# Lecture Note #2
# EECS 571
# Cyber-Physical Systems

Kang G. Shin
CSE/EECS
The University of Michigan

(drawn from many sources including lecture notes of Insup Lee at Upenn and Jack Stankovic at Uva)

# What's CPS?, H. Gill @NSF

- Cyber – computation, communication, and control that are discrete, logical, and switched
- **Physical** – natural and human-made systems governed by the laws of physics and operating in continuous time
- **Cyber-Physical Systems** – systems in which the cyber and physical systems are tightly integrated at *all scales* and *levels*
  - Change from cyber merely appliquéd on physical
  - Change from physical with COTS "computing as parts" mindset
  - Change from ad hoc to grounded, assured development

"CPS will transform how we interact with the physical world just like the Internet transformed how we interact with one another."

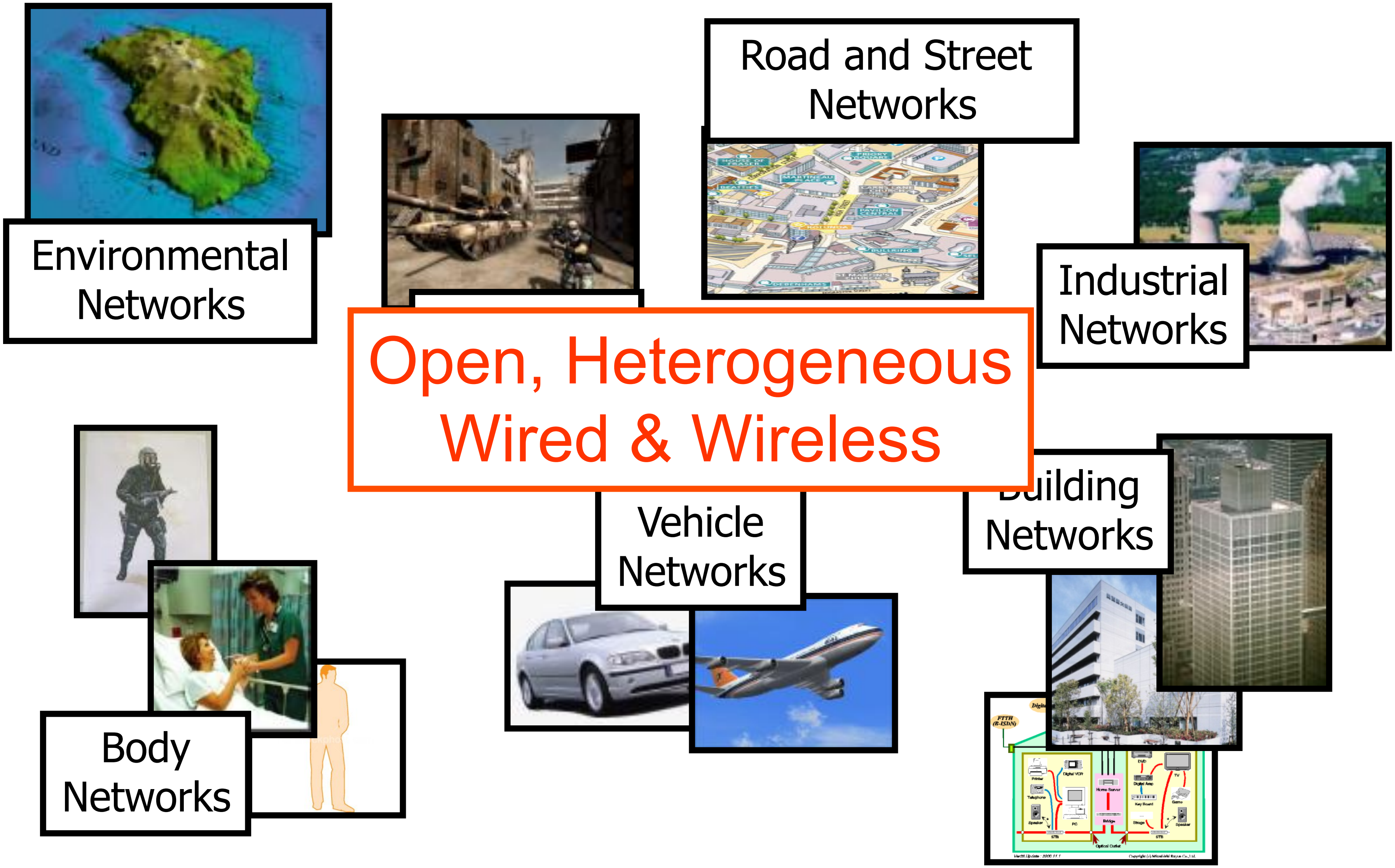
# What's CPS? , cont'd

- Integration of physical systems and processes with networked computing

- Computations and communications are deeply embedded in, and interacting with physical processes to equip physical systems with new capabilities

- Covers a wide range of scale (pacemakers to national power grid)

