Networking in Modern Avionics: Challenges and Opportunities

Sérgio D. Penna
EMBRAER
Avenida Brigadeiro Faria Lima, 2170
12227-901 - São José dos Campos - Brazil
+55-12-3927 4067
sdpenna@embraer.com.br

ABSTRACT
This paper provides an overview of three important emerging standards in modern Avionics - ARINC-664 Part 7 (AFDX), TTP and ARINC-653 - and addresses challenges and opportunities arising from their adoption. Beyond several potential benefits offered by these standards, additional effort should be expected by practitioners when system design requires, for instance, timing analysis for estimating data transmission jitter. This paper presents some of these design challenges and suggests new academic research opportunities for, for instance, extending current timing analysis methods for distributed systems.

Categories and Subject Descriptors
J.2 [**Computer Science**]: Physical Sciences and Engineering – *Digital Data Communication Networks*. C.2.2 [Computer Systems Organization]: Computer Communication Networks - Network Protocols.

General Terms
Avionics, Networking.

Keywords
Networking, Avionics, Digital Data Bus, Time-Triggered Architecture, Operating Systems, Partitioning.

1. INTRODUCTION
The introduction of "Integrated Modular Avionics" (IMA) by the Radio Technical Commission for Aeronautics (RTCA DO-297) in November 2005 [1] gave focus to new industry standards. "Avionics Full Duplex Switched Network" (ARINC 644 Part 7 "AFDX") [2], "Time-Triggered Protocol" (TTA Group "TTP") [3] and "Application Executive interface" (ARINC 653 "APEX") [4] emerged offering new levels of modularity and communality to avionic systems. These standards present new challenges for system manufacturers and integrators, but offer new opportunities to improve current analytical methods for predicting system behavior during the design phase.

2. CURRENT AVIONICS DESIGN
Previous avionics systems were dominated by what was commonly called "Federated Architecture", whereby one function or application was confined in one "black box". In federated systems, these "black boxes" communicate through digital buses such as ARINC-429, which provided a point-to-point single-channel communication, or MIL-STD-1553, which provided an arbitrated data bus.

Such architecture led sometimes to excessive cabling, for one box needed to be physically connected to multiple other boxes, so applications could exchange data.

More recently, with the introduction of "IMA - Integrated Modular Avionics", concept formalized in 2005 as the Radio Technical Commission for Aeronautics (RTCA) standard DO-297 "Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations", things began to change.

With IMA, one box could host more than one application, so boxes became cabinets populated with multiple processing and input-output modules. New digital data buses, such as AFDX and TTP, appeared offering better ways of exchanging data among different applications. The use of COTS technologies, in particular Ethernet/IP networking became ubiquitous for obvious reasons, given the multitude of hardware and software resources and academic research around it.

However, not only data communication became a concern under IMA. Software Certification issues and the desire to free application from underlying proprietary operating system software interface favored the advent of another standard ARINC-653 "Avionics Application Software Standard Interface", which enforces not only one single software interface between applications and operating system services, but also impose a strict logical separation between applications running in the same processing module.

The next paragraphs will detail more these three important standards: AFDX, TTP and ARINC-653 at the new challenges system designers and opportunities for academic researchers.

3. THE "AFDX" STANDARD
The "AFDX" standard is the Part 7 of the ARINC-664 "Aircraft Data Network" standard, called "Avionics Full Duplex Switched Ethernet Network" introduced formally in 2005. It describes a "more deterministic" switched Ethernet/IP network, that is, a switched network where a few constraints are applied. On the transmitting end, called "End-System", a data transmission rate is associated to one virtual multicast unidirectional communication channel called "Virtual Link", or VL in terms of a "Bandwidth Allocation Gap", or BAG measured in milliseconds, and a

maximum frame size, called "Lmax" measured in bytes. Thus, the rate is defined as "Lmax/BAG" and is defined per VL.

Since a switched network implies the use of a switch, this piece of hardware became crucial to the design of the network. An AFDX Switch does not only perform packet forwarding as usual, but also enforces Traffic Policing at its input ports. This feature is based in the "Token Bucket" algorithm and discards packets that arrive in a pace faster than "Jswitch" milliseconds. This "Jswitch" quantity is programmed in the AFDX switch and is defined per VL. With Traffic Policing, the AFDX switch protects the network from what is usually called "babbling idiot", a misbehaved node that transmits more that than it is designed to.

