Real Time Systems
Impact of Network Communications

2015 Propulsion Control and Diagnostics Workshop
NASA Glenn Research Center, November 2016

with
Eliot Aretskin-Hariton and Dennis Culley
Intelligent Control and Autonomy Branch
Overview

• Goals of real-time communication networks
• Centralized vs. distributed systems
• Modeling and simulation efforts at GRC
  – Hardware models of multidrop network
  – Software models of multidrop network
• Exploring critical parameters for digital networks
Goals

• Create network models for system simulation
  – What types of failure modes should we expect
  – How can we simulate these failure modes
  – How can we design control systems to overcome these failure modes

• Derive Network requirements
  – What is the minimum speed the network requires to operate
  – What type of security can be used to ensure command authority
Centralized vs. Distributed

**Centralized & Analog**
- All data is available instantly
- Dedicated cable for each node
- A/D handled by central node
- Analog sensor/actuator interfaces prevent easy replacement & alternative sourcing of components

**Distributed & Digital**
- Data is sampled sequentially
- A/D imbedded in the smart node
- Drop-in component compatibility
- Packet delay
- Packet loss
- Packet corruption
Distributed Network Hardware Simulation

• Data flow is limited by hardware selection
• Final specifications of hardware are not yet complete
• Guidelines specifications that we used when choosing a network:
  – Multi-drop bus with RS-485 hardware,
  – Master / Slave with schedule dictated by master
  – 10Mbps maximum speed
  – 20MHz max clock speed
  – 18 bytes per message
  – Preamble, Data,
  – Break Field, Sync Field
  – CRC-15 Checksum
Empirical Network Model: multi-drop network implemented on an RS-485 physical layer

Node 03 (Actuator)
Node 02 (Sensor)
Node 01 (Sensor)
Node 00 (Master)
Physically Distributed Control Functions in Simulation

- **Smart node simulated in Linux / Python**
  - Ported from Simulink
- **Communication**
  - Implemented in C++
  - Close to real-time processor
  - Predictable command execution time
  - 16MHz
  - Software available on NASA GitHub
  - [https://github.com/nasa/EADINLite](https://github.com/nasa/EADINLite)
Simulink Model of Multidrop Network

• Simulated failure modes
  – Packet Loss (% or time dependent)
  – Power Loss
  – Cut Cable
  – Blabbering Idiot
  – CRC Failure

• Final results:
  – Did the data arrive at its destination?
  – Yes/No
Real Time and Faster than Real Time Testing

• Real-time system

- Engine Model
  - (Memory Sharing)
  - User Interface
- DECSS
  - Memory Sharing
  - Master Node
  - RS485 Adapter
  - Microcontrollers

• Faster than real-time system

- C-MAPSS40k Engine Plant Model
- Operator Controls, Displays, Fault Insertion
- C-MAPSS40k Controller
- switch
Scheduling and the Impact on Bandwidth

- Analog systems provide the control system all info. at every time step
- Sensors are oversampled
- Digital bandwidth is limited
- Sensors in real systems sample at different rates
- Careful design considerations required to maintaining controllability while minimizing bandwidth
Information Security and the Impact on Bandwidth

- HMAC authentication can significantly increase message size while providing message source authentication
- Authentication protocols are well understood and widely deployed
- Encryption can limit message size increase, but is relatively untested in real-time systems with limited bandwidth and processing power
Minimum Bandwidth Estimates

- CMAPSS40k specific estimates on minimum bandwidth. Each message
- 29 kbps - 18B message, at minimum time constant (3 messages / 15ms)
- 29 kbps - with encryption
- 66 kbps - with SHA1 authentication (+23B/message)
- 285 kbps - 18B message, 13 messages/ 15ms, SHA1 encryption
- Both encryption and SHA1 require more complex FPGA / ASIC design of to be part of the communication system
- SHA1 is a NSA standard HMAC authentication method
Conclusions

- Analog, centralized control systems have access to all information at all times.
- Digital, distributed control systems have information availability and synchronization challenges.
- Control network modelling allows important exploration of the various limitations imposed by including a network in a control system.
- Empirical methods were used to analyze the data flow in multi-drop networks for the purpose of developing models for simulation.
- Additional concerns about data integrity and authentication will impact resource utilization.
- The network models will be used to explore control system design space and build recommendations on network requirements.
Questions?