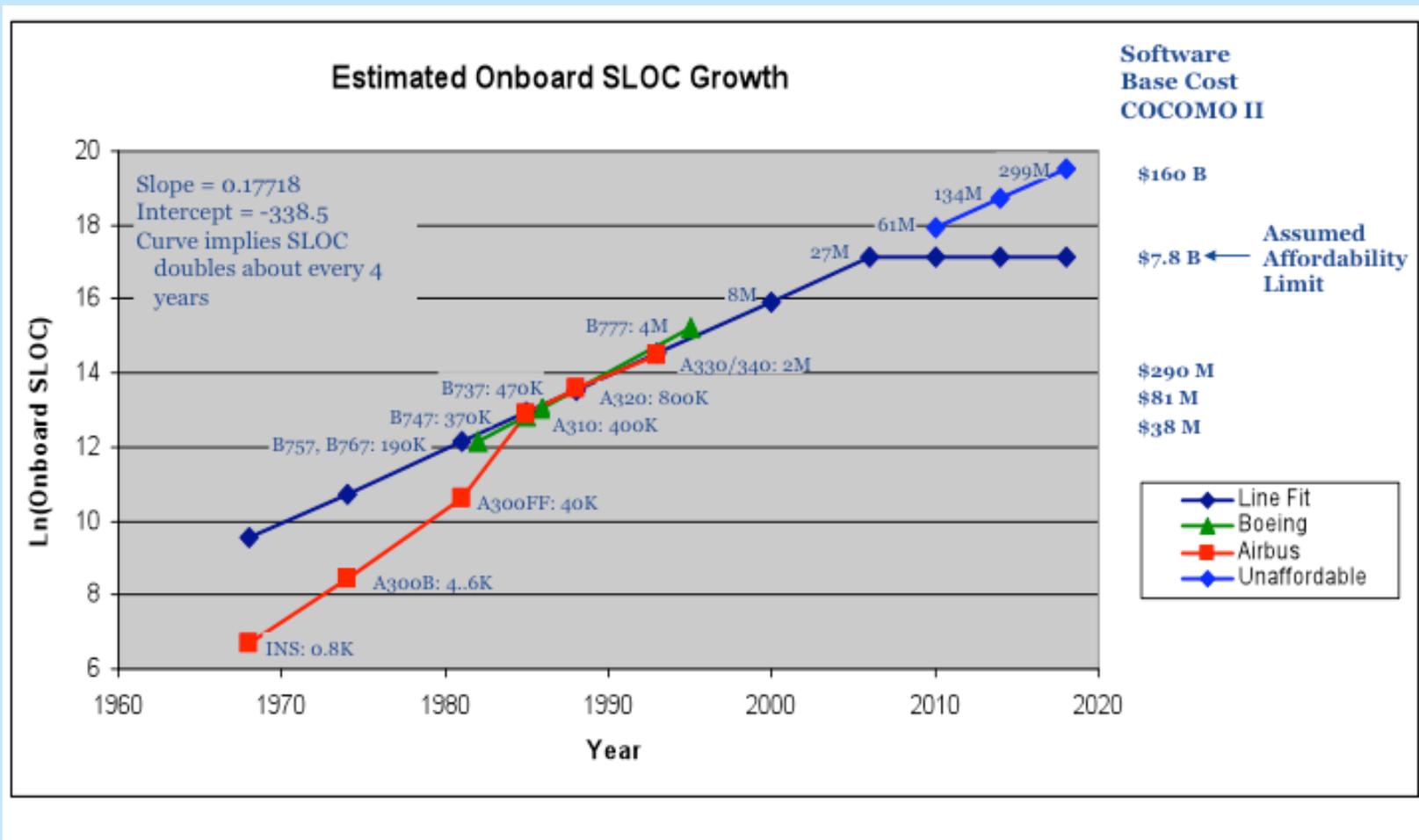


How Much SW in Medical Devices?

