OEM Perspective on Aircraft Network and Time Triggered Technology

Bellevue, Washington – EUA, 13-14 November 2008

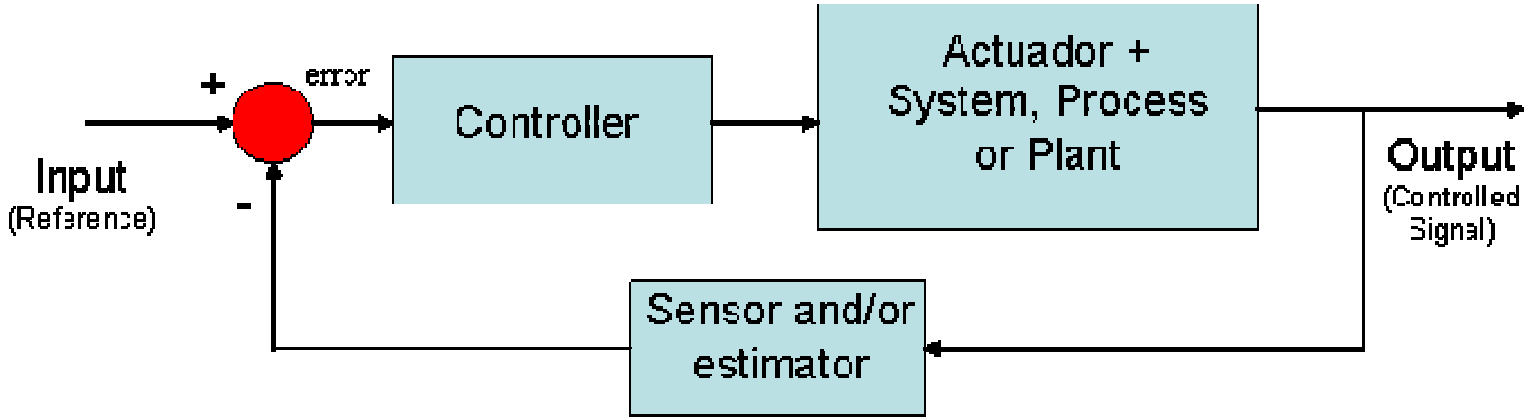
Herminio Duque Lustosa
herminio.lustosa@embraer.com.br

Summary

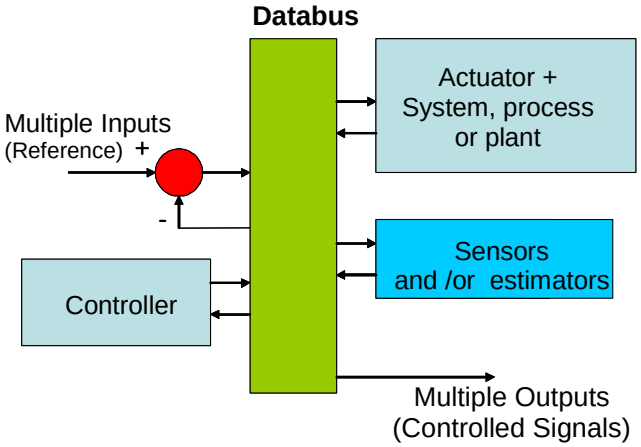
- Network in Control Systems
- OEM Perspective on Aircraft Network
- Types of Applications
- Network Topologies
- COTS in Aeronautical Solutions
- Event-Triggered architecture
- Time-Triggered Architecture
- Time and Event Triggered – Comparison
- Standardization of the TTP
- Embraer experiences with TTP
- Conclusions

Network in Control Systems

Simple Control System



Networked Control System



- more stringent requirements → large amount of data → product with better performance;
- network → simplification.

OEM Perspective on Aircraft Network

- Complex and highly integrated systems are already a reality, e.g. E-Jets 170, 175, 190 and 195
- Network is an efficient way to save weight in electric harnesses;
- Modular architecture which allows composability;
- Development challenges:
  - lack expertise of OEM system integrators and system suppliers;
  - lack of standardization;
  - lack of simulation tools.

- Certification challenges:
  - Overleap paradigms;
  - lack of field experience;
  - expertise of certification authorities.

OEM Perspective on Aircraft Network

- About TTP:
  - A dedicated company to support activities and provide tools;
  - Only one supplier for the TTP chip.
- Next steps:
  - integrate systems with different levels of criticality in same network;
  - dedicated certification guidelines (AC-27 by FAA – AVIATION DATABUS ASSURANCE)

Types of Applications

- **Safety-critical applications** - A safety-critical application is an application whose failure or malfunction may result in:
  - **death** of or serious **injury to people**, or
  - **loss** or severe damage to **equipment** or
  - environmental harm.
  - designed to have a **probability of failure of less than 10^{-9}** per flight hour.
  - similar applications in **military aircraft** are several orders of magnitude less demanding, with a probability of failure typically around or **less than 10^{-7} per flight hour** (presumably because the crew can bail out).

* TTP is suitable mainly for critical applications and applications stringent with time.

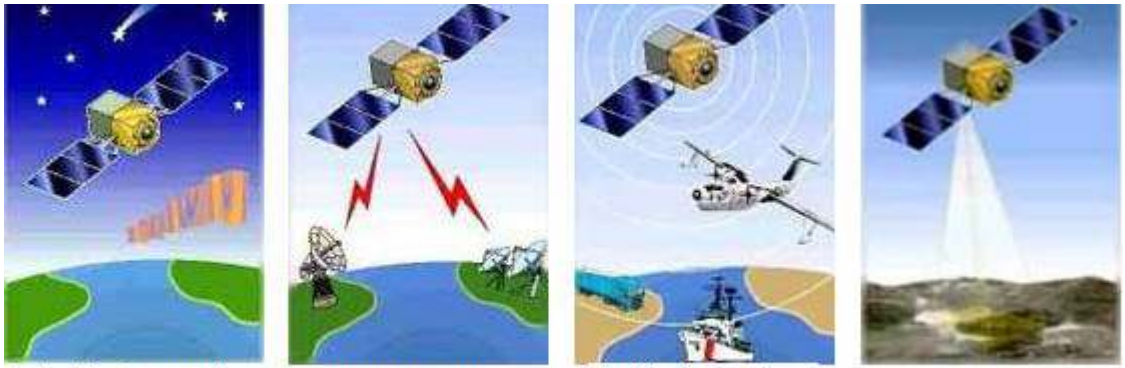
Types of Applications

- **<u>Vehicle-critical applications</u>** – The **cost of the failure** is huge economic penalty rather than loss of life.
  - Designed to have **probabilities of failure less than 10^{-6} to 10^{-7}** per hour of operation.

