BBN TECHNOLOGIES

Dependability Issues in Cyber-Physical Systems

Vicraj Thomas, Ph.D.
vthomas@bbn.com
+1 763 545 5721

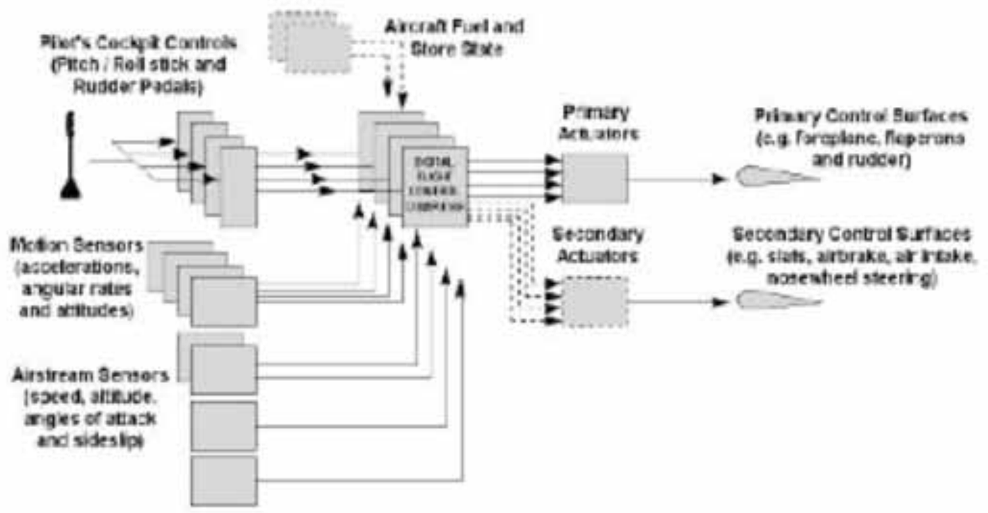
30 June 2008

Cyber Physical Systems

- Sense and affect dynamic physical environments
- Operate in real-time
- Often used in safety-critical applications
- An embedded systems is not necessarily a cyber-physical system
  - E.g. embedded microwave oven controller
- Old wine in new bottles?

Classical Cyber-Physical Systems

- Industrial Process Control
- Aircraft Flight Control Systems



Chris Fielding, “The Design of Fly-by-Wire Flight Control Systems”

Typical industrial process control plant

System Characteristics

- Operate in fairly well characterized environments
  - Frequency and magnitude of environmental events/disturbances
- Operate in fairly insular environments
  - Access to physical plant tightly controlled
  - Operate on designated and access controlled spaces
    - E.g. designated flight routes
- Operate under human supervision: Human can take control if system is unable to cope
  - Plant operator, pilot, etc
- We know how to build and operate such systems

BBN TECHNOLOGIES

Trends: Autonomous Vehicles

- DARPA Grand Challenge (2005)
  - Ground vehicles driving a 132 mile course over desert terrain
- DARPA Urban Challenge (2007)
  - Ground vehicles maneuvering in a mock city environment

Key System Characteristics

- Operate in unpredictable environments
  - Nature, frequency and magnitude of environmental events/disturbances unconstrained
  - Possibly hostile environment
- No human supervision
  - Must autonomously cope with the unexpected
- Classical design techniques do not work

Challenges

- Control
  - Greater reliance on AI
    - Learning, rule-based systems, etc.
- Sensor processing
  - High bandwidth sensors
  - Detection and characterization of threats
  - Real-time processing
  - Sensor reliability
  - False positive/negative rates
  - Sensor synchronization
    - Video, audio, lidar

The Velodyne lidar sensor provides range and reflectivity information for over 1.8 million points every second

Challenges

- Navigation
  - Need to blend multiple navigation aids with different resolutions
    - Satellite navigation: GPS, Galileo, etc.
    - Inertial navigation
    - Landmark based: Buildings, lane markers, etc.
  - Sensor processing and navigation closely linked
- Re-thinking system design
  - Operator comfort systems not needed
  - Controls can be distributed
    - Do not have to be within reach of a human
  - Sensors can be distributed

Challenges

- Safe yet affordable
  - Systems immersed in human society
    - Must not disrupt everyday human activity
  - As adoption rates increase system reliability requirements exceed those for avionics systems
- Societal
  - Willingness to trust automation
  - Need for regulation – controversial
  - Legal – assignment of liability

Yet Autonomous Vehicles are Here!

- Autonomous vehicles in the home
  - Vacuuming floors, mowing lawns
- Autonomous vehicles for agriculture in the works

iRobot autonomous vacuum cleaner

John Deere prototype autonomous tractor

FriendlyRobotics autonomous lawn mower

Today's Autonomous Systems

- Operate in constrained environments
  - Homes, yards, farms without small children and pets
- Small, low-powered, slow-moving
  - Not enough momentum to cause harm
- Simple sensors such as pressure sensors on bumpers sufficient for safe operations
- Early adopters of technology tend to be more forgiving of shortcomings
  - Low expectations fostered by relatively low cost of systems

Concluding Remarks

- Despite challenges cyber-physical systems have evolved rapidly in the last decade
  - "Machines take me by surprise with great frequency" – Alan Turing
- Lack of a disciplined, scientific approach to system design can result in incidents that hamper progress
  - "To err is human, but to really foul things up requires a computer" – Farmers' Almanac 1978