Switched Ethernet is being implemented as an avionics communication architecture. A commercial standard (ARINC-664) and an aircraft vendor specific implementation known as Avionics Full Duplex Switched Ethernet (AFDX) have been developed that define the topology and use of Switched Ethernet in an avionics application.

This paper provides an overview of a Switched Ethernet avionics network and identifies the testing challenges associated with a Switched Ethernet avionics application.
ABSTRACT

Switched Ethernet is being implemented as an avionics communication architecture. A commercial standard (ARINC664) and an aircraft vendor specific implementation known as Avionics Full Duplex Switched Ethernet (AFDX) have been developed that define the topology and use of Switched Ethernet in an avionics application. In avionics applications, the movement of data between devices must take place in a deterministic fashion and needs to be delivered very reliably. All aircraft flight hardware needs to be tested to be sure that it will communicate information properly in the Switched Ethernet network. The airframe manufacturer needs to test the integrated network to verify that all flight hardware is communicating properly. Design verification testing and maintenance testing are required to perform data communication level verification of Switched Ethernet architectures for avionics applications to ensure that all communication is deterministic and reliable. A practical implementation performing the required tests is discussed.
INTRODUCTION

Switched Ethernet is ready to become the communications network most often integrated into avionics applications. It is expected to eventually replace serial I/O and ARINC429 in commercial and even military avionics applications. A commercial standard called ARINC664 has been developed to define Switched Ethernet for commercial aircraft applications.

The two largest commercial airframe manufacturers, Boeing and Airbus, are expected to incorporate ARINC664 into their next generation aircraft. Since the specification of ARINC664 and slight variations of its implementation imposed by the airframe manufacturer are quite similar, this paper will simply refer to these collectively as Avionics Switch Ethernet.

Avionics Switched Ethernet topology and protocol differs from standard Ethernet 802.3 definitions. The two key enhancements in Avionics Switched Ethernet made to standard Ethernet that are essential for an avionics communication network are:

- Redundancy
- Determinism

Because of the redundancy and deterministic features of Avionics Switch Ethernet, a different testing strategy for End Systems on the network and for communications over the network are used. The purpose of Avionics Switched Ethernet testing is to ensure that data is transferred in a timely fashion, and that the integrity of the data on the network is maintained.

AVIONICS SWITCHED ETHERNET OVERVIEW

Avionics Switched Ethernet is a closed network topology. The elements of the topology are End Systems, Switches, and connections. Figure 1 illustrates the Avionics Switched Network topology.

Figure 1

Each End System has a direct, bi-directional connection to a switch. The End System will also have a second bi-directional connection to another switch that is used for the redundant communication path. The switching technology ensures that the connection and bandwidth required to move data from one End System to another is available. The switch fabric is responsible for moving all data over the network in a deterministic manner.

The Virtual Link is the basis of the Avionics Switched Ethernet protocol. The Virtual Link defines the unidirectional connection from one source End System to one or more
destination End System. Each End System will exchange data frames via a defined Virtual Link. All switching for a frame from an End System transmitter to a receiver End System is based on a Virtual Link identifier.

**END SYSTEM**

The End System is the device whose applications access the Avionics Switch Ethernet to send or receive data via the network. The End Systems protocols can be defined against the Open Systems Interconnection (OSI) Network model. The OSI model defines 7 layers associated with network communications. Each layer of the model only needs to accept data from the previous layer and pass data to the next. Each layer performs a function to deliver data from the applications down to the physical network. The Avionics Switched Ethernet End System protocol mapping is shown in Figure 2.

**PHYSICAL LAYER**

The Physical layer is the hardware connection to the network. Avionics Switched Ethernet uses traditional Ethernet cabling. Support is for both 100Mbit/sec and 10Mbit/sec. For aircraft End Systems, connectors need to be compatible with aircraft conditions (i.e., EMI, vibration, heat).

**MAC LAYER**

The Media Access Control (MAC) layer identifies the source End System, and the destination End System. Each End System has a unique 48-bit address as an identifier. The source address is a Unicast address and represents an End System that is unique on the network. Embedded in the MAC destination address is the Virtual Link identifier. This identifier is a 16-bit value that occupies the lower 16-bits of the 48-bit address. Other than the 16-bit Virtual Link identifier, the MAC destination conforms to the Ethernet Multicast address.

Figure 3 shows the Virtual Link identifier embedded in the Ethernet packet frame.
IP LAYER

The Internet Protocol (IP) passes or receives all data of the End System. The IP is responsible for the fragmentation and re-assembly of blocks of data. This is required when the amount of data needed to send is greater than the maximum IP data payload of a single frame. Avionics Switched Ethernet uses the IPv4 (the current 32-bit implementation).

UDP LAYER

The User Datagram Protocol (UDP) parses data from one or multiple applications to the lower network protocols. UDP is used in the Avionics Switched Ethernet because it does not require verification returned from the recipient indicating the receipt of data. UDP simply pushes application data over the network, or accepts the data from the network and forwards to the application.

Ethernet used in most applications use the Transmit Control Protocol (TCP) instead of UDP. TCP enables receipt verification from the receiver to the sender. However, the timing of the receipt is non-deterministic. UDP is preferable in the Avionics Switched network because the network switching fabric insures that the multicast data will reach its final destination reliably. Figure 4 illustrates multiple UDP ports transmitting data over the network.