* TTP is suitable.

Types of Applications

- **<u>Mission-critical applications</u>** – In which a **failure of equipment**, e.g. computer, can cause **an incomplete or aborted mission**.
  - Typical probabilities of failure are **less than 10^{-4} to 10^{-7}** per hour of mission.
  - These applications **do not have so stringent response time**, but typically they need **higher throughput** to process more functions and amount of data.



* TTP is suitable for embedded applications.

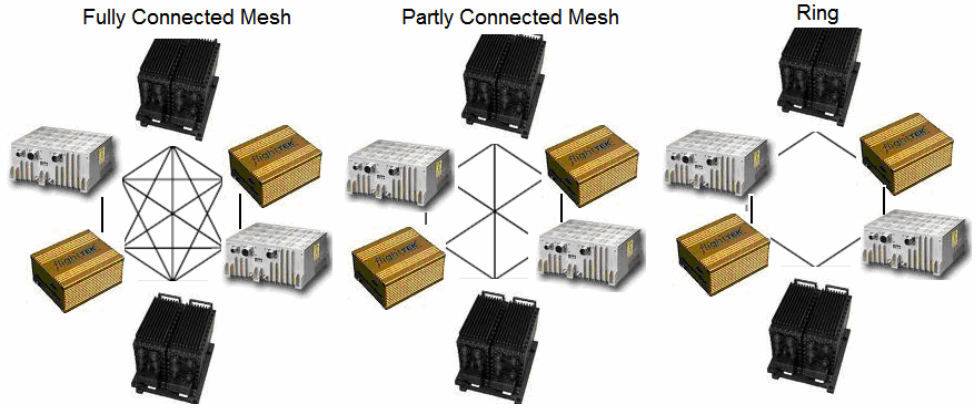
Types of Applications

- **On-line transaction processors (OLTP's)** – by contrast this type of application demand high availability, i.e. uptime, rather than high reliability.
  - **Incorrect operations** can usually be found through audits and **rolled back after the fact**.
  - OLTP applications can **withstand a delay** of seconds to process transactions.
  - The validation of these applications is not so formal.

* TTP is beyond the system requirements.

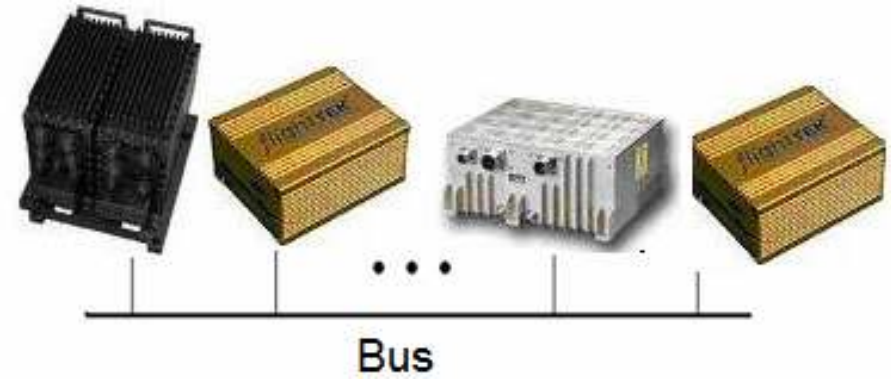
Network Topologies

- Point-to-point



• Very well accepted by the certification authorities – clear determinism;
• Challenge: fault containment and isolation.

- Bus interconnection

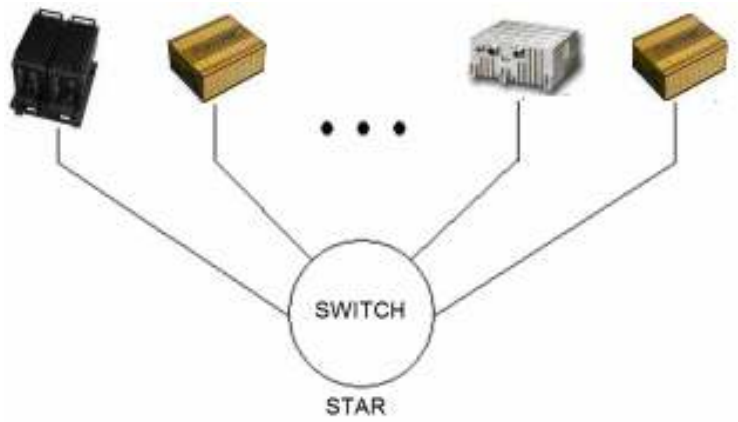


• Single point of failure: bus (properly), e.g. short-circuit;
• No compensation of signal attenuation;
• Very large diffused.

* TTP supports it

Network Topologies

- Star interconnection



• Single point of failure: star (hub);
• Compensation of signal attenuation;
• Not so common in Aeronautics solutions;
• Capable to isolate and contain failures in the branches.

* TTP supports it

COTS in Aeronautical Solutions

EMBRAER

❑ COTS (Components Of The Shelf) in Aeronautics:

➢ It took more than **15 years to adopt COTS** – nowadays several key components, e.g. databuses, are commonly applied in this form.

➢ **Problems related to COTS** components in Aeronautics:

