CYBER PHYSICAL SYSTEMS

[PARTLY ADAPTED FROM SLIDES BY PROF. INSUP LEE, UPENN]

CS 525 C

Instructor: Krishna Venkatasubramanian
CPS Introduction: Outline

- Computing trends
- Cyber Physical Systems
  - Why research CPS?
  - Grand Challenges of CPS
- CPS Characteristics
- CPS Challenges
Computing History

• Mainframe computing (60’s-70’s)
  • Large computers to execute data processing applications

• Desktop computing & Internet (80’s-90’s)
  • One computer at every desk to do business/personal activities

• Ubiquitous computing (00’s)
  • Numerous computing devices in every place/person
  • “Invisible” part of the environment
  • Information anywhere, anytime
Trend 1: Data/Device Proliferation (By Moore’s Law)

- **Medical Devices**
- **Sensor Networks**
- **Industrial Systems**
- **Portable Smart Devices**

Unattended Multihop ad-hoc wireless
Embedded Everywhere
Trend 2: Integration at Scale
(Isolation has cost!)

World Wide Sensor Web

Smart Building Environment

Future Combat System

Low End

Ubiquitous embedded devices
- Large-scale networked embedded systems
- Seamless integration with a physical environment

High End

Complex systems with global integration
- Global Information Grid

Integration & Scaling Challenges
Trend 3: Biological Evolution

The exponential proliferation of embedded devices (afforded by Moore’s Law) is not matched by a corresponding increase in human ability to consume information!

Increasing autonomy (human out of the loop)
Confluence of Trends

#1. Data/Device Proliferation

#2. Integration at Scale

#3. Autonomy (Human are not getting faster)

Distributed, Environment-coupled, Information distilling, Control systems
Cyber-Physical Systems

- Physical and engineered systems whose operations are **monitored, coordinated, controlled and integrated** by a computing and communication core.

- Tight coupling (coordination) between computational and physical resources

- Large-scale system of systems

- Exceeds today’s systems in adaptability, autonomy, efficiency, functionality, reliability, safety, and usability

- Convergence of computation, communication, information, and control
Why Cyber Physical Systems?

• CPS allow us to **add capabilities to physical systems**

• By merging computing and communication with physical processes, CPS brings many benefits:
  • **Safer and more efficient** systems
  • **Reduce the cost** of building and operating systems
  • Build complex systems that provide **new capabilities**

• Technological and Economic Drivers
  • The **decreasing cost of computation**, networking, and sensing
  • Computers and communication are ubiquitous, enables national or global scale CPSs
  • Social and economic forces require more **efficient use of national infrastructure**.
Example 1: Automotive Systems

- 100M lines of code (premium cars)
  - F22 Raptor ~2M
  - Boeing Dreamliner ~7M
- 100 ECUs
- Example: X-by-wire, adaptive cruise control, parking, lane departure warning and engine management driven by software
- Cost of electronics/software: 35% ~ 40% in premium cars (for hybrid it is even higher!)
Example 2: Manned and Unmanned Ariel Vehicles

Dreamliner
- ~1300 networked microprocessors
- 50% of design cost ($ and time)
- **Correctness** of software challenge
- Security an issue --- example GPS spoofing
Example 3. Health Care and Medicine

- **Home care: monitoring and control**
  - Pulse oximeters (oxygen saturation), blood glucose monitors, infusion pumps (insulin), accelerometers (falling, immobility), wearable networks (gait analysis), …
  - **Safety** challenge

- **Operating Room of the Future**
  - Smart alarms (e.g., X-ray + ventilator)
  - Closed loop monitoring and control; multiple treatment stations, plug and play devices; robotic microsurgery (e.g., oxygen + torch)
  - **System coordination** challenge
Example 4. Electric Power Grid

- **Current picture**
  - Equipment protection devices trip locally, reactively
  - Cascading failures: E.g., Aug (US/Canada) and Oct (Europe), 2003

- **Better future?**
  - Real-time cooperative control of protection devices
  - Or -- self-healing -- (re-)aggregate islands of stable bulk power (protection, market motives)
  - Ubiquitous green technologies
  - Issue: standard operational control concerns exhibit wide-area characteristics (bulk power stability and quality, flow control, fault isolation)
Example 5. Robotics

- Manufacturing and Logistics Robotics
- Medical and Healthcare Robotics
- Service Robotics
- A Roadmap for US Robotics from Internet to Robotics, CCC CRA, May 2009
Example 6: Everyday Objects...