- 1983-1997
 - 6% of all recalls attributed to SW
- 1999-2005
 - **Almost doubled:** 11.3% of all recalls attributed to SW
 - 49% of all recalled devices relied on software (up from 24%)
- 1991-2000
 - **Doubled:** # of pacemakers and ICDs recalled because of SW
- 2006

 - Milestone: Over half of medical devices now involve software
- 2002-2010
 - 537+ recalls of SW-based devices affecting 1,527,311+ devices

Increasing Complexity of Aerospace CPS



Ref: Virtual Integration for Improved System Design, Proceedings of the First Analytic Virtual Integration of Cyber Physical Systems Workshop in conjunction with RTSS 2010, prepared by David Redman, Donald Ward, John Chilenski, and Greg Pollari, https://wiki.sei.cmu.edu/aadl/images/d/de/SAVI_Virtual_Integration-AVICPS2010.pdf



SCADA Security

- Targets industrial control systems, such as power plants
- Enters an organization thru an infected removable drive
- Zero-day exploits
- Anti-virus evasion techniques
- P-2-P update propagation
- Reprogramming PLC code
- Sophisticated exploitation of attack surface for a CPS

The New York Times

How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION

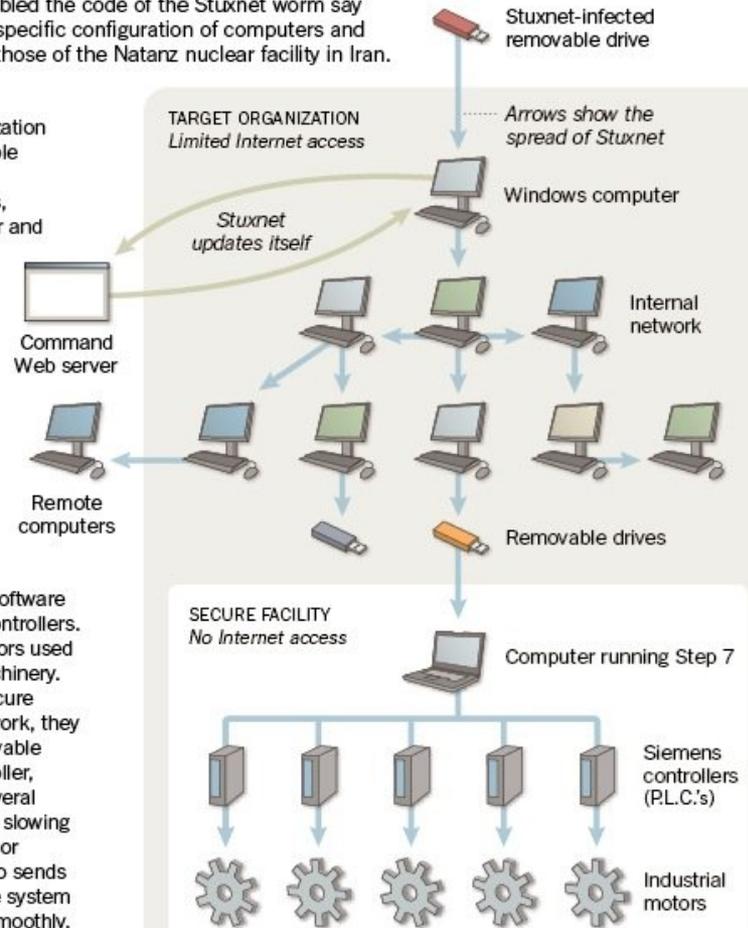
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD

If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

FINAL TARGET

Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.



Source: Symantec

THE NEW YORK TIMES



Why is CPS Security Different?



CPS Security Considerations

- Systems are frequently processor and network constrained
 - Solutions need to be lightweight
 - Enterprise approaches may not be very applicable
- Frequently human operated – but not with a system administrator
 - Security decisions may have enormous impact (economic and safety)
 - Solutions need low false positives – operator is being doing other things
- Systems not always connected
 - Update of security solution not always easy
- Is the physical world “our friend” for CPS security

The key issue: How do we defend. What are general principles for resilience / mission assurance



CPS Security Opportunities – from 2014 CPS Solicitation

- ***System Design*** -- How do we design CPS to be ***safe, secure, and resilient*** in a variety of unanticipated and rapidly evolving environments and disturbances? How do we integrate privacy and security into CPS design?
- **Additional DHS / HSARPA focus areas**
 - Particular interests in security technologies relevant to cyber-physical systems.
 - CPS related to transportation, emergency response, energy, and healthcare are considered especially relevant for HSARPA