# Computing in Physical Systems



Environmental Networks

Road and Street Networks

Industrial Networks

Open, Heterogeneous Wired & Wireless

Building Networks

Vehicle Networks

Body Networks

# CPS Characteristics

- CPS are physical and engineered systems whose operations are monitored, coordinated, controlled, and integrated.

- This intimate coupling between the cyber and physical is what differentiates CPS from other fields.

# CPS Characteristics, H. Gill@NSF

Some hallmark characteristics:

- Cyber capability in every physical component
- Networked at multiple and extreme scales
- Complex at multiple temporal and spatial scales
- Constituent elements are coupled logically and physically
- Dynamically reorganizing/reconfiguring; “open systems”
- High degrees of automation, control loops closed at many scales
- Unconventional computational & physical substrates (such as bio, nano, chem, ...)
- Operation must be dependable, certified in some cases.

# Questions on CPS

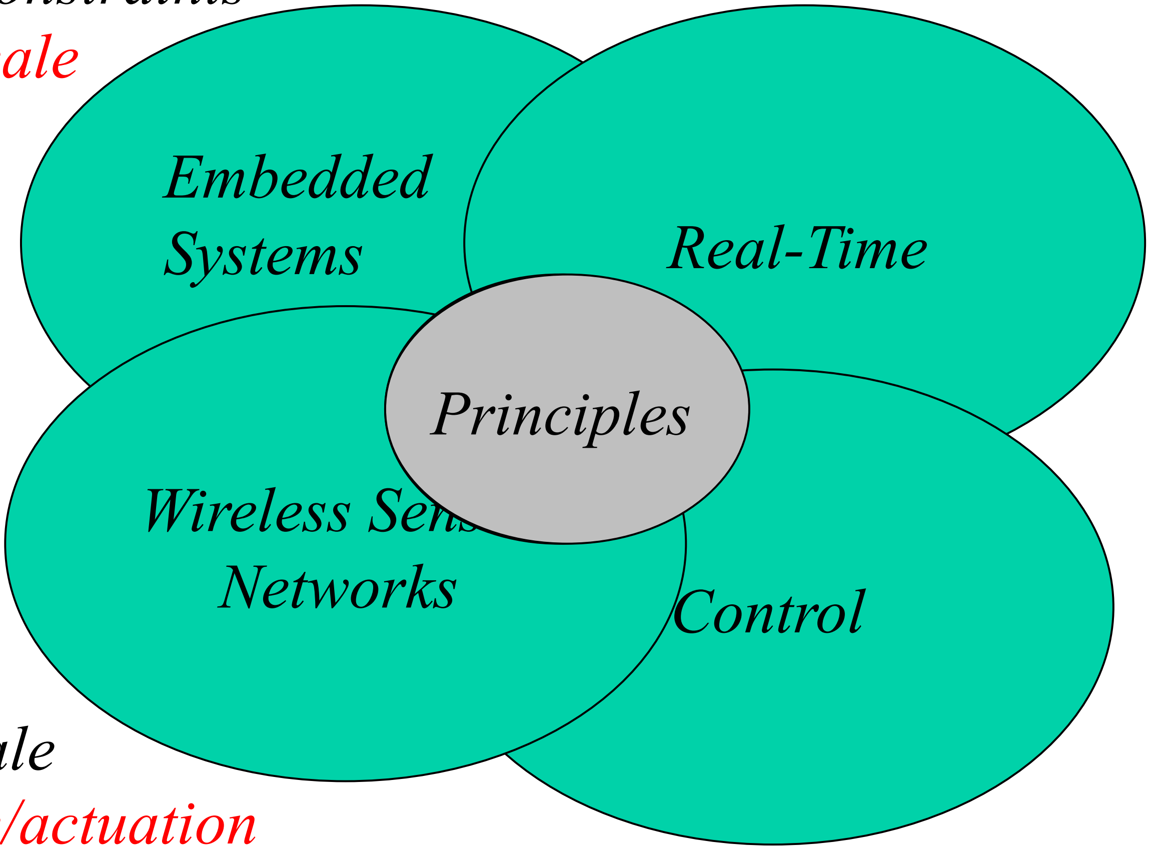
- Are CPS simply embedded systems on steroids?
  - Interact with the physical world
  - Constraints on cpu, power, cost, memory, bandwidth, …
- Is the Internet just a LAN on steroids?