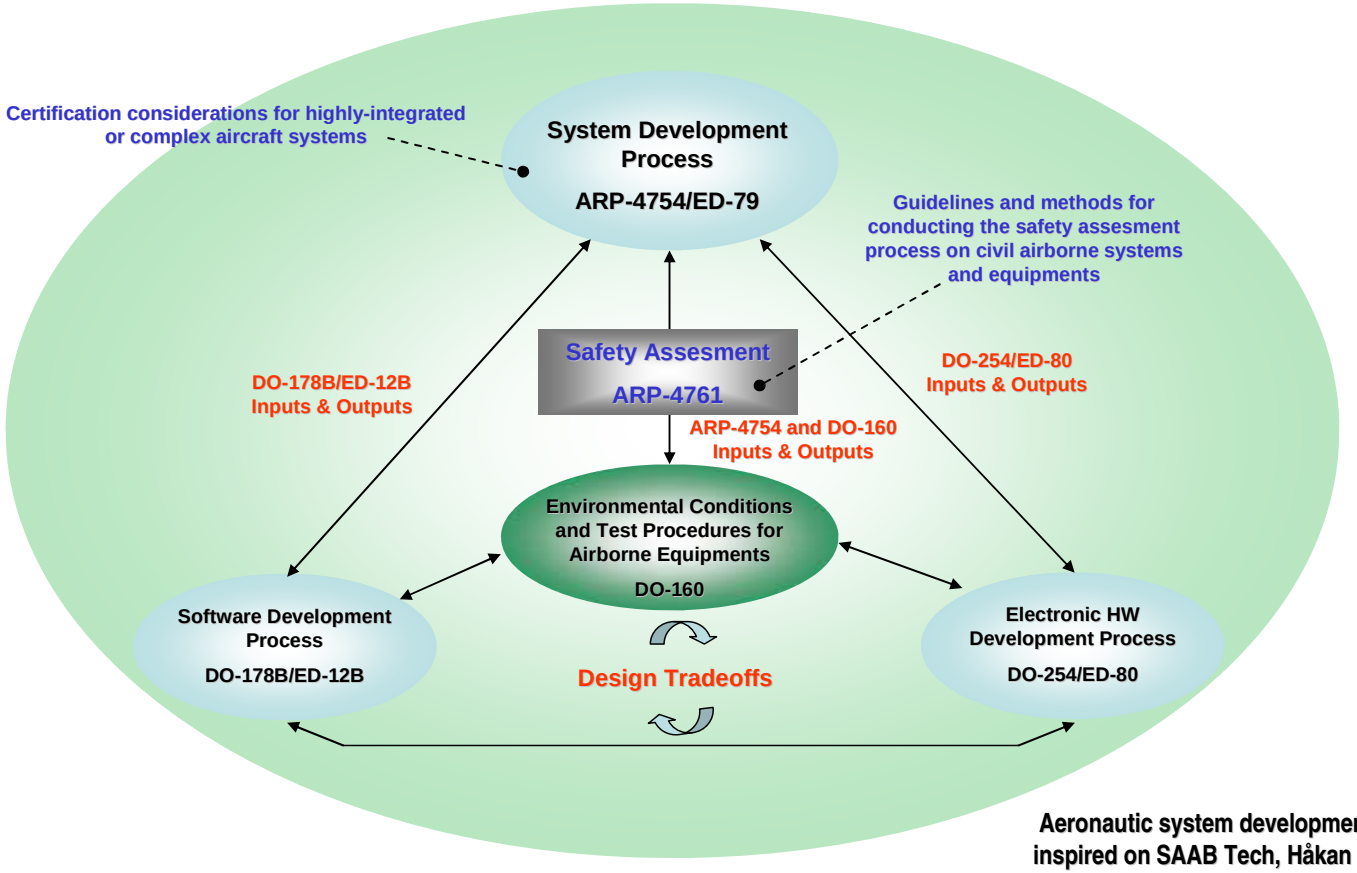
- Short commercial life (obsolescence factor); TTP = NOT OK
- Extended temperature range; TTP = OK
- Incomplete specifications; TTP = OK
- Lack of support in safety, security and certification issues; TTP = OK

COTS in Aeronautical Solutions

- Products developed by the Aeronautic industry shall meet a very long **life-cycle** (~30 years);
- **Natural tendency:** COTS (microprocessors, PLDs, databuses etc.) developed in/for the Automotive industry have been applied in the Aeronautic products;
- **Challenges:** certification guidelines more restrictive to cover aspects not covered that are essential to the Aeronautics.

COTS in Aeronautical Solutions

- The **Aeronautics demands are very low versus the Automotive demands to drive its design requirements**, then the cost to be paid is the **individual qualification** as follows:



Aeronautic system development process inspired on SAAB Tech, Håkan Forsberg, 2004

COTS in Aeronautical Solutions

- The rules ARP-4754, ARP-4761 and DO-178B are commonly applied to any aeronautic design independent on use of COTS;

- **RTCA DO-160** defines a series of minimum standard **environmental test conditions** (categories) and applicable test procedures for airborne equipment, with the purpose to provide a laboratory means of determining the performance characteristics of airborne equipment in environmental conditions representative of its applications;

- **RTCA DO-254** is an industry standard written specifically for complex electronic hardware and requested in case of use of COTS. The standard provides guidance for design assurance during the development of airborne electronic hardware such that the hardware performs its intended function in a specified environment.

COTS in Aeronautical Solutions

- **HW Design Assurance**
  - **RTCA DO-254 defines system development assurance levels:**

A. Catastrophic

B. Hazardous/severe-major

C. Major

D. Minor

E. No effect

  - Additional information:
    - DO-254 has ~30% more objectives than DO-178B;
    - For level A up to 27 documents must be produced to demonstrate the complete qualification;
    - Painful and expensive to qualify changes after certification.

COTS in Aeronautical Solutions

EMBRAER

- **Additional Design Assurance Issues:**
  - **Architectural mitigation techniques** such as dissimilar implementation, redundancy, monitors, isolation, partitioning etc. For example, in a Flight Controls application that adopts TTP as a main databus, it is necessary to have something dissimilar in a critical path way of command, e.g., CAN Bus, A-429 etc.;
  - **Product service experience**, which is applicable whenever functions that use previously developed hardware are used as a part of the design;
  - **Advanced verification methods** such as elemental analysis, safety-specific analysis or formal methods.

TTP Field Experience

- Large application on Automotive Industry;
- Aeronautic applications:
  - A380: Cabin Pressure – DAL “B” – certified and in service;

  - B787: Electric system – Level “A” – under certification;