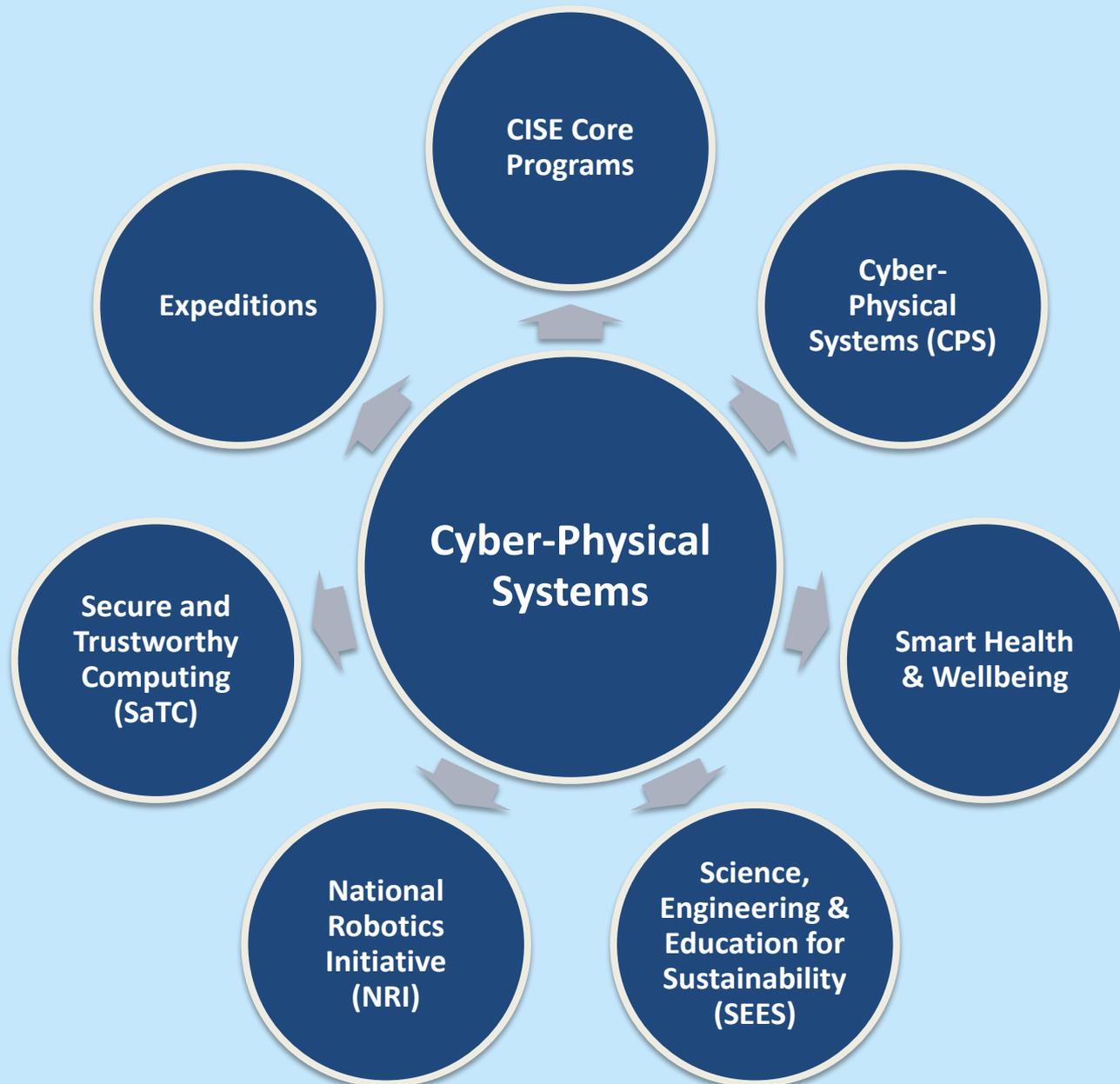


CPS Program has Strong and Growing Interest in CPS Security

- Presentations at ACSAC and CPS Week 2014
- CPS 2014 Solicitation
 - Approximately 3 x CPS security focused proposals (as compared to 2013)
 - DHS S&T partnership
 - CPS FY 2015 solicitation in the works
- NSF / Intel Partnership on CPS Security (NSF 14-571)
 - Ideas Lab joint with Secure and Trustworthy Computing program
 - Proposals due 28 Oct
 - <http://www.nsf.gov/pubs/2014/nsf14571/nsf14571.htm>
- Secure and Trustworthy Computing Core Solicitation – FY 2015 is out



