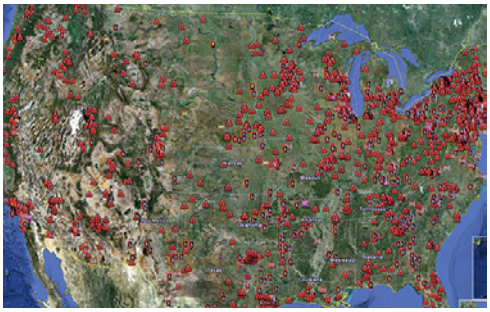
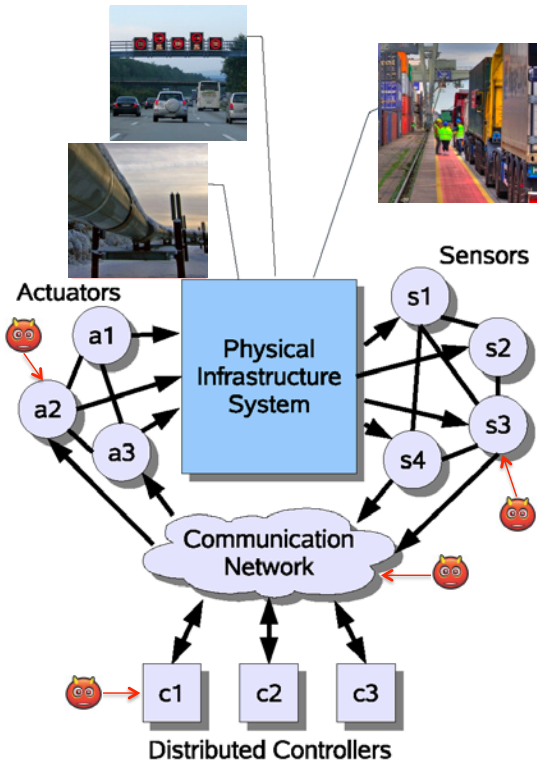
Resilient Cyberphysical Systems

Cyberphysical systems (CPSs) are being increasingly deployed in critical infrastructures such as electric power, water, transportation, and other networks. These deployments are facilitating real-time monitoring and closed-loop control by exploiting advances in wireless sensor-actuator networks, the Internet of Everything, data-driven analytics, and machine-to-machine interfaces. CPS operations depend on the synergy of computational and physical components. In addition, in many cases, CPSs also interact with human decision makers. Fundamentally, once we admit that CPS operations depend on actions of humans (albeit to different degrees), we also have to admit that malicious entities could take charge of CPS control by exploiting cyber insecurities or physical faults, or their combination. Therefore, to improve CPS resilience, we need diagnostic tools and automatic control algorithms that ensure survivability in the presence of both security attacks and random faults and include models of the incentives of human decision makers in the design process.



In December 2012, the U.S. Department of Homeland Security released a map of approximately 7,200 control system devices that appear to be directly linked to the Internet and are vulnerable to attack.

Cyberphysical Systems



Cyber attacks on CPS control elements can result in the loss of availability (denial-of-service attack) and/or integrity (deception attack) of safety-critical measurement and control data.

Cyber Vulnerabilities in CPS

Recent incidents (e.g., the Stuxnet attack) confirm that control systems for critical infrastructures are targets of highly motivated teams of attackers with access to ample financial and technical resources.

Cyber vulnerabilities arise in CPSs due to:

- Wider deployment of off-the-shelf information technology (IT) devices. CPSs inherit the vulnerabilities of these devices and thus are subject to software bugs and hardware failures.
- Replacement of proprietary protocols and closed networks with standard open Internet protocols and shared networks. Malicious attackers capable of exploiting protocol and network insecurities can target CPS operations.
- Generation, use, and modification of CPS data by multiple parties. This poses new challenges in access control and authorization among the strategic players, such as the operators, the IT vendors, and the end users.
- The presence of a large number of remotely accessible field devices. Thus, sensor-control data becomes prone to adversarial manipulation.