The AFDX data frame uses a suffix (lower 16 bits) in its multicast MAC Destination Address to define a VL. The remainder of the frame takes its model from UDP/IP with one difference: the last byte is reserved for count frames from 1 to 255, a quantity used in AFDX'es "Redundancy Management". The AFDX network uses two physically separated channels, so each AFDX "End- System" transmits the same data frame in these two channels at the same time. In the receiving "End- System", the "Sequence Number" is used by the "Redundancy Manager" to discard frame copies that arrive too late.

Designers of an AFDX network need to take into account several potential sources of transmission jitter. On the transmitting "End-System", frames are queued before reaching the physical medium. Inside the AFDX switch, forwarded frames are queued in the output port before they depart to their destination node. The measure of jitter is relevant to the AFDX network design, for the "Jswitch" quantity must be correctly estimated and programmed in the switch for each VL.

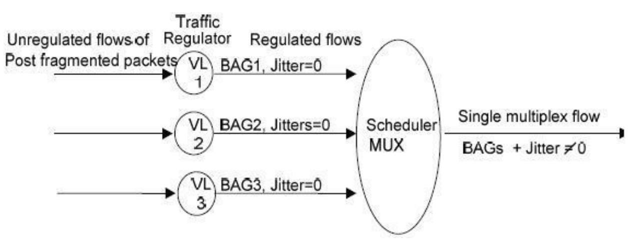

Figure 1. Virtual Link Flow Regulation in AFDX.

Adapted from ARINC-664 Part 7, Page 12 – Figure3-6.

Figure 1 shows how traffic flow is regulated on a transmitting AFDX End-System. Note that transmission jitter should be expected after messages are produced at a rate equal to BAG for each VL.

4. THE "TTP" STANDARD

The "Time-Triggered Protocol" (TTP) was introduced in 2003 by the "Time-Triggered Architecture Group" (TTA-Group) and has been recently adopted by SAE as the AS6003 standard.

The basic principle of TTP communication is "Time-Division Multiple Access" (TDMA). TTP nodes are time-synchronized and are allowed to transmit using the full speed of the physical medium for a limited time period. TTP node transmits in turns according to a precise schedule recoded in the "Message Description List" copied in each TTP node before operation starts. Each TTP node has one reserved transmission "Slot", many "Slots" form a "Round", and many "Rounds" form a "TTP cluster". "Rounds" are usually short in the order of a few milliseconds and "TTP Clusters" are as long as a few tens of milliseconds.

Messages transmitted in each "Slot" can be as long as 240 bytes and the format is application dependent. Clock synchronization is achieved using an distributed clock correction algorithm described as "Fault Tolerant Average" (FTA) [5]. The TTP network has two physically separated channels that can be used in redundancy or as two independent channels.

Designers of a TTP network need to take into account the period and the execution time of the applications that transmit and receive data, for its is essential for time-critical applications, such as a Flight Control System, that the data produced is consumed as early as possible.

Figure 2 shows a typical TTP Cluster taken from TTTech's "Brake-by-Wire" book example, as displayed by TTPlan®, TTTech's own TTP configuration tool. It has 7 slots and 4 rounds of 2,500 microseconds each. Note that, in this case, the two physical channels are used independently to transmit different size messages.

5. THE ARINC-653 STANDARD

The ARINC-653 standard was formally introduced in 2005. In its words: "The primary objective of this Specification is to define a general-purpose APEX (APplication/EXecutive) interface between the Operating System (O/S) of an avionics computer resource and the application software". This standard introduces two important concepts: "Temporal Partitioning" and "Spatial Partitioning".

"Temporal Partitioning" is realized by the introduction of a fixed periodic scheduling of "Partitions", a limited time-window where applications are allowed to execute. "Spatial Partitioning" is realized by the definition of each "Partition" virtual address space at system startup. This logical separation allows applications of different criticality levels (as defined in the ARP-4754 standards) to run in the same processing module.

Furthermore, the ARINC-653 standard defines a complete set of operating system services for managing partitions, processes and data communication within a partition and between partitions. The latter introduces the concept of "ports", which in turn are immediately associated to UDP ports as used by AFDX networks.