- Confluence of the right technologies at the right time can result in
  - Fundamental paradigm shift
  - Totally new systems
  - Revolutionize business, science, entertainment, …

# Confluence of Four Areas

*Cost*
*Form factor*
*Severe constraints*
*Small-scale*
*Closed*

*Scheduling*
*Fault-tolerance*
*Wired networks*



*Embedded Systems*

*Real-Time*

*Principles*

*Wireless Sen Networks*

*Control*

*Noisy*
*Sensing*
*Large-scale*
*Real-time/actuation*
*Open*

*Linear*
*Adaptive*
*Distributed*
*Decentralized*
*Closed*

# Realistic (Integrated) Solutions

- CPS must tolerate
  - Failures
  - Noise
  - Uncertainty
  - Imprecision
  - Security attacks
  - Lack of perfect synchrony
  - Scale
  - Openness
  - Increasing complexity
  - Heterogeneity
  - Disconnectedness

# Challenges Arise

- Assumptions underlying distributed systems technology has changed dramatically
  - New abstractions needed
  - Wired => wireless
  - Unlimited power => limited power
  - User interface (screen/mouse) => sensors/real world interface
  - *Fixed* set of resources => resources are *dynamically* added/deleted
  - Each node is important => *aggregate behavior* is important
  - Location unimportant => location is critical

# New Theories

- Compositional
- Control Theory
- Optimization
- Real-Time
- Integration Issues
- Openness, Mobility, Uncertainty, Concurrency, Noise, Faults, Attacks, Self-Healing, etc.

# CPS - Enabler for Dramatic Innovation

- New global-scale, personal medical service delivery systems
- New paradigms for scientific discovery
- Smart (micro) agriculture
- Towards the end of terrorism
- Smart, networked vehicles
- New generation Internet

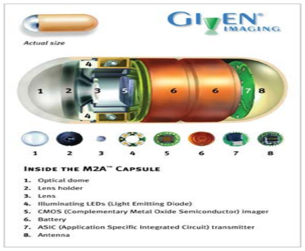
# Example: Automotive Telematics

- In 2005, 30-90 processors per car
  - Engine control, break system, airbag deployment system
  - Windshield wiper, door locks, entertainment systems
  - Example: BMW 745i
    - 2,000,000 LOCs
    - Window CE OS
    - Over 60 microprocessors
      - 53 8-bit, 11 32-bit, 7 16-bit
    - Multiple networks
    - Buggy?

