

Next Generation Sensor Actuator Systems

Vic Thomas
10 July 2007

Honeywell

- **Next generation sensor actuator systems: Key features**
- **Examples from three application domains**
 - Avionics
 - Industrial Process Control
 - Space Robotics
- **Suggested research topics**
- **Concluding remarks**

- **Key features**

- **Largely wireless**

- ◆ Dynamic with changing topologies, sensors, actuators

- **Large scale**

- **Provable system properties**

- ◆ Safety, reliability, determinism

- **Mission aware**

- ◆ Autonomous adaptation of communications, control, operator interfaces based on mission needs

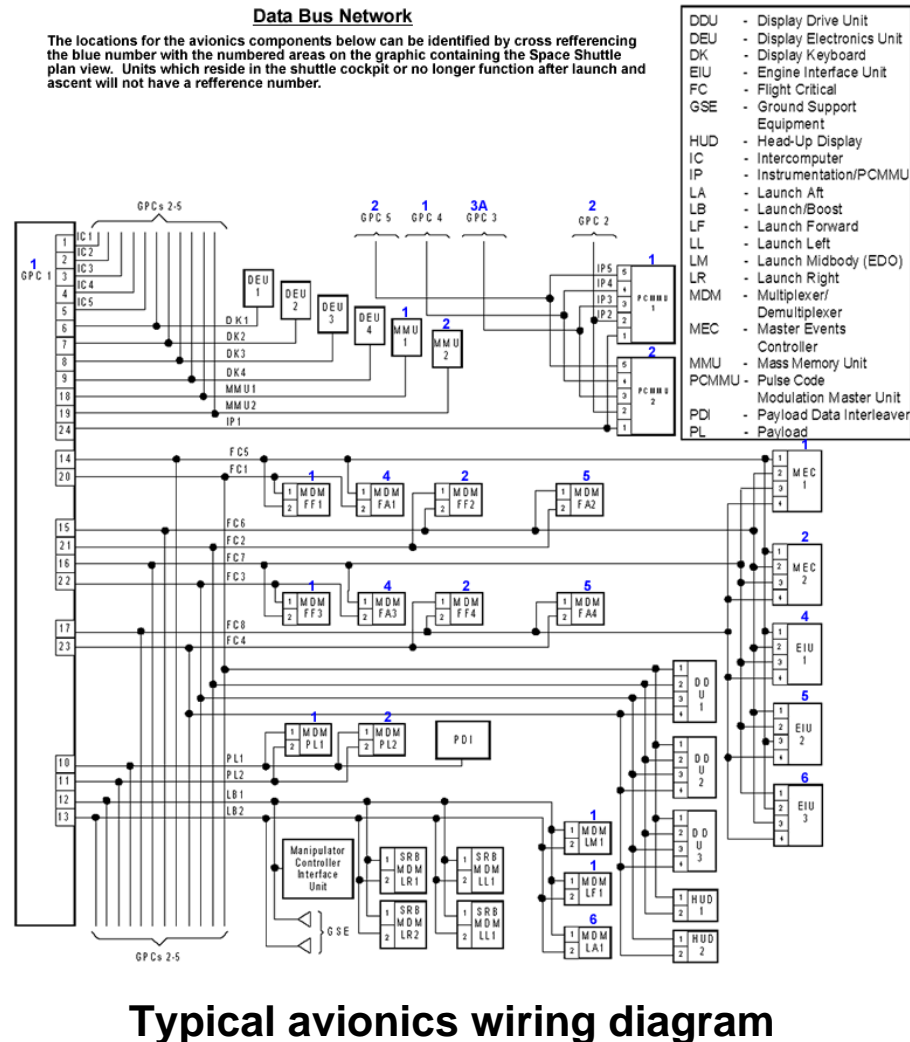
- **Distributed control**

- ◆ Flexible control structures

- Next generation sensor actuator systems: Key features
- **Examples from three application domains**
 - Avionics
 - Industrial Process Control
 - Space Robotics
- Suggested research topics
- Concluding remarks