Contributors: Saurabh Amin, MIT, USA; Galina Schwartz and S. Shankar Sastry, University of California, Berkeley, USA

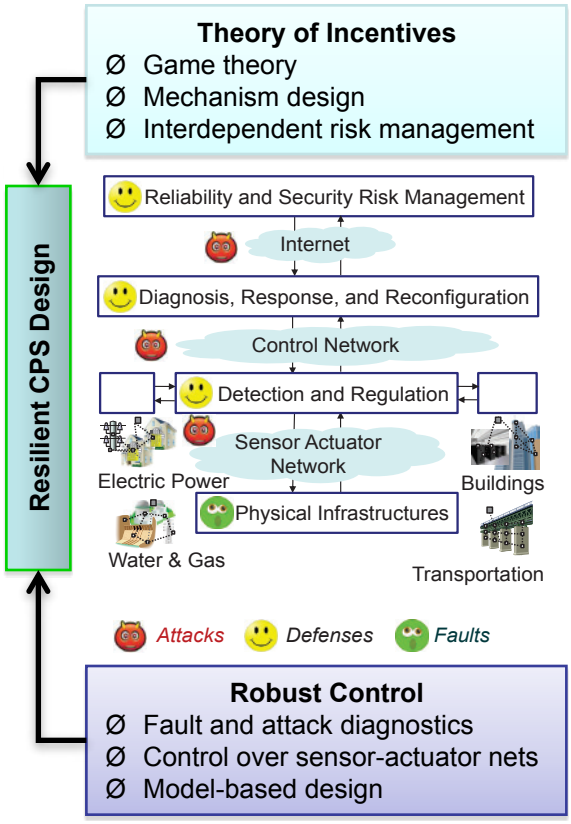
From: *The Impact of Control Technology*, 2nd ed., T. Samad and A.M. Annaswamy (eds.), 2014. Available at www.ieeecss.org.

Control and Incentive Tools for Resilient CPS Operation

Resilient operation of CPSs requires the following high-confidence attributes: functional correctness (by design) for real-time operations, robustness to reliability failures (fault tolerance), and survivability even during successful attacks (operation through attacks). Designers and operators of CPSs currently lack comprehensive tools for resilient operation. Major challenges include: (1) spatiotemporal and hybrid dynamics of cyberphysical processes; (2) a large number of interactions with interdependencies; and (3) effects of public and private uncertainties. Notably, two distinct domains of tools have emerged to respond to these challenges:

- Robust control over networks: These tools primarily address safety and performance issues in closed-loop control over sensor-actuator networks.
- Theory of incentives: These tools provide ways to analyze and influence the strategic interactions of human decision makers.

To date, control and incentive tools have been designed and implemented separately. This separation was natural due to the lack of advanced CPS technologies in legacy supervisory control and data acquisition (SCADA) systems. Modern CPSs no longer permit such separation of control and incentive tools. The failure of loosely coupled tools in ensuring resilient operation of CPSs is evident in chronically unresolved design conflicts between efficiency and robustness against faults and attacks and the lack of proper incentive structures to enable private entities (or players) that operate the CPSs to maintain resilience. Consequently, control and incentive tools designed in isolation, or without cognizance of strategic interactions between private entities and interdependent processes in CPSs, are inadequate to maintain resilience.



The challenge of resilient CPS design: *The development of an integrated resilient design methodology necessitates a rigorous analytical framework to allow the co-design of control and incentive tools. This framework will enable designers and operators to build resilience into CPSs by maintaining synergistic integrations of human-centric elements with automated diagnostic and control processes.*

Emerging CPSs for Transportation and Electricity Infrastructures	Tools Based on Robust Control Theory	Tools Based on the Theory of Incentives
Active road traffic management	Distributed sensing and control	Congestion pricing and incentives
NextGen air traffic operations	Robust scheduling and routing	Strategic resource reallocation
Smart electricity transmission	Wide-area monitoring	Contractual design
Power markets, including nondispatchable generators	Risk-limiting dispatch	Market design
Smart electricity distribution	Distributed load control	Demand response schemes
Energy-efficient building operations	Predictive control of devices	Energy-saving incentives

For more information, visit http://ics-cert.us-cert.gov, http://www.gao.gov/products/GAO-12-926T, http://www.nist.gov/itl/cyberframework.cfm, http://www.nist.gov/el/smartgrid/cybersg.cfm, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, and http://en.wikipedia.org/wiki/Stuxnet.