- Smart Fridge that orders food
- Cooker that shows and cooks recipes
- Transparent Smart Window
Ultimately, CPS will transform how we interact with the physical world just like the internet transformed how we interact with one another.
Why a systematic study Cyber-Physical Systems is needed?
Environment-coupled nature

- Cyber-Physical Systems have computations and communication deeply embedded in and interacting with physical processes.

- Physical processes are inherently at a different time-scale than computational processes.
  - Problem becomes that of managing time, as time critical cyber processes can be made to wait by physical processes.
  - Example --- vital signs (heart beat).

- Physical processes may affect the cyber element in unexpected ways.
  - Example – tissue growth on implanted sensors that causes measurement inaccuracies leading to sub-optimal control of the physical process.

- Timeliness, safety, reliability, security, privacy, and adaptability all take on a different character.
Example: Ariane 5

- Unmanned rocket launched June 4th 1996
- Exploded 37 seconds into its flight
- 10 years $7 billion project
- Software error
- **Physical system/process** around the software changed
- Perfectly functional code ported from Ariane 4 rocket did not work
Other Examples: Auto Recalls

• **1.5M** (in US) Honda Accord, CR-V and Element vehicles recalled “to update the software that controls their automatic transmissions”

• **~75K** Toyota Hybrids recalled for “could enter a "fail-safe" mode that shuts down the engine, allowing only limited operation using the electric motor. The problem, caused by a software error in the Electronic Control Module (ECM) system, triggers up to five warning lights while shutting down the engine.”
More Auto Recalls

• ~8K Volvo S60 recalled to fix “software for fuel pump units, as the software was not compatible with all fuel pumps and components, resulting in insufficient fuel transfer in the pump units, which could cause the vehicle to stall.”
Interaction Complexity

• Cyber-physical systems are systems of systems
  • Composition of systems is about interactions of systems

  • One of the Three Mile Island investigators
  • A member of recent Nuclear Regulatory Commission (NRC) Study “Software for Dependable Systems: Sufficient Evidence?”

• Posits that sufficiently complex systems can produce accidents without a simple cause due to
  • interactive complexity and tight coupling
Interaction Complexity (contd..)

- A complex system exhibits complex interactions due to
  - **Unexpected interferences** that are not visible or not immediately comprehensible
  - Unfamiliar or **unintended feedback loops**
  - **Limited isolation** of failed components

- A complex system is tightly coupled when it has
  - **Rigidly ordered processes** (as in sequence A must follow B)
  - **Little slack in resources** (requiring precise quantities of specific resources for successful operation).
Example: Mars PATH Finder

• Landed on the Martian surface on July 4th, 1997
  • Unconventional landing – bouncing into the Martian surface

• A few days later, not long after Pathfinder started gathering meteorological data, the spacecraft began experiencing total system reset, each resulting in losses of data
Examples (contd..)

• Pathfinder has an “information bus” and a bus management thread [very critical – used by navigation, etc.] at high priority
• The meteorological data gathering thread ran as an infrequent, low priority thread, and used the data bus to publish its data (while holding the mutex on bus).
• A communication thread that ran with medium priority.
• Chain of events:
  • The meteorological data thread wants to put data on the information bus and locks it
  • This causes the information bus thread to block
  • Later when the communication task interrupted the meteorological data thread and executed ---- causing priority inversion.
  • After some time passed, a watch dog timer, noticing that the information bus had not been executed for some time concluded that something had gone really bad, and initiated a total system reset.
Other Examples: Medical Devices

- **25%** of all device recalls are bug related
- **1.5M devices** recalled in last 8 years
- Between 1999-2005 the number of recalls due to software problems **doubled**
- Example:
  - In 2011 Moog Medical ambulatory infusion pump recall “… due to a software anomaly which leads to software Error Code 45 (EC45), resulting in a shutdown of the pump. This failure may result in a delay or interruption of therapy, which could result in serious injury and/or death.”
Responsibility

How can we provide people and society with CPS that they can trust their lives on?