System designers that decide for the ARINC-653 "APEX" face the challenge of not only having to estimate the execution time of tasks, but also to decide how long should be the duration of each partition where these tasks are expected to execute. Should an application exceed the allotted time-window of its partition, it will be suspended and resumed only in the next partition period.

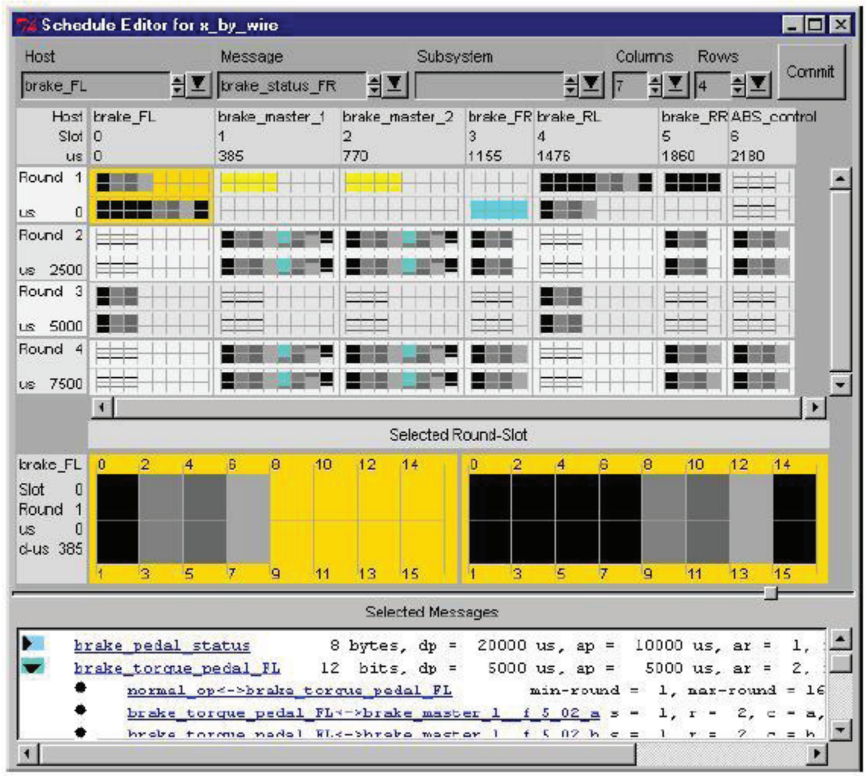

Figure 2. A typical TTP Cluster shown in TTPlan®.

Adapted from TTTech Computer Technik AG.

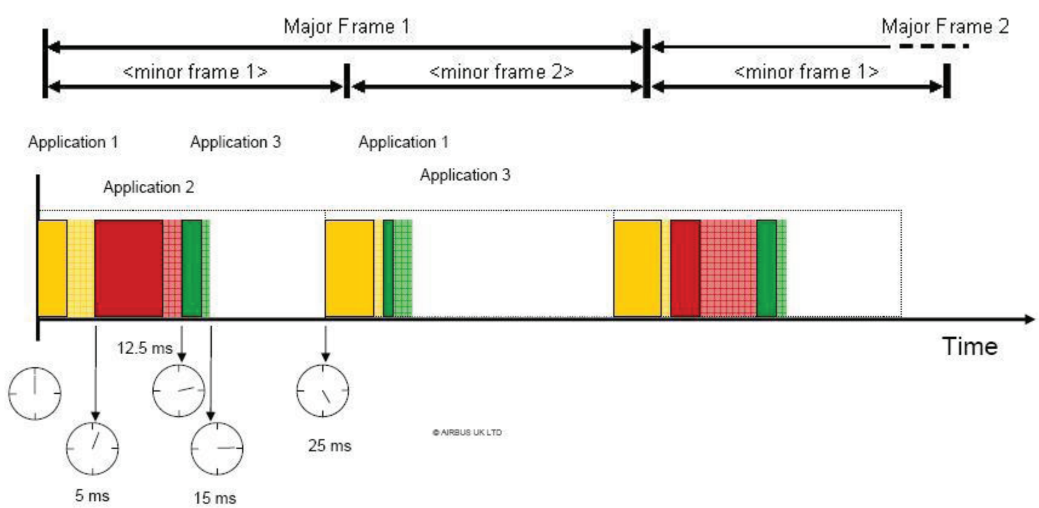

Figure 3. A typical temporal partitioning in ARINC-653.