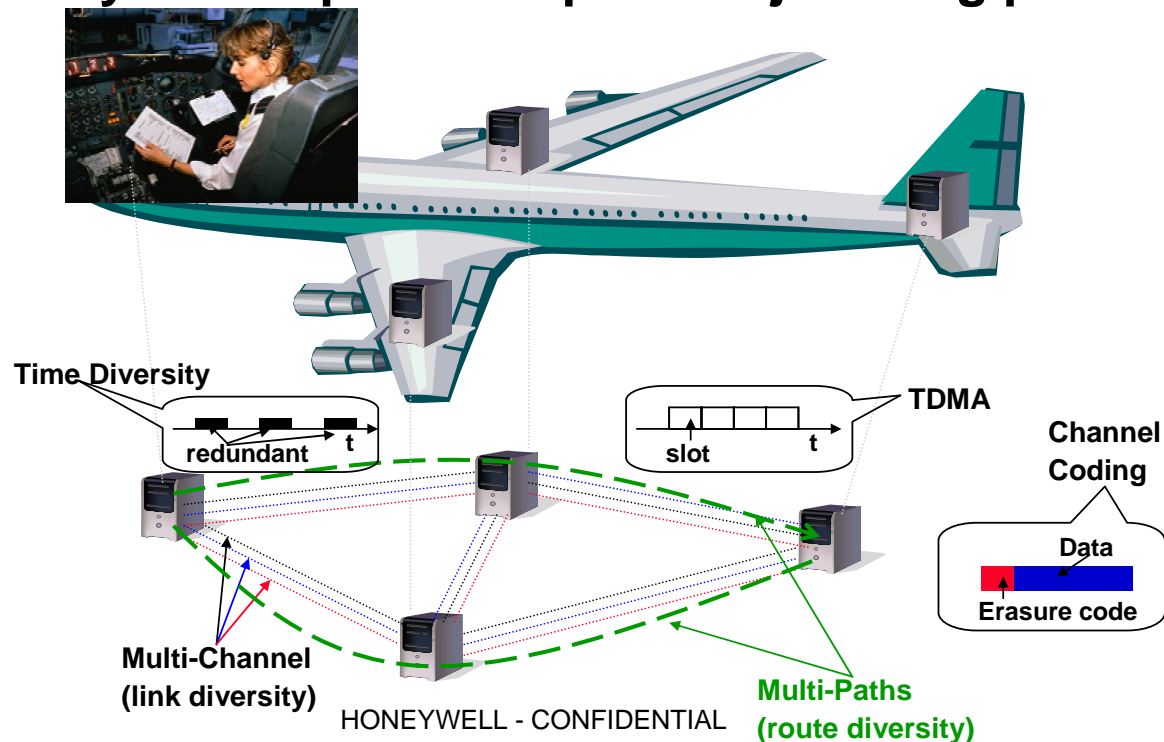
Avionics: State-of-the-Practice

- Almost all wired networks
- Wireless networks mainly for cabin services
- Newer wireless applications
 - Emergency lighting
 - Lavatory and cargo smoke detectors
- Benefits
 - Reduced weight
 - ◆ Translates to lower fuel costs
 - Ease of re-configurability of aircraft
 - Lower installation and maintenance costs
 - Eliminate loose connector problem



Avionics: Next Generation

- **Wireless technologies for flight-essential functions**
- **Technology based in exploiting multiple forms of redundancy**
 - Frequency redundancy, time redundancy, coding redundancy (direct sequence and erasure coding), network path redundancy
 - Redundancy techniques also provide jamming protection



- **Technology**
 - Meeting bandwidth requirements despite multiple forms of redundancy
- **Certification**
 - Need convincing arguments on system safety and security
 - Lack of experience with technology
 - ◆ Failure modes, attack models, etc. not well understood
- **Spectrum**
 - Need protected spectrum for such applications
 - ◆ FAA will not certify high-criticality wireless application in unprotected bands
- **Mitigation plan**
 - Start with low-criticality applications such as vehicle health management
 - ◆ Larger in scale than existing wireless networks
 - Wireless system with wired backup
 - All wireless system