CPS Support across NSF



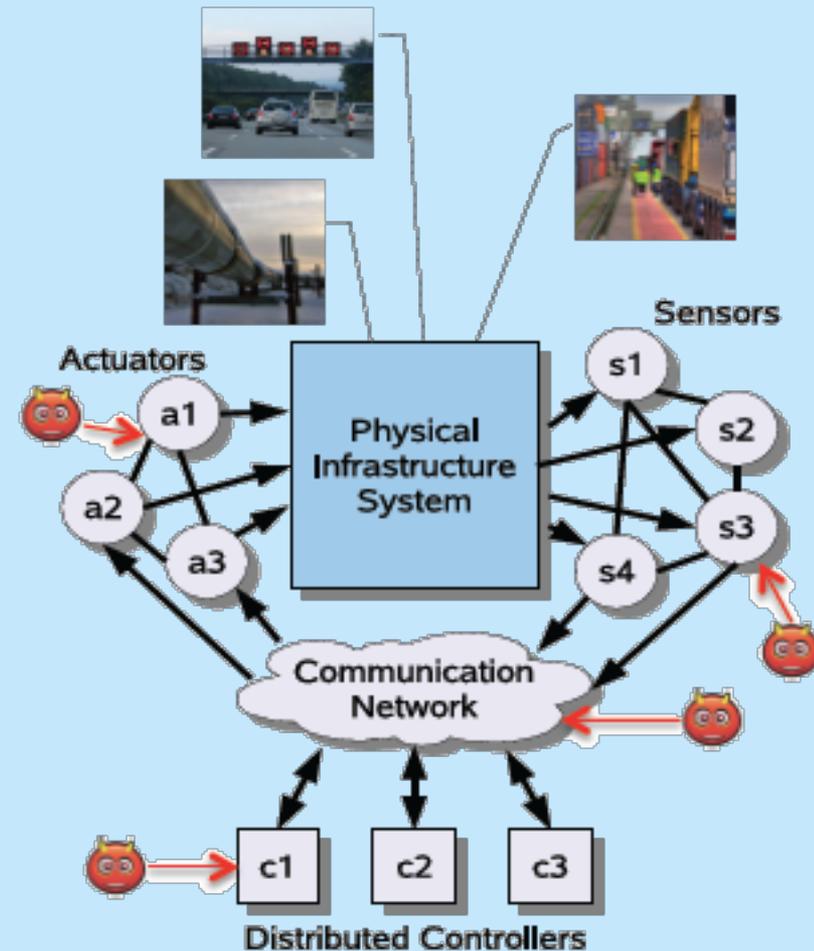
Some Example CPS Security and Resilience Activities



