Opening Remarks

Cybersecurity in Cyber-Physical Systems Workshop
hosted by
NIST Information Technology Laboratory
April 23-24, 2012

George W. Arnold, Eng.Sc.D.
Director, Smart Grid and Cyber-Physical Systems Program
Office
Engineering Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce
NIST At A Glance

Gaithersburg, MD

- NIST Research Laboratories
- Manufacturing Extension Partnership
- Baldrige Performance Excellence Award
- Technology Innovation Program

Boulder, CO

~ 2,900 employees
~ 2,600 associates and facility users
~ 1,600 field staff in partner organizations
~ 400 NIST staff serving on 1,000 national and international standards committees
The NIST Laboratories

NIST’s work enables
• Advancing manufacturing and services
• Helping ensure fair trade
• Improving public safety and security
• Improving quality of life

NIST works with
• Industry
• Academia
• Other agencies
• Government agencies
• Measurement laboratories
• Standards organizations

Providing measurement solutions for industry and the Nation
Smart Grid: An Example of a CPS

NIST Smart Grid Reference Model
Smart Manufacturing: Another CPS Application

Smart Manufacturing refers to manufacturing production systems at the equipment, factory, and enterprise levels that integrate cyber and physical systems by combining:

- **smart operating systems** to monitor, control, and optimize performance
- **systems engineering-based** architectures and standards, and
- **embedded and/or distributed** sensing, computing, communications, actuation, and control technologies

...to enable **innovative production, products, and/or systems of products** that enhance **economic and sustainability performance**
Definition of Cyber-Physical Systems

Function:
Cyber physical systems are hybrid networked cyber and engineered physical elements co-designed to create adaptive and predictive systems for enhanced performance*

Essential Characteristics:
• Co-design treats cyber, engineered, and human elements as integral components of a functional whole system to create synergy and enable desired, emergent properties
• Integration of deep physics-based and digital world models provides learning and predictive capabilities for decision support (e.g., diagnostics, prognostics) and autonomous function
• Systems engineering-based architectures and standards provide for modularity and composability for customization, systems of products, and complex or dynamic applications
• Reciprocal feedback loops between computational elements and distributed sensing/actuation and monitoring/control elements enables adaptive multi-objective performance
• Networked cyber components provide a basis for scalability, complexity management, and resilience

*Performance metrics include safety and security, reliability, agility and stability, efficiency and sustainability, privacy
CPS Application Sectors and Benefits

Application Sectors:

- **Manufacturing** (includes smart production equipment, processes, automation, control, and networks; new product design)
- **Transportation** (includes intelligent vehicles and traffic control)
- **Infrastructure** (includes smart utility grids and smart buildings/structures)
- **Health Care** (includes body area networks and assistive systems)
- **Emergency Response** (includes detection and surveillance systems, communication networks, and emergency response equipment)
- **Warfighting** (includes soldier equipment systems, weapons systems and systems of systems, logistics systems)

Benefits:

- Improved quality of life and economic security through innovative functions, production, products, and/or systems of products
NIST CPS Context

- Growing demands on NIST for standards associated with smart systems applications
  - Smart Buildings, Smart Grid and Infrastructure, Smart Manufacturing, Smart Health Care, Smart Transportation, ...
- NIST has responded with programs in individual domain areas
- Significant crosscutting technology gaps and fundamental research challenges exist
- Potential impact on manufacturing: Innovative new classes of manufactured products, systems of products, and production systems
CPS Platform Technology Gaps and R&D Grand Challenges

• **Platform Technology Gaps** (Systems-Engineering Based Architectures and Standards)
  – Modularity and composability
  – Deep-physics and digital world model integration
  – Control, communications, and interoperability (adaptive and predictive; time synchronization)
  – Cyber-security
  – Scalability, complexity management, and resilience (integration with legacy systems)
  – Wireless sensing and actuation
  – Validation and verification; assurance and certification (software, controls, system)

• **R&D Grand Challenges**
  – Co-designing hybrid networked systems with integrated cyber, engineered, and human elements
  – Synthesizing and evolving complex, dynamic systems with predictable behavior (diagnostics, prognostics); anticipating emergent behaviors arising from interactions
  – Multi-scale, multi-physics modeling across discrete and continuous domains
  – Incorporating uncertainty and risk into reasoning and decision-making
  – Modeling and defining levels of autonomy and optimizing role of the human
  – Enabling education and workforce development; technology transfer
NIST CPS Actions

- NIST CPS Working Group (EL, ITL, SCO, OLES; January 2011)
- Cooperative Agreement with UMD for CPS research (Kick-off December 2011)
  - Book assessing state-of-the-art
  - Market analysis to guide R&D investments
  - Platform-based architecture and standards framework
  - Fundamental research in modeling and synthesis
- Short Course for Executives delivered by world class industry and research leaders (January 19-20, 2012)
- Cyber-security for Cyber-Physical Systems Workshop (April 23-24)
- Planned CTO Roundtable (June 2012)
Cybersecurity of CPS: New Challenges

- Need to address all the conventional aspects of cybersecurity, plus
- New issues and threats, e.g.
  - Complex software with non-deterministic behavior
  - Precise timing requirements
  - Cyber system as a threat vector for attack on the physical system rather than the object of attack