- Cars are sensors and actuators in V2V networks
  - Active networked safety alerts
  - Autonomous navigation
  - …

# Example: Health Care and Medicine

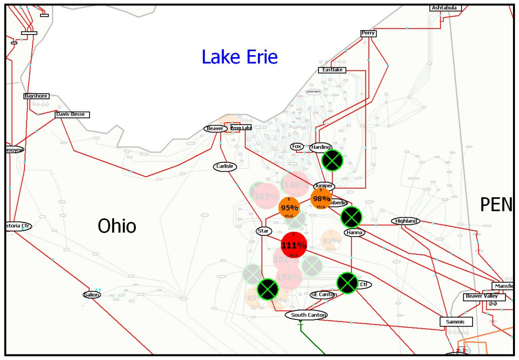
- National Health Information Network, Electronic Patient Record initiative
  - Medical records at any point of service
  - Hospital, OR, ICU, …, EMT?
- Home care: monitoring and control
  - Pulse oximeters (oxygen saturation), blood glucose monitors, infusion pumps (insulin), accelerometers (falling, immobility), wearable networks (gait analysis), …
- Operating Room of the Future
  - Closed-loop monitoring and control; multiple treatment stations, plug and play devices; robotic microsurgery (remotely guided?)
  - System coordination challenge
- Progress in bioinformatics: gene, protein expression; systems biology; disease dynamics, control mechanisms

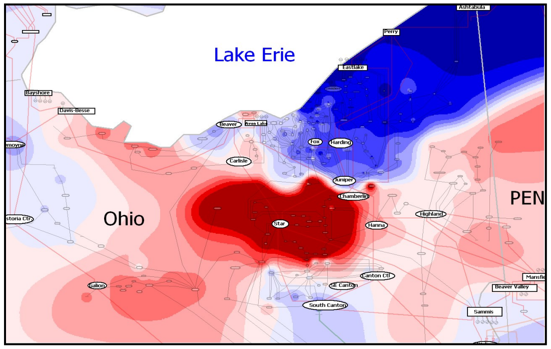

GIVEN IMAGING
Actual size
1
2
3
4
5
6
7
8
INSIDE THE M2A™ CAPSULE
1. Optical dome
2. Lens holder
3. Lens
4. Illuminating LEDs (Light Emitting Diode)
5. CMOS (Complementary Metal Oxide Semiconductor) imager
6. Battery
7. ASIC (Application Specific Integrated Circuit) transmitter
8. Antenna

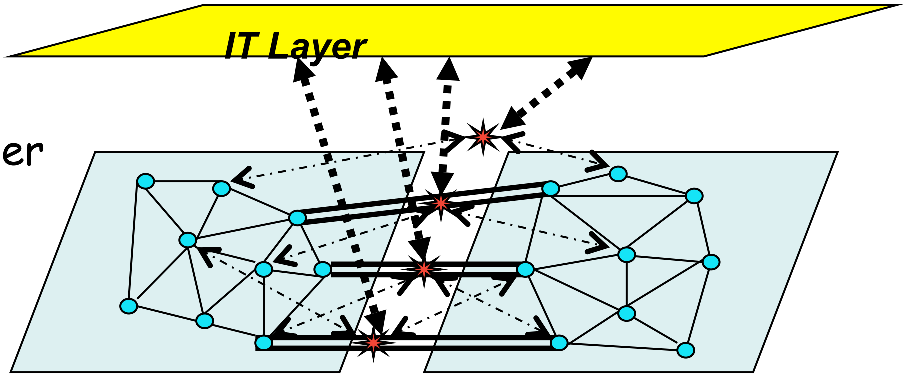
*Images thanks to Dr. Julian Goldman, Dr. Fred Pearce*

# Example: Electric Power Grid

- **Current picture:**
  - Equipment protection devices trip *locally, reactively*
  - Cascading failure: August (US/Canada) and October (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)
  - Technology vectors: FACTS, PMUs
  - Context: market (timing?) behavior, power routing transactions, regulation