Foundations of Resilient Cyber Physical Systems

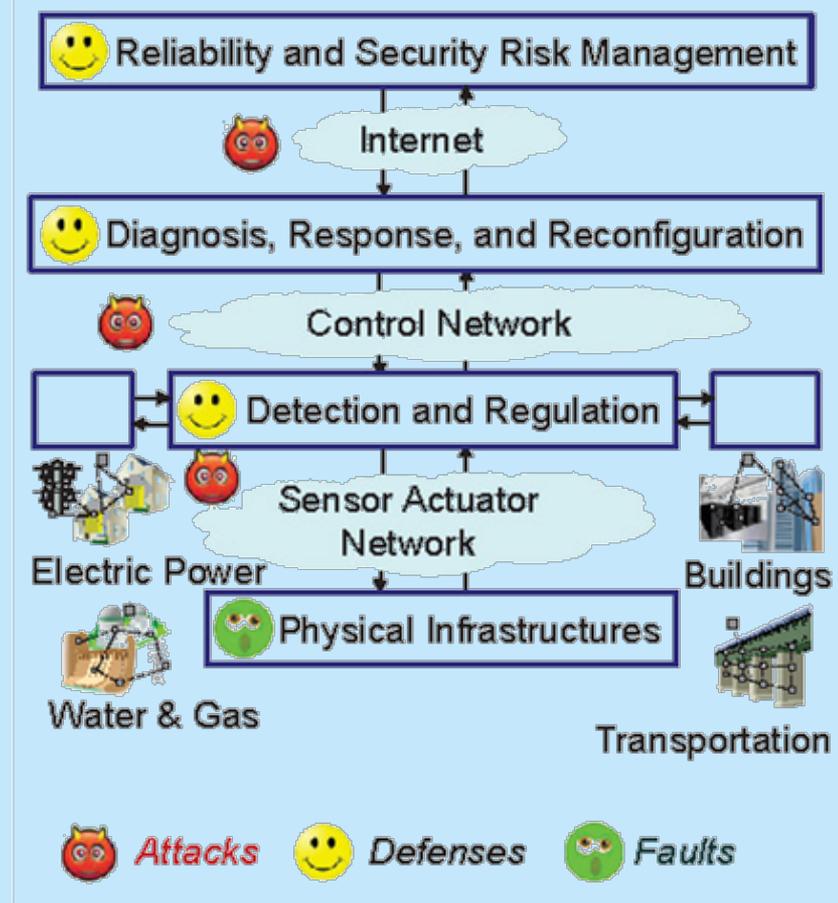
Key Drivers for Resilient CPS

- Attributes of Resilience
 - Functional correctness (by design)
 - Robustness to *reliability* failures (faults)
 - Survivability against *security* failures (attacks)
- Challenges to Resilience
 - Spatio-temporal dynamics
 - Many strategic interactions with network interdependencies
 - Inherent uncertainties (public & private)
 - Tightly coupled control and economic incentives



FORCES Research Focus for CPS

- Resilient Control
 - Threat assessment & detection
 - Fault-tolerant & attack diagnostics
 - Real-time predictive response
 - Model-based design
- Economic Incentives
 - Incentive (game) theory for resilience
 - Mechanism design
 - Interdependent risk assessment
 - Insurance & risk distribution



Smart Roads – Smart America Challenge 2014

**Vanderbilt University - Institute for Software-Integrated Systems
UC Berkeley – NSF FORCES and Connected Corridors Projects**





SMARTROADS



NSF FORCES and Connected Corridors Projects, UC Berkeley Institute for Software-Integrated Systems, Vanderbilt University

The Smart Roads testbed / system integrates advanced control algorithms and high-fidelity simulation software with real-time data to *predict* and *manage* traffic flows, to support resilience to cyber attacks.

The Status Quo:



Complex and interconnected road networks

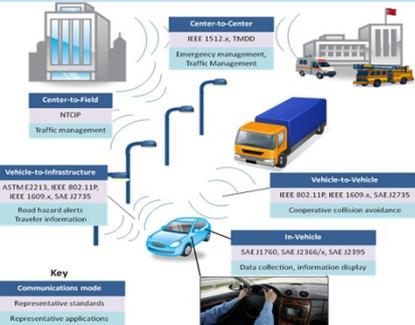


Emergency vehicles delayed due to traffic



World's largest traffic jam: 100+ Km/10+ days

Vulnerable Communication & Control:



FHWA ITS Connections



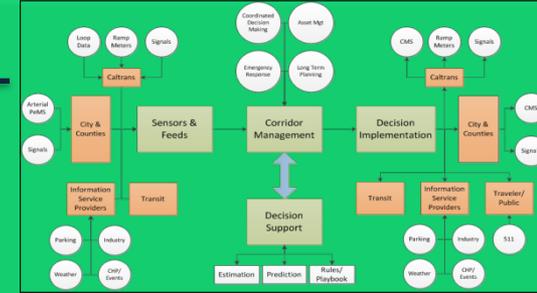
Cobweb of global critical IT Infrastructure

Our Solution:

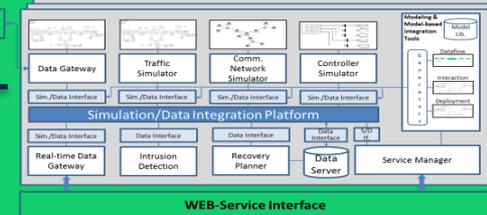
Connected Corridors (CC)

+

High-fidelity simulation software (C2WT)