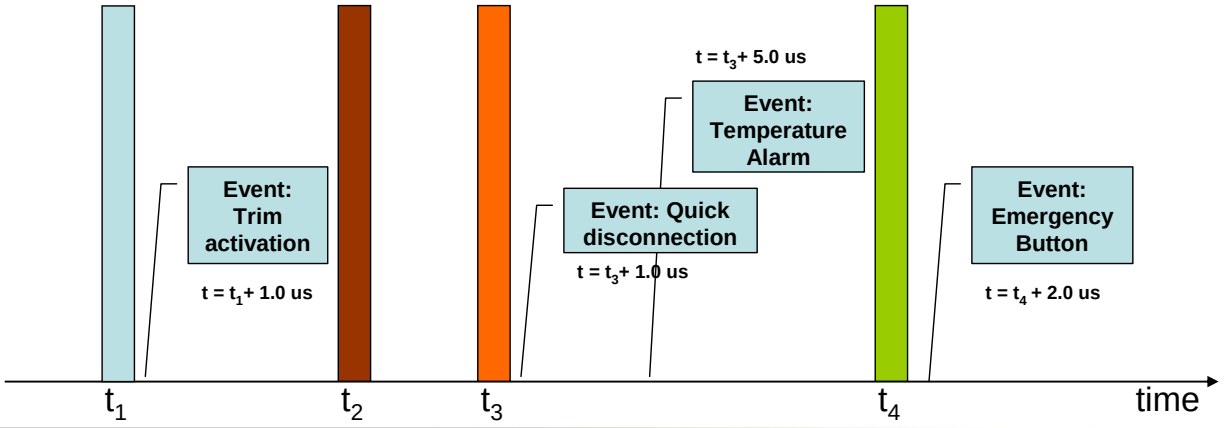
  - Honeywell FADEC – Aermacchi M-346 and Lockheed Martin F-16 – certified – DAL “A” defense.

Event-Triggered Architecture

- Event-triggered architecture is a system architecture pattern promoting the production, detection, consumption and reaction to events.
- An event can be defined as "a significant change in state". For example, activation of an emergency button;
- Example: like CAN Bus and ARIN-429.

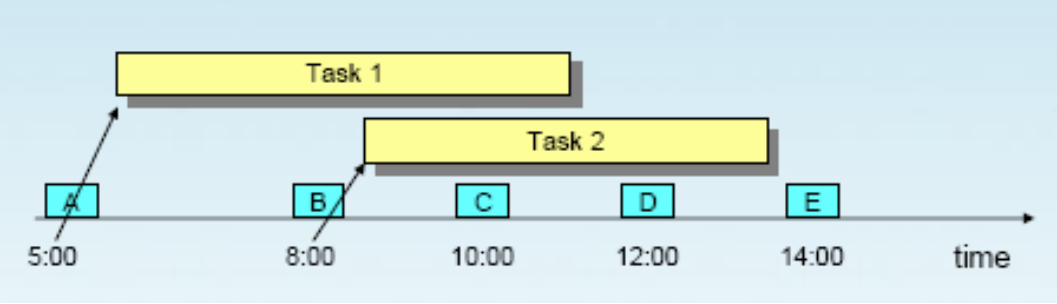
Time-Triggered Architecture

- A **real-time system is Time-Triggered** (TT) if the control signals are derived from the progression of a notion of time, triggering actions such as
  - ✓ sending and receiving messages
  - ✓ activation of tasks
  - ✓ recognition of external state changes
- The exact moments of event occurrences can be time-stamped locally, but do not trigger any other activity (especially transmissions).

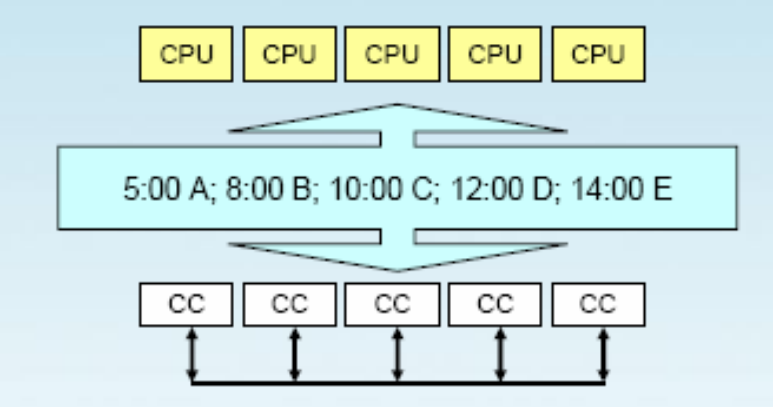


Time-Triggered Architecture

- The communication system operates in a time-triggered, i.e., it is based on global-time to manage all transmission activity;
- The applications can utilize this communication system global-time to manage their own activities;
- Between application and communication system, there is a well-defined interface with properties established at design time ("schedule");
- The timing properties of this interface are ***globally specified***.



Source: TTTECH



Source: TTTECH

Time and Event Triggered - Comparison

EMBRAER

❑ Time-Triggered

- ✓ high predictability
- ✓ high design effort
- ✓ deterministic testing due to clear timing behaviour
- ✓ extensibility easy only if planned in system schedule
- ✓ always composable

❑ Event-Triggered

- ✓ low predictability
- ✓ design allows grey areas
- ✓ large number of test cases
- ✓ easy extensibility by simply adding new nodes/identifiers
- ✓ not usually composable

❑ **FlexRay®** is an initiative that conciliates both concepts in the same databus.

Standardization of the TTP

- **SAE standardization of TTP bus is in progress;**
- **Benefits of a TTP standardization:**
  - Ensures compatible physical implementations;
  - Enables common test/maintenance equipment;
  - Leverages industry investments;
  - Ensures openness and enables multiple component and tool suppliers;
  - Identify specific characteristics of TTP that shall be addressed on the standardization.

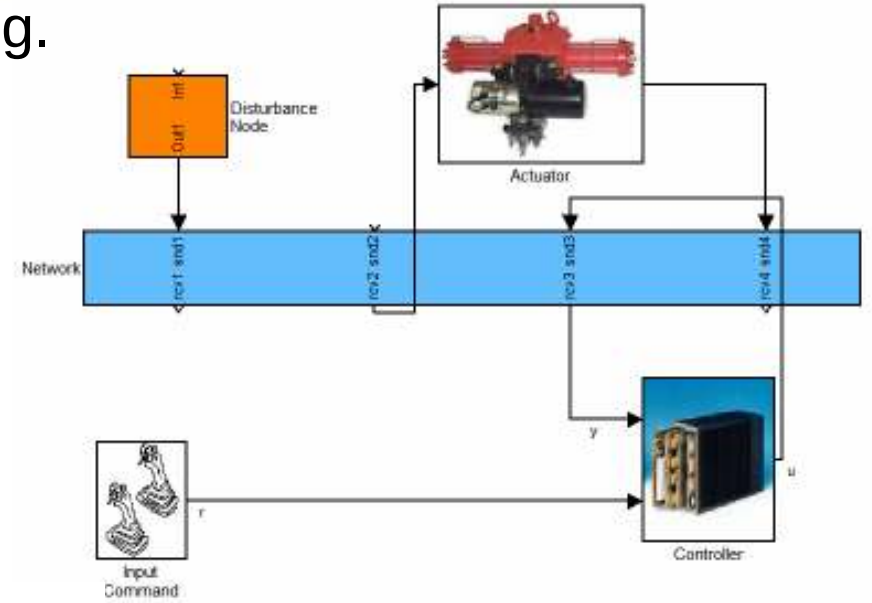
EMBRAER supports the standardization of the TTP databus as an SAE standard for usage on our future systems/aircraft and cross-industry applications.