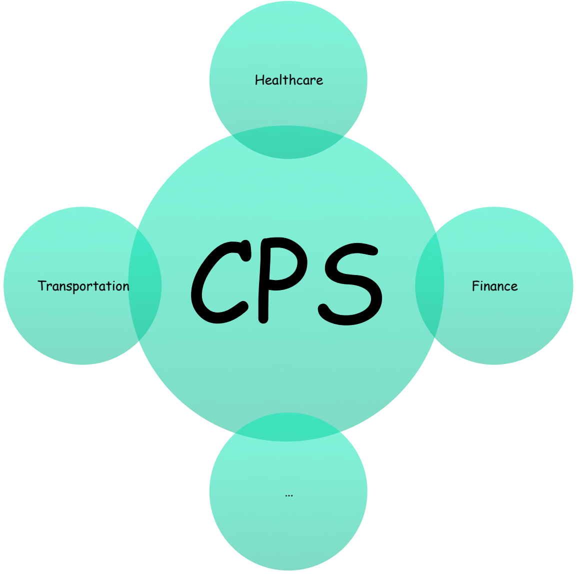




*Images thanks to William H. Sanders, Bruce Krogh, and Marija Ilic*

# Application Domains of Cyber-Physical Systems

- Healthcare
  - Medical devices
  - Health management networks
- Transportation
  - Automotive electronics
  - Vehicular networks and smart highways
  - Aviation and airspace management
  - Avionics
  - Railroad systems
- Process control
- Large-scale Infrastructure
  - Physical infrastructure monitoring and control
  - Electricity generation and distribution
  - Building and environmental controls
- Defense systems
- Tele-physical operations
  - Telemedicine
  - Tele-manipulation



*In general, any "X by wire(less)" where X is anything that is physical in nature.*

# Grand Visions and Societal Impact

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

# Key Trends in Systems

- System complexity
  - Increasing functionality
  - Increasing integration and networking interoperability
  - Growing importance and reliance on software
  - Increasing number of non-functional constraints
- Nature of tomorrow's systems
  - Dynamic, ever-changing, dependable, high-confidence
  - Self-*(aware, adapting, repairing, sustaining)
- Cyber-Physical Systems everywhere, used by everyone, for everything
  - *Expectations*: 24/7 availability, 100% reliability, 100% connectivity, instantaneous response, remember everything forever, …
  - *Classes*: young to old, able and disabled, rich and poor, literate and illiterate, …
  - *Numbers*: individuals, special groups, social networks, cultures, populations, …

# Societal Challenge

- How can we provide people and society with cyber-physical systems that they can trust their lives on?

*Trustworthy:*
*reliable, secure,*
*privacy-preserving,*
*usable, etc.*

- Partial list of complex system failures
  - Denver baggage handling system ($300M)
  - Power blackout in NY (2003)
  - Ariane 5 (1996)
  - Mars Pathfinder (1997)
  - Mars Climate Orbiter ($125M, 1999)
  - The Patriot Missile (1991)
  - USS Yorktown (1998)
  - Therac-25 (1985-1988)
  - London Ambulance System (£9M, 1992)
  - Pacemakers (500K recalls during 1990-2000)
  - Numerous computer-related Incidents wth commer aircraft (http://www.rvs.uni-bielefeld.de/publications/compendium/incidents_and_accidents/index.html)

# R&D Needs

Development of high-confidence CPS requires

- 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
- Systems Software and Network Supports
  - Virtualization, RTOS, Middleware, …
  - Predictable (not best-effort) communication with QoS, predictable delay & jitter bounds, …
  - Trusted embedded software components
    - To help structured system design and system development
    - To reduce the cost of overall system development and maintenance efforts
    - To support the reuse of components within product families
- Validation and Certification
  - Metrics for certification/validation
  - Evidence-based certification, Incremental certification