Cloud-Deployed Model-based Integration Platform Instances



Testbed Integration Center



Well-managed and resilient traffic flows

Cyber Attacks



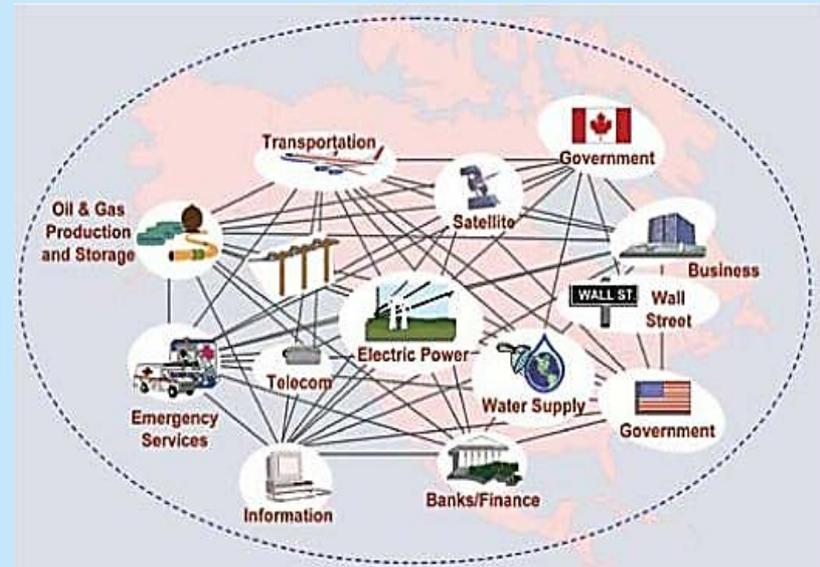
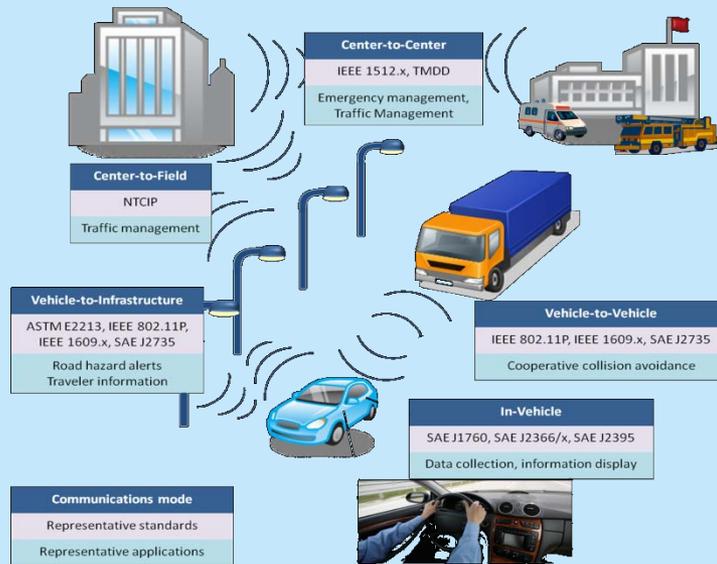
Connected Corridors

- The “next generation” of Integrated Corridor Management is being developed and ultimately piloted on a congested, urban freeway and arterial network in Southern California by **UC Berkeley** and a team of transportation agency and jurisdictional partners. Called Connected Corridors, it takes ICM to a new level by integrating freeway and arterial operations.
- **How?** The freeway ramps and arterial traffic signals will talk to each other, and decisions will be made via playbook scenarios, about what to do during incidents and events in near “real time.”



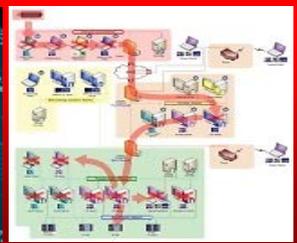
Coordination and Control ... need networks....

Vulnerable Communication & Control:



Highway IT Connections ←| |→ Global web of critical IT infrastructure

Cyber Attacks



CPS Testbed

- The CPS testbed / system integrates **advanced control algorithms** and high-fidelity **simulation software** with real-time data to *predict* and *manage* traffic flows, to support resilience to cyber attacks.