Partial list of CPS failures

- Denver baggage handling system ($300M)
- Mars Pathfinder (1997)
- Mars Climate Orbiter ($125M, 1999)
- The Patriot Missile (1991)
- USS Yorktown (1998)
- London Ambulance System (£9M, 1992)
- Pacemakers (500K recalls during 1990-2000)
- Numerous computer-related incidents with commercial aircrafts (http://www.rvs.uni-bielefeld.de/publications/compendium/incidents_and_accidents/index.html)

Trustworthy: reliable, safe, secure, privacy-preserving, usable, etc.
Observations

Old school approach to developing embedded systems --- viewing software independently from its environment --- does not work

Old school approach to developing embedded systems --- ad-hoc development and composition of complex systems --- does not work
CPS Grand Challenges

- **Zero automotive traffic fatalities**, injuries minimized, and significantly reduced traffic congestion and delays
- **Blackout-free electricity** generation and distribution
- **Energy-aware buildings**
- **Perpetual life assistants** for busy, older or disabled people
- **Location-independent access to world-class medicine**
- **Extreme-yield agriculture**
- **Reduce testing and integration time and costs** of complex CPS systems (e.g. avionics) by one to two orders of magnitude
- **Physical critical infrastructure that calls for preventive maintenance**
- **Self-correcting, self-certifying CPS** for “one-off” applications
CPS Characteristics

• Heterogeneity
  • Made up of diverse computational entities from sensors/actuators to large scale processing elements
  • E.g., datacenter

• Networked
  • Essential for coordinated and timely control of physical element
  • Often wireless

• Actuation
  • Can modify the physical environment through actuation
  • Closed-loop control, often with non-savvy people in the midst
  • E.g., pacemaker

• Mission Critical Deployment
  • Deployments in critical situation
  • E.g., health management, power grids
Operational Modes

Passive Mode
E.g., Monitoring enemy troop Movement in a battlefield

Autonomic Mode
E.g., Thermal Aware Scheduling in a Data Center

Active Mode
E.g., Artificial Pancreas with closed-loop control of the patient’s insulin
CPS Challenges

• **System Composition**
  - Building System of Systems
  - “Grand Theme” of CPS
  - Need to ensure that composed system is safe
  - Two approach: System-level composition, Co-design

• **Theory Modeling and Analysis**
  - Complexity of CPS high enough that mathematical model based engineering essential
  - E.g.: **Hybrid Systems** --- that consider both discrete and continuous time dynamics of underlying components of CPS
CPS Challenges

• Programming Abstractions
  • Functional behavior of CPS should be separated from requirements of timeliness, QoS, dependability etc.
  • **Model-based development**: Functionality should be stated using models — state machines, dataflow graphs — and code for the system should be generated automatically
  • Advantages: (1) easy to share designs, (2) detailed knowledge of target platform not needed
CPS Challenges

• **Architecture**
  - CPS are **Society-scale** systems
    - Reliability and Scalability are essential
  - **New network protocols** needed for connecting such large-scale, heterogeneous system of systems
    - Network delays minimized
    - Resource visualization essential
    - Real-time, group communication methods are needed
  - **Fault tolerance** has to be built in
    - Given uncertainties in the underlying physical process
• **Big Data**
  - All the data collected from the sensor-actuator systems in CPS needs to be processed efficiently
  - Techniques needed to ensure the results can be visualized easily by users
CPS Challenges

• Safety, Security and Privacy
  • Primary aim of all CPS design
    • Ensure no harm comes to the underlying physical process
  • Ensuring security/privacy crucial for safety
    • CPS are deployed in missions critical settings
    • Collect sensitive data and can actuate changes in the physical process
    • Composing individually secure systems into a composed system might not be good enough

• Computation and Energy limitations
  • Utilizing properties from underlying physical process might be a way to proceed
CPS Challenges