Adapted from ARTIST2 – Integrated Modular Avionics A380.

Figure 3 shows one temporal partition configuration [6], where three applications (in colors yellow, red and green) occupy limited time windows within what is frequently called “minor frames”, where they are allowed to run until they either finish execution (spare time is indicated by a “checkered” colored pattern) or become suspended in favor of the next partition. Note that application “red” is allowed to run for time 5 to time 12.5 milliseconds in the first “minor-frame”, while applications “yellow” and “green” are allowed to run in the first and second “minor-frames”. Not also that the temporal behavior repeats itself every two “minor-frames” in what the standard calls “Major-Frame”.

6. CHALLENGES AND OPPORTUNITIES

System designers willing to adopt AFDX, TTP and ARINC-653 standards need to decide:

- ✓ For the AFDX network configuration: How many Virtual Links? How many AFDX Switches? What Bandwidth Allocation Gaps (BAGs) to choose?
- ✓ For the TTP Cluster configuration: How many Slots? How many Rounds? How big the messages should be?
- ✓ For the ARINC-653 processing load distribution: How many processing modules? How many partitions per module? How long should be the duration of each partition?

Further, issues about and time, as well as task synchronization should also be addressed and decided upon.

As for researchers, new design challenges offer great opportunities for:

- ✓ Extending current analysis methods: “Timing Analysis” should be able to analyse the entire distributed system, from task scheduling in processing modules to delays in message transmission and reception.
- ✓ Creating configuration and optimization tools: The bigger the system, the more automation should be in place for configuring and optimizing it (a lengthy analysis process is never practical).
- ✓ Pursuing further studies on time synchronization in distributed systems: Should hardware support for time synchronization always be in place? How good time synchronization using exclusively software should be?

In addition, the fact that the ARINC-653 standard offers little guidance for “extra-cabinet” communication offers another great opportunity for studies that eventually may fill in this important gap, avoiding OS supplier specific implementation and securing, true application portability.

7. CONCLUSION

With the introduction of IMA, new industry standards such as AFDX, TTP and APEX present new challenges for system manufacturers and integrators, but more important, opportunities for new academic endeavors, such as:

- ✓ Composition of AFDX, TTP and ARINC-653, extending current “Holistic Timing Analysis” methods for evaluating task WCRT/BCRT and message transmission jitter;
- ✓ Include “Data Aging” in the analysis;
- ✓ “Fill-in-the-blanks” where ARINC-653 left physical I/O unmapped (materialize “Pseudo Partitions”);
- ✓ Formally evaluate and recommend standard Time Synchronization Protocols for distributed systems, such as Network Timing Protocol (NTP) and IEEE-1588 Precision Time Protocol in time-critical applications;
- ✓ Could a “Virtual Machine Hypervisor” be an alternative to ARINC-653?

In the years to come, more theoretical studies shall be required as time-critical applications developed using AFDX, TTP and ARINC-653 mature.

8. REFERENCES

[1] RADIO TECHNICAL COMMISION FOR AERONAUTICS - RTCA DO-297: Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations. Washington D.C., USA, November 2005.

[2] AERONAUTICAL RADIO INCORPORATED - ARINC specification 664: Aircraft Data Networks – Part 7, Avionics Full-Duplex Switched Ethernet (AFDX) Network, June 27th, 2005.

[3] TTA-GROUP. Time-Triggered Protocol (TTP/C) High-Level Specification Document – Protocol Version 1.1, Edition 1.4.3, Vienna, Austria, November 19th, 2003.

[4] AERONAUTICAL RADIO INCORPORATED. ARINC specification 653P1-2: Avionics Application Software Standard Interface Part 1 – Required Services, December 1st, 2005.

[5] Kopetz H. and Ochsenreiter W. 1987. Clock Synchronization in Distributed Real-Time. In IEEE TRANSACTIONS ON COMPUTERS, Vol. C-36, No. 8 (August 1987), 933-940.

[6] Itier J.B. 2007. A380 Integrated Modular Avionics. http://www.artist-embedded.org/docs/Events/2007/IMA/Slides/ARTIST2_IMA_Itier.pdf. Accessed in November 24th.