▶ Use cases

Off-line

- ▶ High-fidelity simulation of road traffic, based on real data
- ▶ Development and evaluation of novel control algorithms – before they are applied
- ▶ Study of cyber effects on the networks and on the system
- ▶ Training of system operators in preparation for emergencies

On-line

- ▶ Real-time monitoring of traffic and predictive simulation
- ▶ Real-time control of traffic by ramp metering
- ▶ Real-time situational awareness about the status of the network



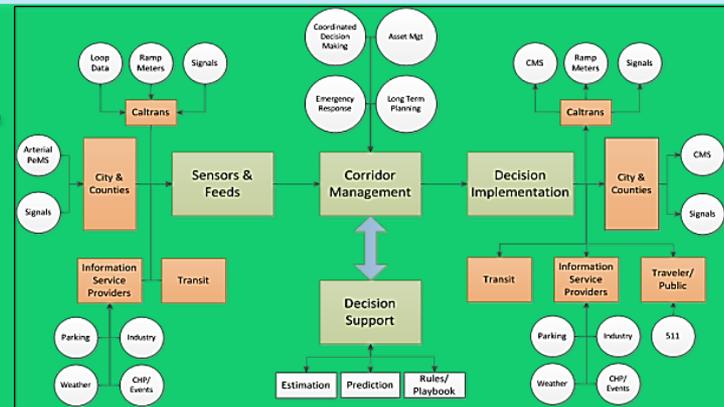
Integrated CPS Testbed

Our Solution:

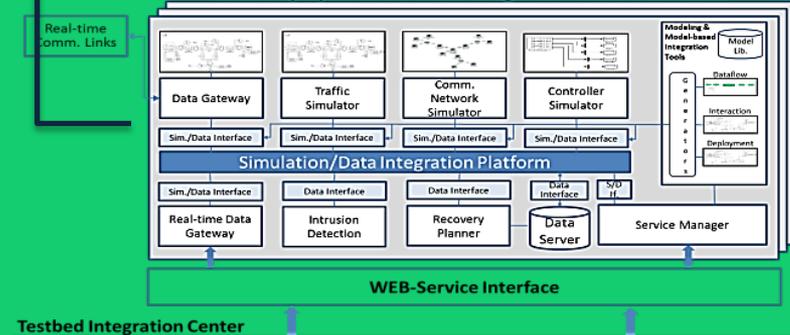
Connected Corridors
(CC)

+

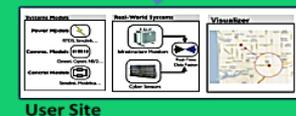
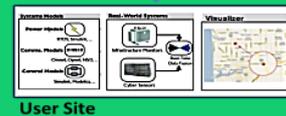
High-fidelity
simulation software
(C2WT)



Cloud-Deployed Model-based Integration Platform Instances



Testbed Integration Center



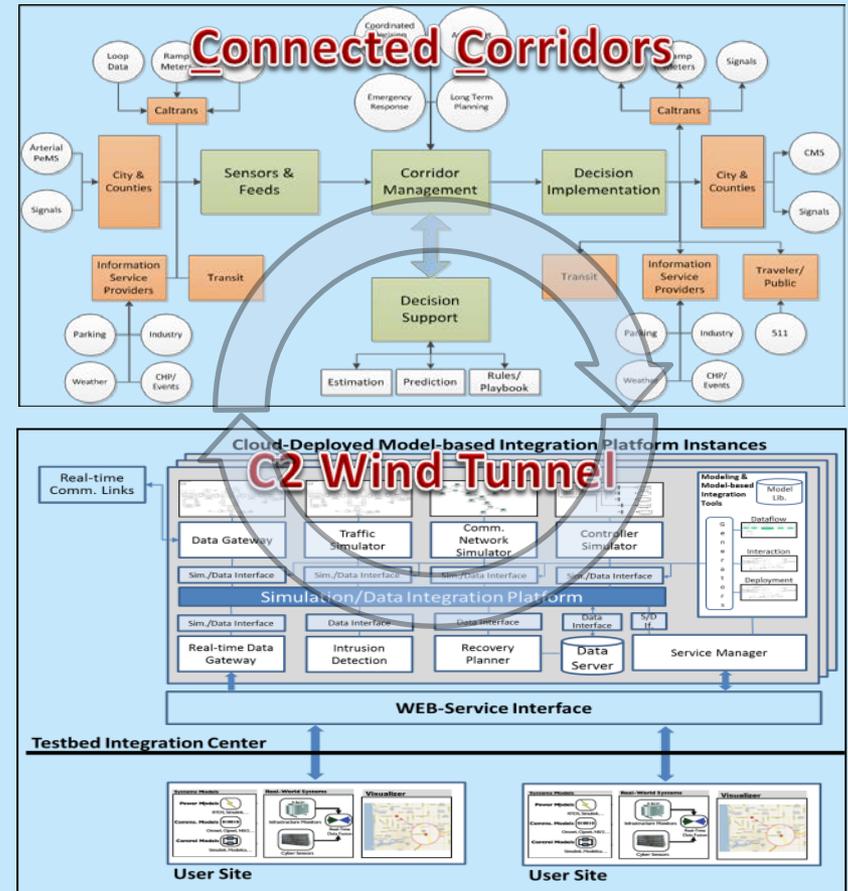
Well-managed and resilient traffic flows