• Validation and Certification
  • Given complexity of CPS, it is essential to certify them based on scientific foundations
  • Two step process:
    • Design has right properties
    • Implementation conforms to the design
  • Tools required for:
    • Eliciting models from requirements
    • Validating models that meet right properties
    • Metrics for validating implementation w.r.t. requirements
  • Essential for quantifying reliability, liability, risk of such systems
  • Makes them insurable
It is about reinventing…

- electric grid
- transportation
- healthcare
- building energy management
- aerospace
- manufacturing
- agriculture
- mining
- …
CPS Community Activities

- High Confidence Software Platform for Cyber Physical Systems
- NSF Workshop on Cyber Physical Systems
- NIST: Cyber Security for Cyber Physical Systems
- National Workshop on Research on High-Confidence Transportation Cyber Physical Systems: Automotive Aviation & Rail
- New Research Directions in for Future Cyber Physical Energy Systems
Smart Buildings

• 3.3 Trillion KWHr is used in cooling and lighting buildings
• Buildings use approximately 70% of total electricity usage in Europe
• Emit approximately 40% of greenhouse gases (GHG) annually in US

http://energyofsolandwind.com/energy-efficient-house.htm
Ex3: Electricity Generation & Management

SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.

- **Smart appliances**: Can shut off in response to frequency fluctuations.
- **Demand management**: Use can be shifted to off-peak times to save money.
- **Processors**: Execute special protection schemes in microseconds.
- **Sensors**: Detect fluctuations and disturbances, and can signal for areas to be isolated.
- **Storage**: Energy generated at off-peak times could be stored in batteries for later use.
- **Generators**: Energy from small generators and solar panels can reduce overall demand on the grid.

[http://energyinformative.org/what-is-the-smart-grid/](http://energyinformative.org/what-is-the-smart-grid/)
Ex4: Medical Devices

- Pacemaker, Infusion Pump, MRI machines have 80K, 700K, 7M lines of code
- Pump alone have lead to 20K injuries and 700 deaths from 2005-2009

http://www.health.com/
CPS Potential Benefits

- Address Societal Scale Problems:
  - Global Warming and Energy Shortage
    - Coordinated generation, transmission and consumption of power
  - Continuous Health management
    - Birth to death health monitoring and management
  - Physical infrastructure maintenance
    - Buildings and bridge health monitoring
  - Traffic congestion and accidents
    - Route planning based on improved traffic/road condition awareness
    - Intelligent control of vehicle (lane-drift warning, automatic emergency braking)
Potential Accidental Systems

• Many systems created without conscious design by interconnecting separately designed components or separate systems.
  • Unsound composition: the interconnects produce desired behaviors most of the time
  • Feature interactions: promote unanticipated interactions, which could lead to system failures or accidents

• Modes of interactions
  • Among computation components
  • Through shared resources
  • Through the controlled plant (e.g., the patient)
  • Through human operators
  • Through the larger Environment

• E.g., Medical Device PnP could facilitate the construction of accidental systems
  • blood pressure sensor connected to bed height, resulting in the criticality inversion problem
Other Examples: Auto Recalls

- **1.5M** (in US) Honda Accord, CR-V and Element vehicles recalled “to update the software that controls their automatic transmissions”
- **~75K** Toyota Hybrids recalled for “could enter a "fail-safe" mode that shuts down the engine, allowing only limited operation using the electric motor. The problem, caused by a software error in the Electronic Control Module (ECM) system, triggers up to five warning lights while shutting down the engine.”
- **~8K** Volvo S60 recalled to fix “ software for fuel pump units, as the software was not compatible with all fuel pumps and components, resulting in insufficient fuel transfer in the pump units, which could cause the vehicle to stall.”
R&D Needs for High-Confidence CPS

- **Engineering design techniques and tools**
  - Modeling and analysis, requirements capture, hybrid systems, testing
  - Capture and optimization of inter-dependencies of different requirements
  - Domain-specific model-based tools
  - Plant, environment, and user models

- **Systems Software and Network Supports**
  - Virtualization, RTOS, Middleware, …
  - Predictable (not best-effort) communication with QoS, predictable delay & jitter bounds, …
  - Trusted embedded software components

- **Validation and Certification**
  - Metrics for certification/validation
  - Evidence-based certification, Incremental certification