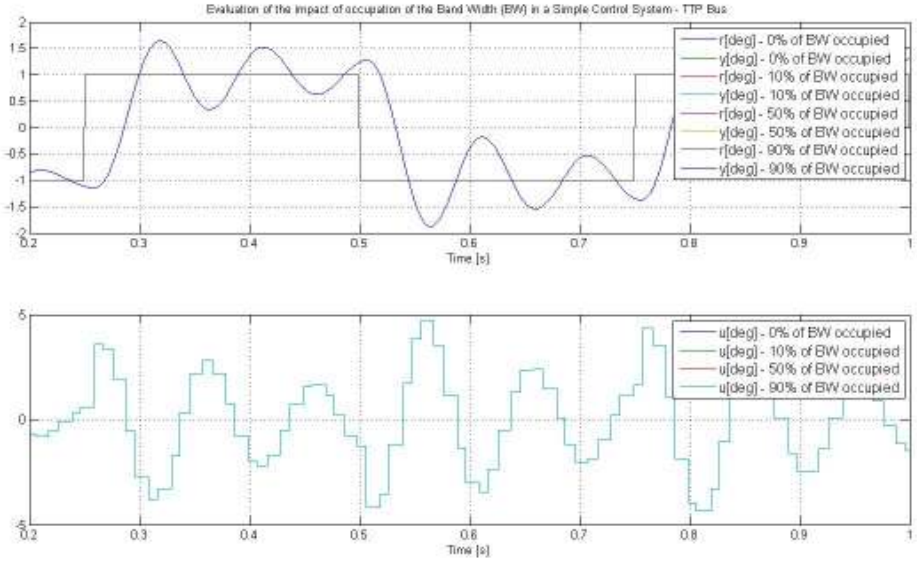
TTP Potential Use and Risk Evaluation

- Physical layer:
  - Definition of the type of wiring harness;
  - EMI/EMC levels;
  - Handling of the wiring, connections and routing for installation purposes.
- Integration between application and databus
  - RTOS specification
  - The application of TTP defines the concept of the System Architecture as time triggered.
- As the number of earlier applications are too low; and none civilian with DAL “A”, then the level of severity required by FAA, EASA and ANAC will be very hard.
- System integration benefits: time deterministic, composability and masterless.

EMBRAER Experiences With TTP

- Evaluation of simulation tools, e.g. TrueTime®:
  - Robustness to bus traffic variations;
  - Robustness to BW variations.
- Planning to have productive experiments.





Parameter	% of BW occupied - TTP Bus (TDMA) - BW = 90 Kbps			
	0%	10%	50%	90%
Peak value [deg]	1.642	1.642	1.642	1.642
instant of the peak [s]	0.319	0.319	0.319	0.319
overshoot [%]	64.20%	64.20%	64.20%	64.20%
Settling time [s]*	>> 0,25	>> 0,25	>> 0,25	>> 0,25

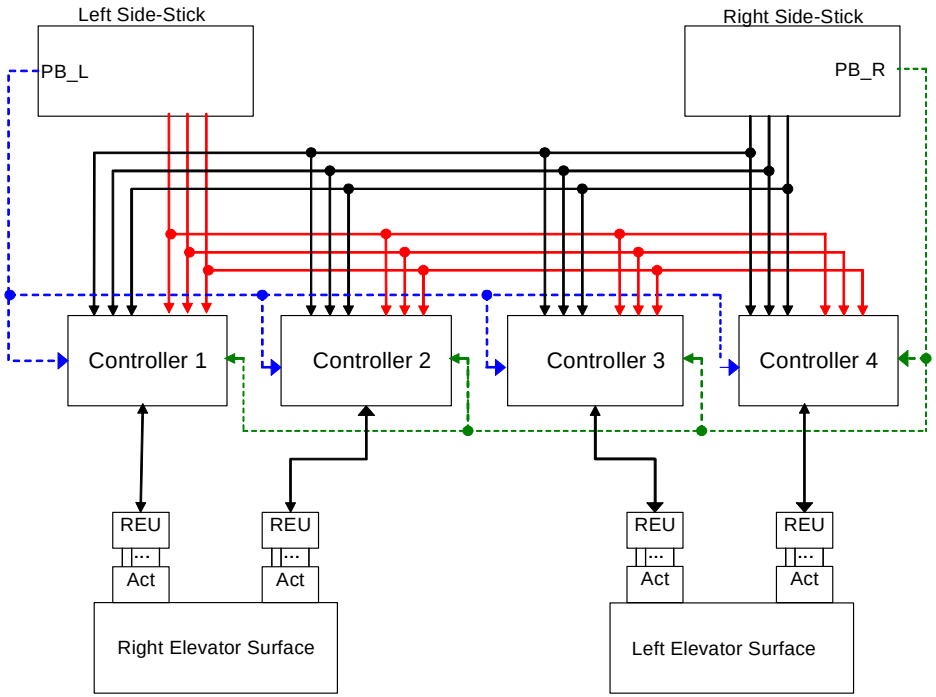
* in reference to the raising edge of the input

