Certifiable Wireless Data Buses

Vic Thomas
vic.thomas@honeywell.com
Honeywell Labs

28 March 2007
Certifiable Wireless Data Buses

- Objective: Replace wired avionics data buses with wireless data buses
  - Can we replace a wired bus such as ARINC 629 with a wireless equivalent?

- Rationale:
  - Reduced weight
    - Translates to lower fuel costs
  - Ease of re-configurability of aircraft
  - Lower installation and maintenance costs
Wireless data buses are being used for

- Cabin entertainment systems
  - Reduces cost associated with changing seat pitch, seasonal changes in configuration (number of 1st class seats)

- Lavatory smoke detectors
  - Today airplanes have superfluous wiring to accommodate different configurations used by different airlines

- Cargo hold smoke detectors

- Emergency lighting system

All wireless data buses used today are for non-critical applications
CTQs for Wireless Data Buses for Critical Functions

- Reliability
- Availability
- Data integrity
- Determinism
  - Bounded delivery times, low jitter
- Security
  - Low susceptibility to denial-of-service attacks (jamming)
  - Authenticated messages
  - Encryption?
- Non-interference
  - Must not interfere with existing radios and avionics
- Bandwidth
  - Provide bandwidth comparable to modern wired data buses
- Certifiable
  - Convince appropriate authorities that system meets above properties
Challenges

• Certification is the biggest challenge
• Requirements are not well understood
  - E.g.: “How much” jamming resilience is required?
    - How is this specified?
    - How “jamming resistant” are today’s avionics when personal radios are not allowed on board
• Lack of a good understanding of the faults suffered by wireless networks
• Current certification processes may inadequate
  - Limited to understanding the effects of on-board wireless systems on existing radios and avionics
• Where in the RF spectrum should these networks operate?
  - The only globally available frequency band is the 2.4 GHz ISM band
• Requires a change in the mind-set of the certification authorities
  - Knee-jerk reaction is to reject anything wireless as being inherently un-certifiable
Designing a Wireless Data Bus

- Given any dependability and security requirements it is possible to design a wireless data bus that meets those requirements
  - Must have sufficient spectrum available
Commonly Used Techniques for Dependability and Security

• A combination of techniques will be needed to meet dependability, determinism and security requirements

• Different techniques provide tolerance for different kinds of faults and are implemented at different layers of the protocol stack
Techniques for Jamming Resistance

- **Spread spectrum techniques**
  - Spread energy over larger part of the spectrum
  - Frequency hopping and Direct Sequence Pseudo Noise are commonly used
    - Time Hop and Transform Domain spread spectrum techniques less common
- **Typically use combination of techniques**
  - Frequency hopping + direct sequence
    - Permits use of widely spaced bands (hop among bands and spread energy within band)
- **For additional protection, send same bit(s) over multiple frequency hops**
  - Keeps a narrow-band jammer from taking out a part of the communication
- **For Frequency Hopping, hopping sequence must not be guessable**
  - Cryptographic techniques
    - Can’t guess seed of random number generator by observing generated numbers
  - Re-seed all random number generators during scheduled maintenance
Techniques for Reliability, Determinism and Security

• Physical/Link layer
  - Bits transmitted over multiple frequency hops
  - Determinism
    ♦ Build on deterministic MAC technology developed by Honeywell

• Network layer: At least N independent pre-computed routes between any two nodes
  - Tolerates failures on nodes
  - Build on Honeywell ACS routing protocol that guarantees two independent routes between a data source and a data sink

• Application layer: Control applications that can tolerate delayed or lost messages

• Security
  - Needed for authentication and possibly encryption
    ♦ Build on Beep-Beep embedded encryption algorithm developed by Honeywell
  - Aircraft wide-key, changed during scheduled maintenance
Spectrum Considerations

• Availability of spectrum that can be used world-wide is a problem

• Option 1: Work in the 2.4 GHz unlicensed band
  - Very crowded with consumer electronic devices

• Option 2: Petition ITU for new spectrum allocation
  - Very difficult and time-consuming process

• Option 2: Reassign unused spectrum already allocated for Aeronautical use
  - E.g. Microwave Landing Systems (MLS)
    - MLS systems are being made obsolete by GPS precision landing systems
  - Other promising portions of the RF spectrum have been identified
Reliability Advantages of Wireless

- **Wireless data buses will be more tolerant of certain faults commonly suffered by wired data buses**
  - Loose cable connections
    - Most common cause of network failure
  - EMP
    - Easier to design EMP protection for wireless data buses
Phased Approach to Deploying Wireless Data Buses

• Wireless data bus as a backup to a wired data bus
  - Will help gain experience with the use of wireless for essential functions

• Replace segments of a wired data bus with a wireless data bus
  - Use wireless in areas where network reconfiguration would be required when aircraft is reconfigured
  - Use wireless in places hard to reach with wiring

• All wireless systems

It’s only a matter of time before we see wireless network based critical avionics systems.