Industrial Control: State-of-the-Practice

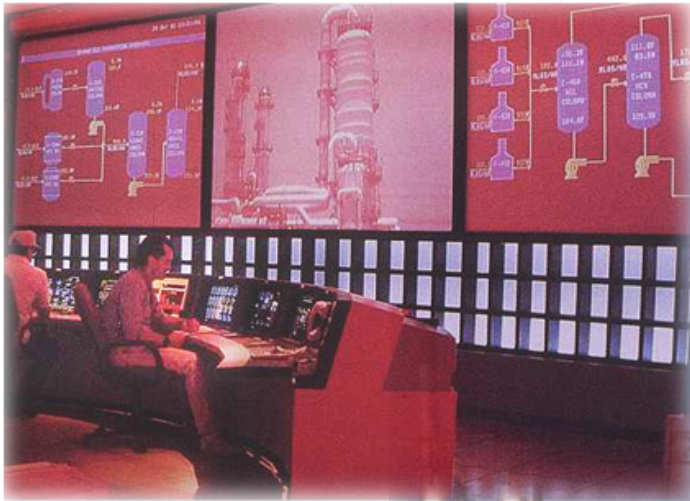
Honeywell

Typical Unit:

- 1000 to 1500 sensors
- 200 to 300 actuators
- Area: 1 square mile

Typical Process Plant

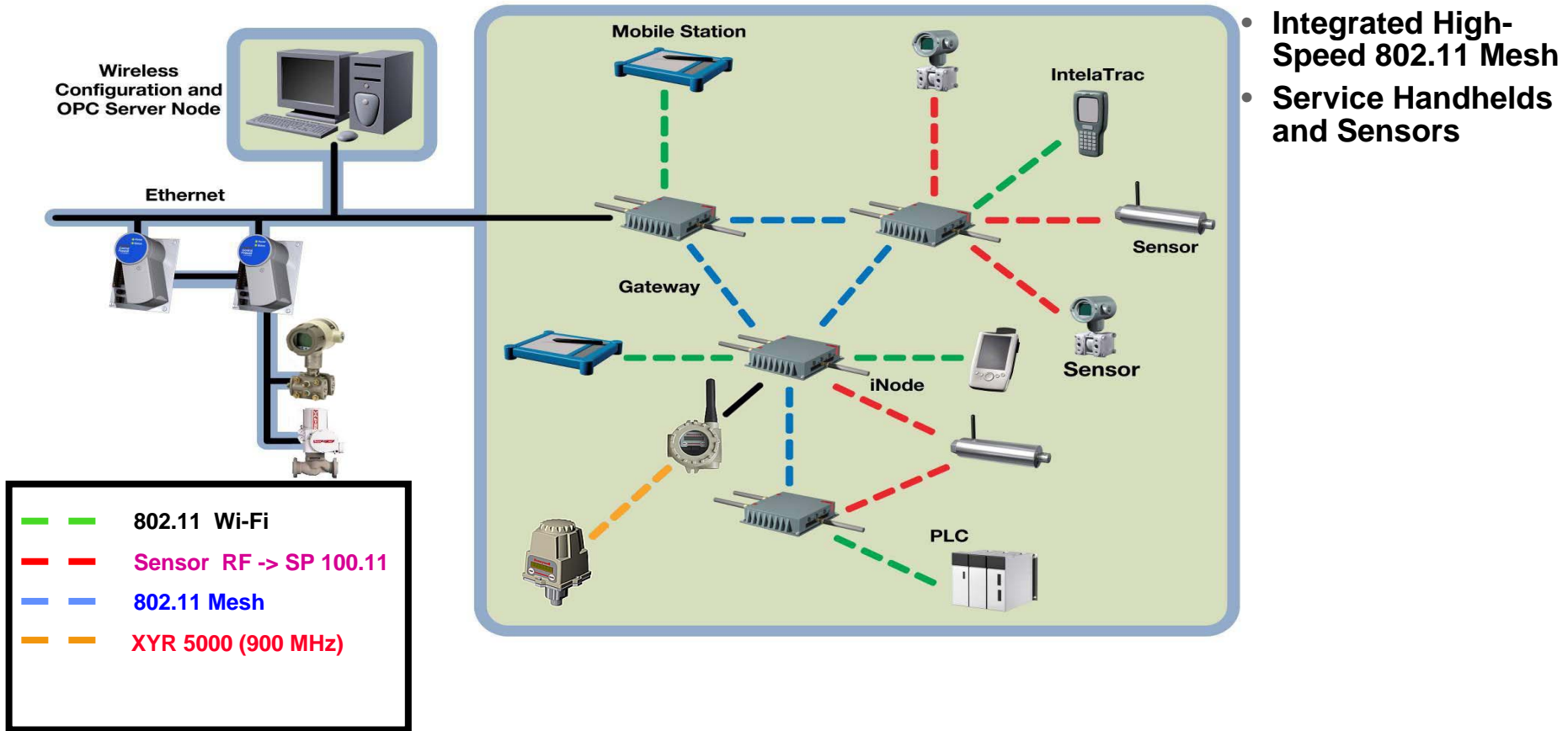
- 6 to 8 units



Typical Control System

- 300 to 450 control points
- Control loops: 20ms to 5sec
- Miles of dual-redundant cables to sensors/actuators

Industrial Control: Next Generation



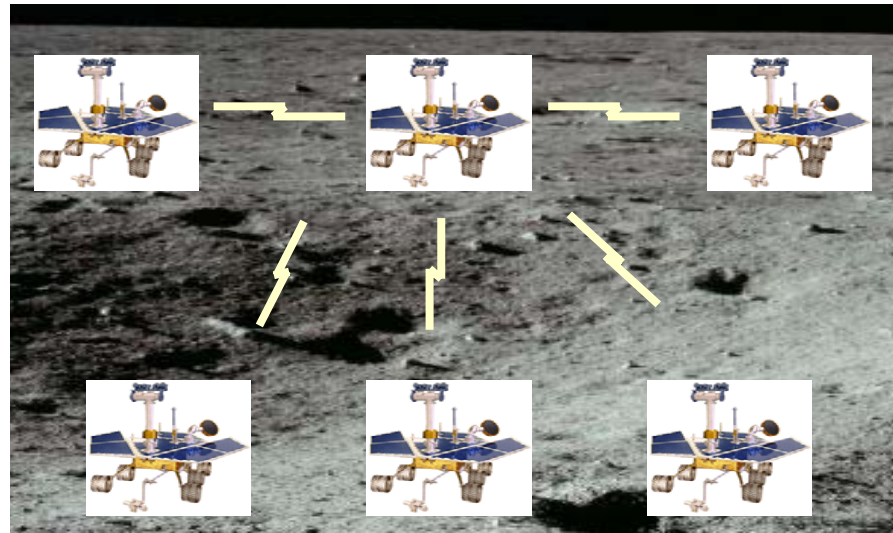
- Early versions being readied for deployment
- Not ready for an all-wireless network

- **Lack of experience with technology**
 - Failure modes, attack models, etc. not well understood
 - ◆ Industrial espionage major concern
- **Shared infrastructure by control and non-control applications (e.g. handheld PDAs)**
- **Low power communication technologies**
 - Customers want devices with battery lives > 1 year
- **Spectrum**
 - Possible solution: Use different frequencies in different regions