Smart Roads – Demo at Smart America

Working prototype of a Smart Transportation System, working on real data collected from a segment of an interstate highway near a major city that shows

- 1) how the CPS improves the experience on the road,
- 2) how a cyber-attack could degrade that experience, and
- 3) how trained operators and clever algorithms can recognize and mitigate the effects of the attack, leading to recovery.



Smart Roads Benefits

- Projects such as Coordinated Corridors will
 - improve quality of life for residents and commuters in urban corridors by decreasing greenhouse gas emissions;
 - encourage use of public transportation; and
 - move all types of traffic more efficiently (including autos, buses, trucks, and delivery vehicles) thus keeping workers and the economy moving.
- But with cyber-security ... communities reap additional benefits: preventing cyber-attacks before they happen, informing decision-makers if by some chance a cyber-attack does get through the system, and even potentially enabling the system to take required actions to counter the attack, allowing system recovery to occur much more quickly.



Foundations of Secure Cyber Physical Systems

- Cyber-physical systems regulating critical infrastructures, such as electrical grids and water networks, are increasingly geographically distributed, necessitating communication between remote sensors, actuators and controllers
- Combination of networked computational and physical subsystems leads to new security vulnerabilities that adversaries can exploit
- Approach: design new secure protocols and architectures for CPS through a unified conceptual framework - models for the physical system and the communication/computation network to define precise attack models and vulnerabilities
- Models are used to design protocols with provable security guarantees, thus enabling the design of more trustworthy architectures and components
- Applications: smart buildings, transportation networks, and smart grids

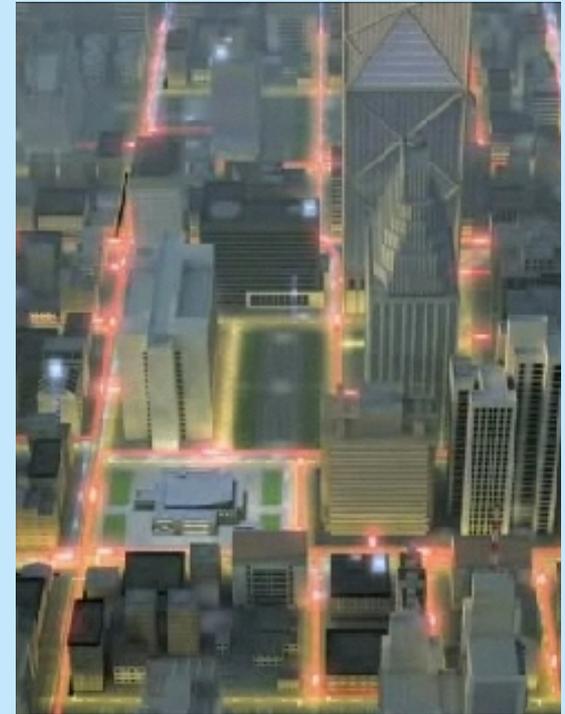


Image Credit: Cisco, Inc.



Enabling Smart Systems for the Future

- Many of tomorrow's **breakthroughs** will occur at the **intersections of diverse disciplines**.
- We need to invest in a **research pipeline** comprising of long-term foundational research for cyber-physical systems, experimental prototypes, and early deployments to spur innovative applications.
- The CPS R&D community will continue to have a **transformative and durable impact** on our national priorities.
- We, working with other federal agencies, are committed to foster this emerging, consolidating research community and to reinforce its sustained role in advancing **frontiers of science and engineering innovation**.
- A **vibrant discovery and innovation ecosystem** is critical to success





Thanks!

dcorman@nsf.gov