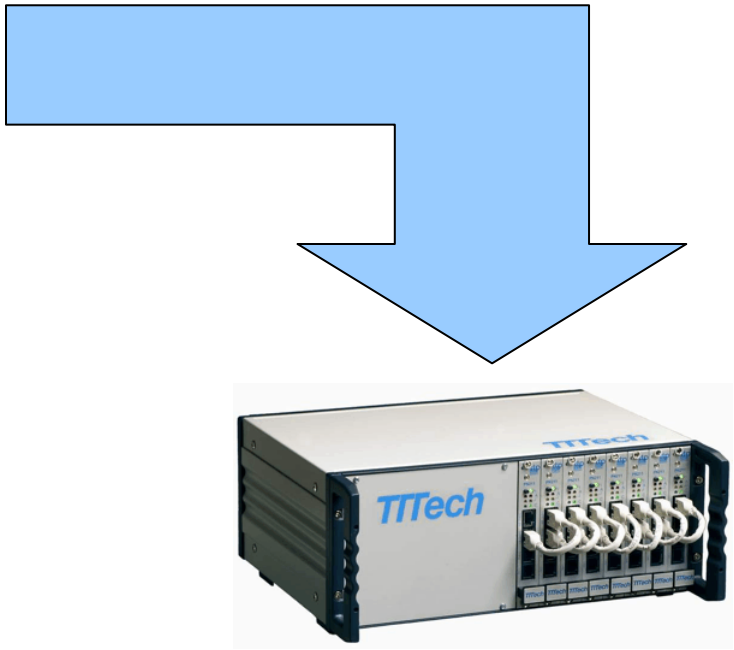
Test Results - Discussions

- The simulation performed before to the real implementation improve the efficiency of the process, but the model shall be validated in comparison with the real hardware;
- The simulation is complementary to a complete evaluation that requests theoretical analysis and implementation in a real hardware.

EMBRAER Experiences With TTP

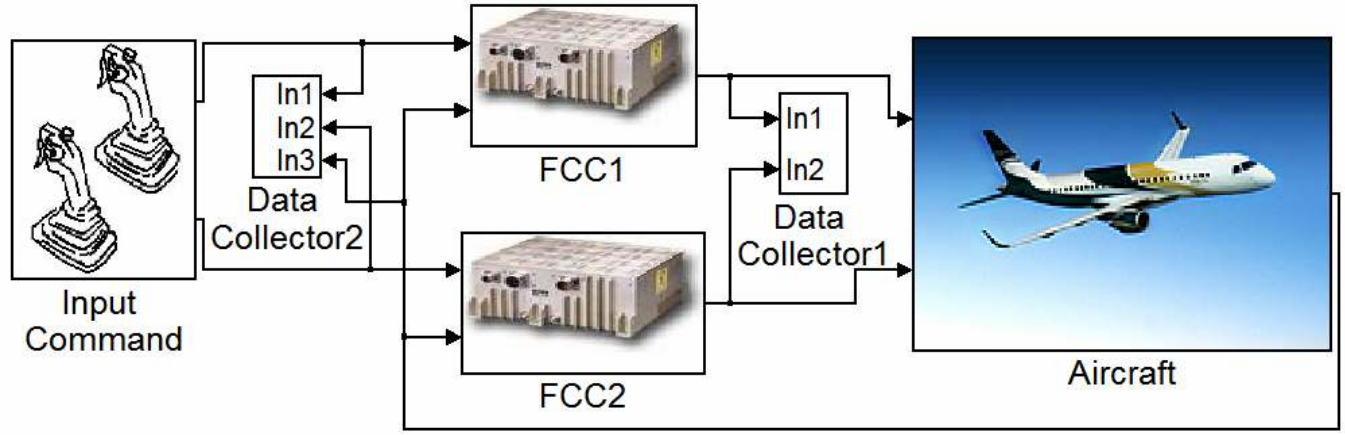
- **Pilot project**
  - Simulation of a simple elevator controller in real time;
  - Closed-loop control laws.

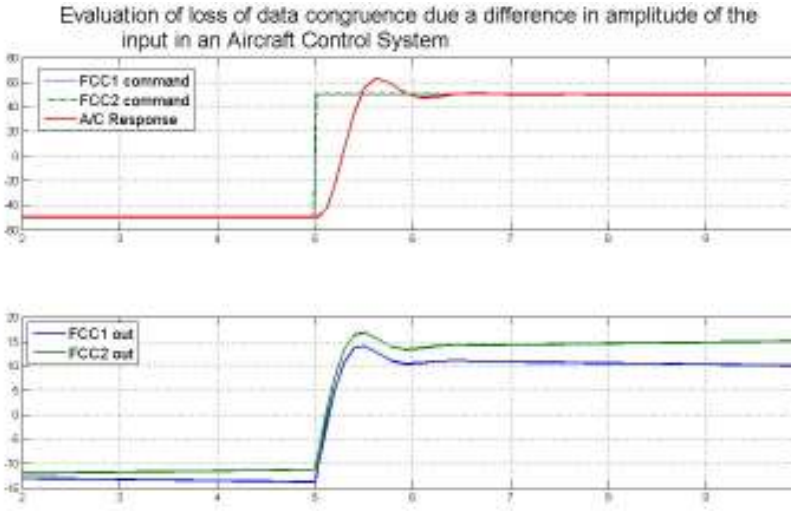


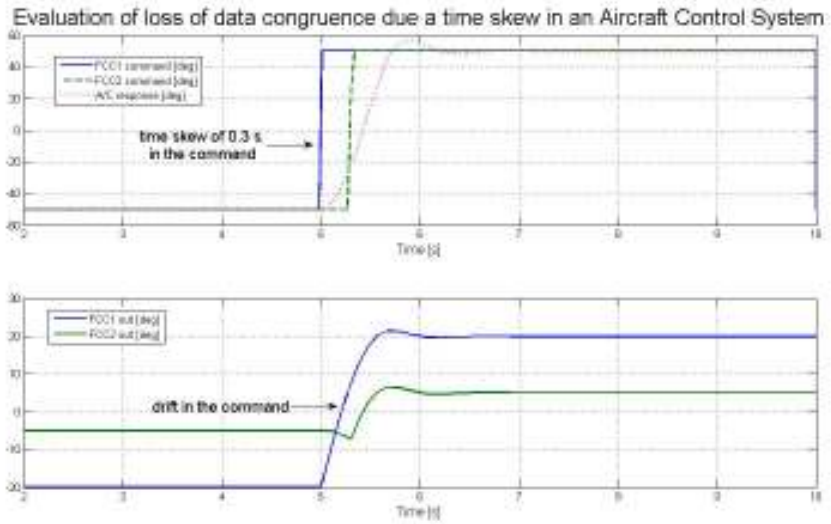


Contribution: Embraer/FBW-SCE/GRIJO, L.F., 2007.