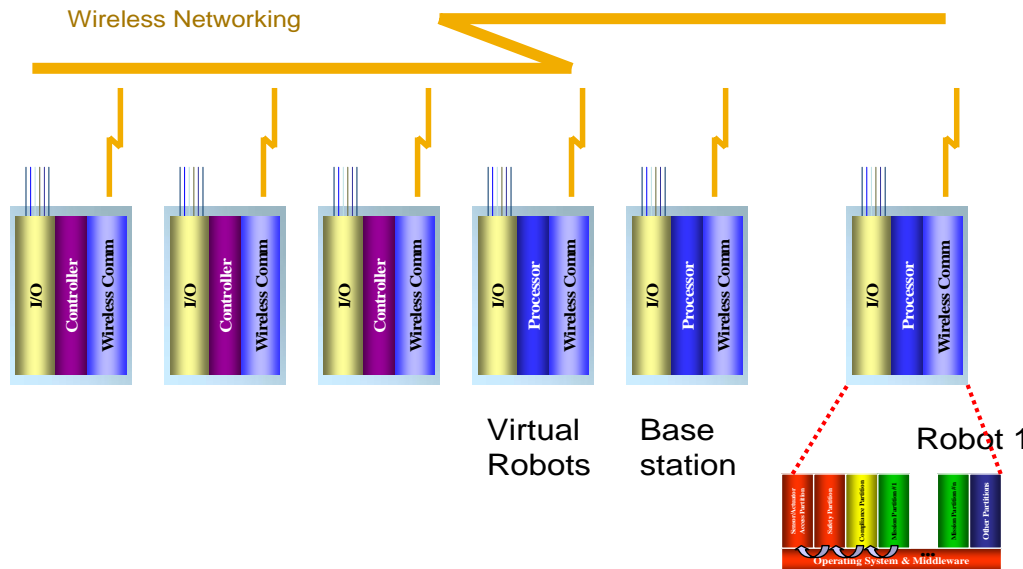
- **Vehicles/robots with little autonomy**
 - All control from ground
- **Low mission productivity**
 - Long delays in the control loop (sensor-control-actuator)
- **Rigid control structure**
 - Different communication links and protocols to International Space Station, Space Shuttle, Mars Rovers, etc.
 - Inability to distribute or shift control as mission unfolds

Space Robotics: Next Generation

- Multiple small robotics collaboratively accomplish mission
- Modular avionics architectures
- Enabled by mobile wireless technologies that can meet virtual backplane requirements.



Operational View



Architectural View

Time and Space Partitioning

Space Robotics: Challenges

- **Fine grained distributed control**
 - Any vehicle can take on role of controller
 - Highly deterministic network
 - ◆ Network is the back-plane
- **Mobile ad-hoc network**
 - Yet performance needs to be predictable

- Next generation sensor actuator systems: Key features
- Examples from three application domains
 - Avionics
 - Industrial Process Control
 - Space Robotics
- **Suggested research topics**
- **Concluding remarks**

- **User/Application/System needs:**
 - **System resources managed in a coordinated manner**
 - ◆ Cf. today's systems where each resource manager optimizes resources independently according to some pre-determined optimization criteria
 - **Network-wide system resources managed as whole**
 - ◆ No unnatural separation of “compute resources” (CPU, memory, bandwidth) and “application resources” (fuel, ammunition, sensors)
- **Research topics:**
 - **Formal models for missions**
 - ◆ Mission structures, objectives, ontologies, etc.
 - **Formal models for systems and resources**
 - ◆ Platforms, sensors, bandwidth, etc. and ontologies
 - **Formal models are essential for self-organizing, self-managing networks of autonomous systems**
 - ◆ Systems that are not self-managing and optimizing will be brittle against changing operational conditions
 - **Self-optimizing reflective systems**
 - ◆ Systems that reflect on their behaviour with respect to the application and manage resources accordingly

Systems with Provable Operational Properties

- **User/Application/System needs:**
 - **Systems with provable safety, security and performance properties**
- **Research topics:**
 - **Mechanisms for specifying system properties to be maintained**
 - **Configuration and runtime mechanisms that ensure properties are maintained**
 - **Calculus to prove to certification and other authorities that system properties cannot be violated**

- **Next generation sensor-actuator systems have the potential of radically improving the state-of-the practice**
- **Specific requirements vary by application area but many common technology needs**
 - **Formal identification and representation of system safety and integrity requirements**
 - ◆ Invariants that must be maintained at all times
 - **Design, configuration and run-time mechanisms to ensure system integrity isn't violated**
 - ◆ Network and control-theory based techniques
 - **Resilience to failures**
 - ◆ Sensor and actuator failures in addition to traditional computer and network failures
 - **Human-system interaction**
 - ◆ Including mechanisms to convey to humans what the system is doing and why