# Scientific Challenges

- Computations and Abstractions
  - Computational abstractions
  - Novel Real-time embedded systems abstractions for CPS
  - Model-based development of CPS
- Compositionality
  - Composition and interoperation of cyber physical systems
  - Compositional frameworks for both functional, temporal, and non-functional properties
  - Robustness, safety, and security of cyber physical systems
- Systems & Network Supports
  - CPS Architecture, virtualization
  - Wireless and smart sensor networks
  - Predictable real-time and QoS guranattees at multiple scales
- New foundations
  - Control (distributed, multi-level in space and time) and hybrid systems - cognition of environment and system state, and closing the loop
  - Dealing with uncertainties and adaptability - graceful adaptation to applications, environments, and resource availability
  - Scalability, reliability, robustness, stability of system of systems
  - Science of certification - evidence-based certification, measures of verfication, validation, and testing

# Software, the Great Enabler

- Good news: anything is possible in software!
- Bad news: anything is possible in software!

- It is the software that affects system complexity and also cost.
  - Software development stands for 70-80 % of the overall development cost for some embedded systems.

# Embedded Software - Goals

- Trustworthy: should not fail (or at least gracefully degrade), and safe to use. The existence of embedded software becomes apparent only when an embedded system fails.
- Context- and Situation-Aware: should be able to sense people, environment, and threats and to plan/notify/actuate responses to provide real-time interaction with the dynamically changing physical environment with limited resources.
- Seamless Integration: should be invisible at multiple levels of a hierarchy: home systems, metropolitan systems, regional systems, and national systems.
- Validation and Certification: should be able to assure that embedded systems work correctly with respect to functional and nonfunctional requirements with high degree of certainty.

# Software Research Challenges

- Need new notions of “correctness” and “compositionality”
  - Factor in context of use, unpredictable environment, emergent properties, dynamism, interoperability
  - What are desired properties of and metrics for both software and systems (e.g., resource use)
- Need new formal models and logics for reasoning about CPS
  - Uncertainty, physical world, mental model of human user
  - Hybrid automata, probabilistic logic
- Need new verification/analysis tools usable by domain engineers
  - Push-button, lightweight
  - Integrated with rest of system development process

# Interaction Complexity

- We know how to design and build components.
- Systems are about the interactions of components.
  - Some interactions are unintended and unanticipated
    - Interoperability
    - Emerging behaviors
- "Normal Accidents", an influential book by Charles Perrow (1984)
  - One of the Three Mile Island investigators
  - And a member of recent NRC Study "Software for Dependable Systems: Sufficient Evidence?"
  - A sociologist, not a computer scientist
- Posits that sufficiently complex systems can produce accidents without a simple cause due to
  - interactive complexity and tight coupling

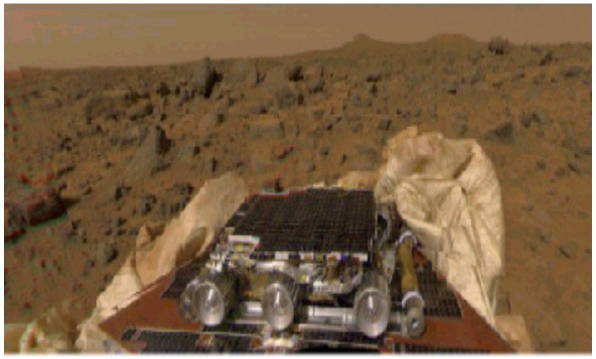
# Potential Accidental Systems

- 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 share 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

# Unexpected interactions

- Landed on the Martian surface on July 4th, 1997
- Unconventional landing – boucing 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

***Incompatible Cross Domain Protocols***



*Pathological Interaction between RT and synchronization protocols Pathfinder caused repeated resets, nearly doomed the mission*

*[Sha]*

# Final Thoughts

- Real-time issues, WSN issues, control issues should *not* be addressed *alone*

- Connection to the physical world will be so pervasive that systems will be *open* even if you think they are not

  =>New abstractions and composition techniques needed.

# More Info

http://varma.ece.cmu.edu/InfoCPS/Workshops.html

http://www.iccps.org