Motivation: Data Congruence



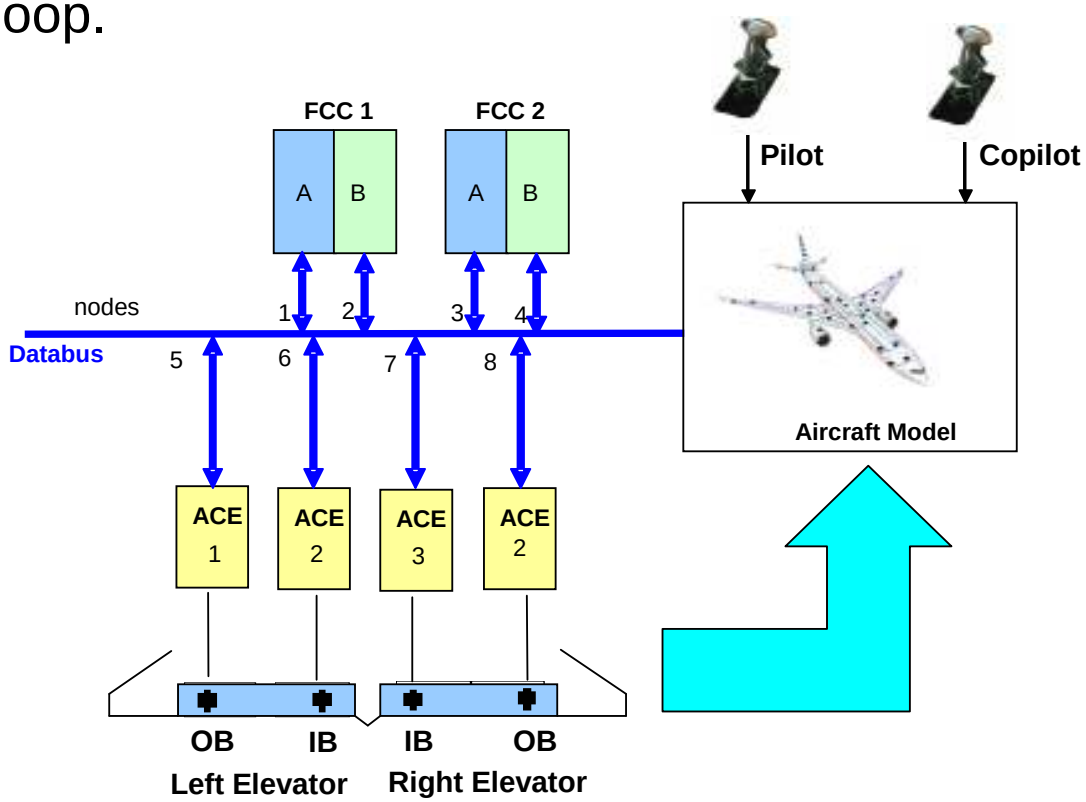




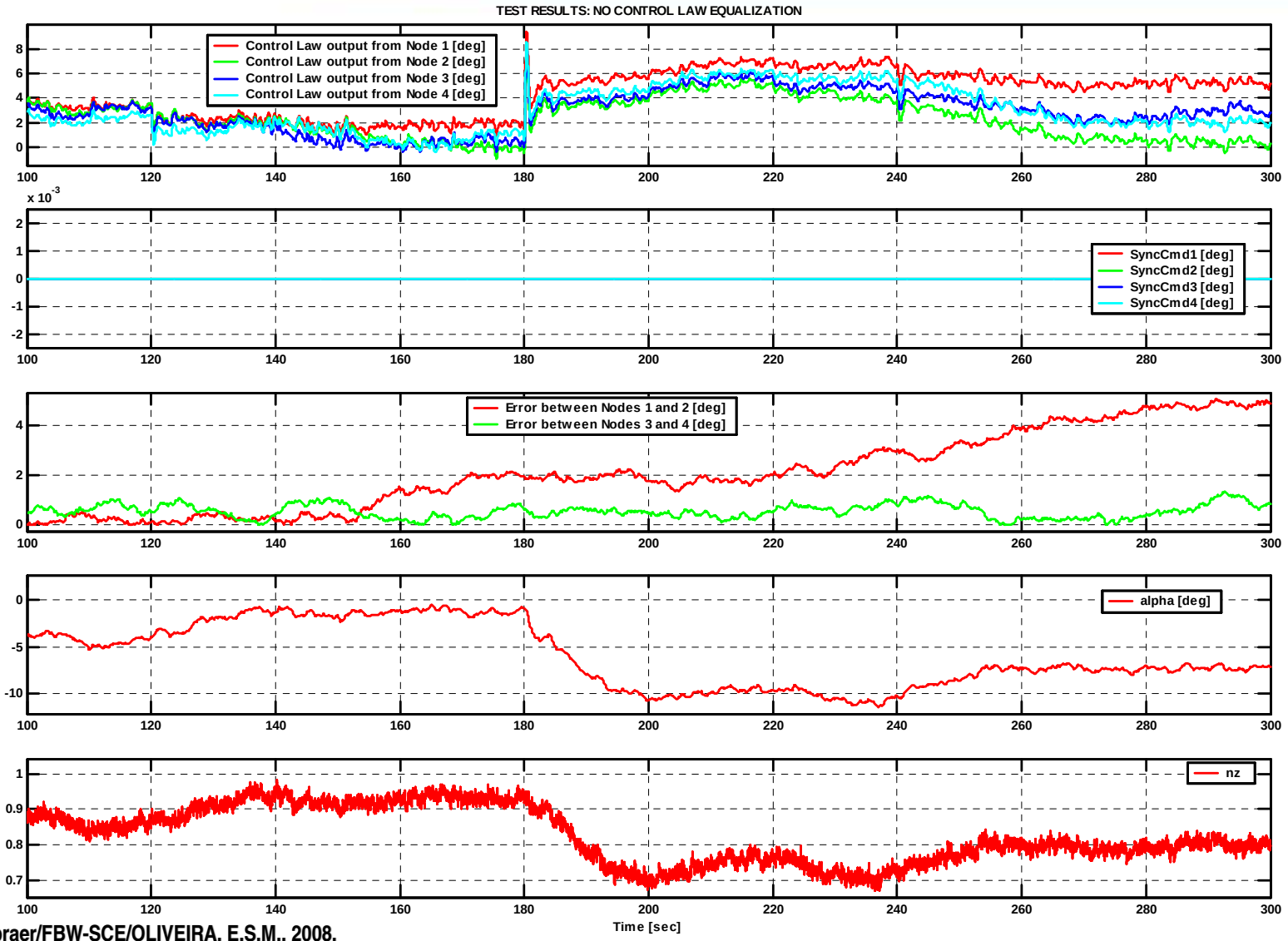
EMBRAER Experiences With TTP

❑ Synchronism of integrators trough TTP:

- ➢ The control law acts over the longitudinal axis of the airplane. The longitudinal axis is controlled by four actuators;
- ➢ The Actuator Control Electronics (ACEs) process the actuator commands which will be consumed by the airplane model closing the loop.

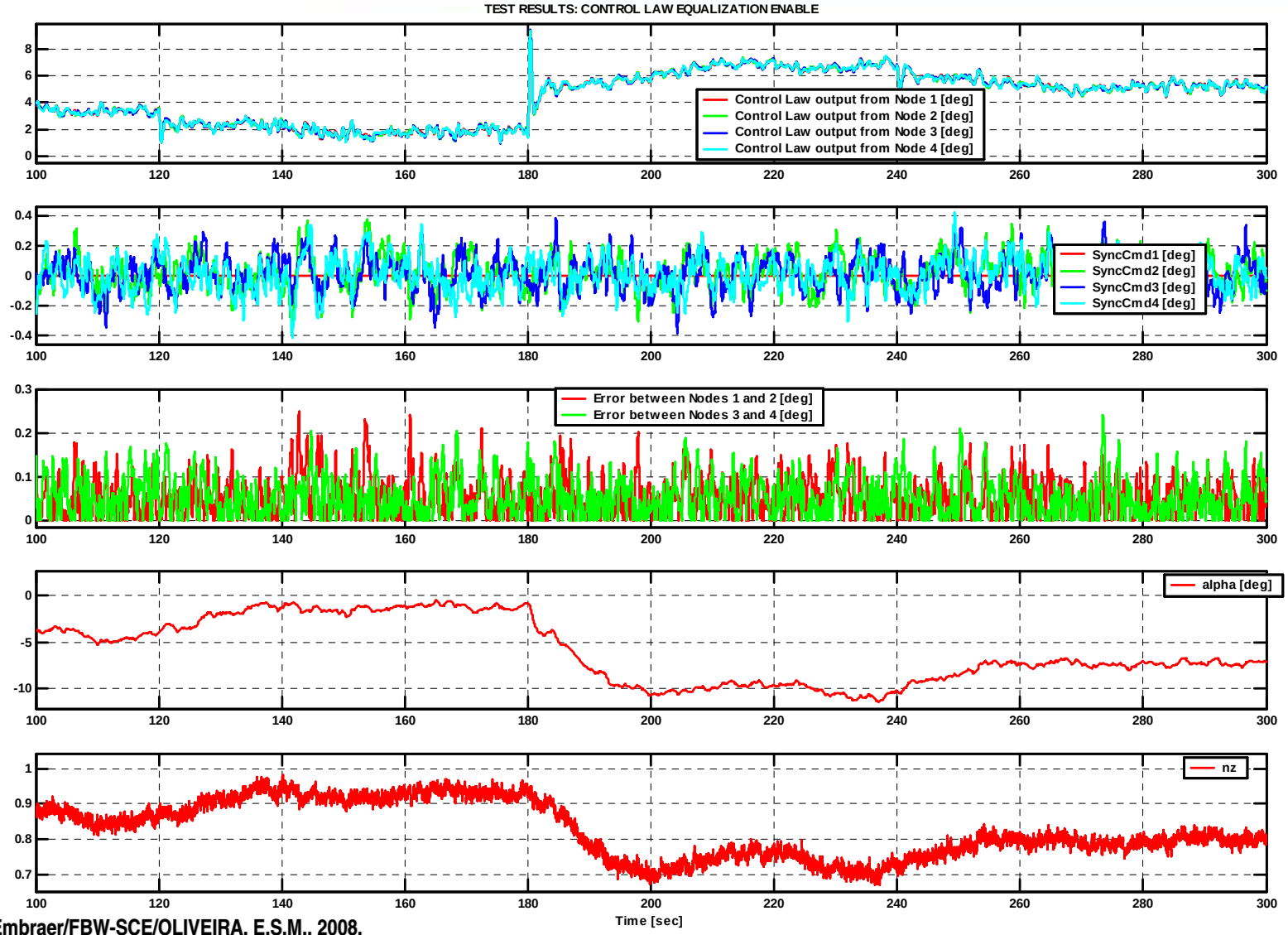


Test Results – no integrators synchronization



Contribution: Embraer/FBW-SCE/OLIVEIRA, E.S.M., 2008.

Test Results – integrators synchronization



Contribution: Embraer/FBW-SCE/OLIVEIRA, E.S.M., 2008.

Test Results - Discussions

- The TTP Bus improves the system to synchronize mathematical integrations embedded in different processors, however it does not solve the problem completely;
- Considerations about the TTP Cluster and tools:
  - Powerful tool to evaluate, in advance, solutions to be implemented in the final target;
  - Power up and electric transients evaluation;
  - The tools to debug the software are not satisfactorily efficient. It is necessary to instrument the software to do it.
- The TTP development tools were considered useful and friendly;
- The technical support provided by TTP supplier has been very good;

Conclusions

- The documents about TTP bus presents a satisfactory level of completeness;
- Certification as per FAR/JAR-25 has been under evaluation; up to this moment it has concluded the following:
  - It is mandatory to have an architectural mitigation, e.g., dissimilar redundancy in the critical path way of command;
  - Physical layer shall be very carefully defined, tested and qualified.
- TTP is suitable for flight test instrumentation – compliant with FAR/JAR 25.1301:
  - Easy plug-in of slaves or monitor nodes;
  - Loss of slaves does not affect the communication.

Conclusions

- As the time-triggered philosophy brings determinism to the system, we expect to have in the future a **portable architecture**, more robust and with an enhanced level of safety;
- The TTP Bus has potential to be integrated in an Aeronautic final product in a safety critical system.

Acknowledgements

✓ *TTTech for the invitation;*

✓ *EMBRAER for the authorization to participate of this Forum and the technical contributions of Luiz F. Grijo and Eduardo S. M. Oliveira.*

✓ *INPE (Prof. Dr. Marcelo L. O. Souza) for the technical support in the Master Degree, which has a subject correlated with this presentation.*

OEM Perspective on Aircraft Network and Time Triggered Technology

Thank you!

Bellevue, Washington – EUA, 13-14 November 2008

Herminio Duque Lustosa
herminio.lustosa@embraer.com.br