DATA SCHEDULING

Each End System controls the flow of Virtual Links in accordance with a Bandwidth Allocation Gap (BAG). The BAG values are time slices allocated by an End System to transmit data for a Virtual Link. The BAG times are defined in milliseconds (typically 1ms, 2 ms, 4ms, 8ms, up to 128ms). Therefore, a maximum of 1,000 frames per second (per VL) may be transmitted or received.

Each transmitting End System manages its own Virtual Links. Each VL can have a different BAG value associated with it. The transmitting End System must implement a “scheduler” to manage the flow of output of these VLs. The scheduler function may impose some jitter associated with the output of the VLs in a timely manner. The VL BAG plus the jitter introduced by the scheduler, and the network latency equate to a window in time where VL traffic can occur. The management of these VL windows by the End System is called traffic shaping.

End Systems receiving data must also manage incoming data. Avionics Switched Ethernet use redundant
connections to minimize data loss. The transmitting End System will send the same frame over 2 separate switching paths to the same receiving End System. A skew time (a short delay measured in microseconds) is inserted between the transmission of the frame over the redundant path. The receiving End System will acquire both frames. It will keep the first valid frame, and discard the other.

In conjunction with redundancy management, the receiving End System will check each data frame for errors. This data integrity checking is done per Virtual Link and per network connection independently. Integrity checks are based on frame sequence number, and data checks within the frame.

Figure 5 illustrates the destination End System performing frame integrity checking and redundancy management.

The switch is responsible for managing (or filtering) data traffic. The switch implements a special function to ensure that each transmitting port sends its defined Virtual Link frames within its allotted window. Remember, a window is a time period consisting of the BAG plus any jitter. If there is too much jitter associated with a frame transmission, the frames sent outside the window tolerances are discarded. The discarded frame statistics are also stored in the management information database.

SWITCHING

The switches used in Avionics Switched Ethernet perform connections based on the Virtual Link identifier located in the MAC protocol layer of the data frame. Each switch is configured with a configuration table. This table defines the Virtual Link assignments to physical network ports. As a frame is received, its Virtual Link identifier is checked against the configuration table to route the frame to its destination port(s). The switch will also perform checks for proper frame size, frame integrity, and proper Virtual Link addressing. Invalid frames are discarded. A management information database is kept with statistics of the invalid frames.
TESTING AVIONICS SWITCHED ETHERNET

Testing is a critical element for the process of integrating any avionics system. It is important to completely understand the behavior of each individual component and the whole system during normal operations, as well as behaviors and reactions to system faults. Testing is required to understand the movement of data over the Avionics Switched Ethernet as well as understanding the data that is being passed.

Testing occurs in the following two phases.

- Testing individual End Systems
- Testing End Systems in the Switched Ethernet Network

INDIVIDUAL END SYSTEM TESTING

Avionics End Systems are delivered to the airframe manufacturer from many suppliers. The End Systems will specialize in a particular function for the aircraft (i.e., heads-up-display, navigation, collision avoidance radar). These individual End Systems need to be tested individually prior to being placed on the aircraft’s Switch Ethernet network to insure that they operate correctly. Testing associated with individual End Systems should answer the following questions.

- Do the End System’s ports transmit correct Virtual Links at appropriate BAG intervals?
- How many transmit errors are produced over a long time period?
- Does the End System receive and process Virtual Link frames?
- How does the End System react to receiving incorrect Virtual Links, frames with protocol errors, or frames with bad data in them?
- Is the End System’s redundancy management and integrity checking working?

NETWORK SYSTEM TESTS

Individual End Systems are eventually integrated into the Switched Ethernet. Effective testing is required during integration to ensure that the new End System operates efficiently. Network frame flow testing reveals flaws in the system design and implementation. Testing associated with checking the Switched Ethernet network frame flow includes the following.

- Monitoring each End System for frame errors associated with frame movement over the network.
- Checking the deterministic flow of Virtual Links from each End System.
- Checking the redundancy of the network.
- Checking the network reaction and tolerance of errors.
TEST SYSTEM

A test system is required to effectively perform the testing. There are commercially available Ethernet Protocol Analyzers and Switched Ethernet Test interfaces that can perform various degrees of testing. Most commercial Ethernet Analyzers are effective for testing protocol errors only. They are not capable of monitoring Virtual Links within the MAC protocol field, or at looking at the data payload of the frame in real time.

The Avionics Switched Ethernet test system requires the use of an interface specifically designed for Avionics Switched Ethernet applications. These interfaces will perform all of the necessary protocol analysis, and they have the capability of examining the Virtual Link information and frame data payload in real-time. There are currently a few commercial manufacturers of these products available.

The test system will have to interface to an End System or to the Switched Ethernet Network fabric directly. The Test System performs the following three different types of tests.

1. Traffic Generation
2. Traffic Monitoring
3. Receive Operation

TRAFFIC GENERATION

Traffic generation is the ability to produce multiple Virtual Link frames from a single port, or redundant ports. The Virtual Links will be sent to an End System to simulate the complete network, or to a switch and simulate one End System. It is important to test by generating multiple Virtual Link frames, with the ability to generate the payload data.

Since most End Systems will be using applications communicating through UDP protocol ports, these ports must also be simulated. The setup of the Virtual Link for simulation will include the following parameters required for true simulation.

- Virtual Link identifier
- Bandwidth Allocation Gap
- Type of application (UDP, IP, MAC)
- Network connection (single or redundant)
- Skew time
- Frame size
- Frame data

The traffic generator needs to implement a robust scheduler capable of sequencing multiple Virtual Link frames. The inter-message gaps between Virtual Links and frames need to be programmable. This enables testing the End System and determining its tolerances at various rates. The ability to coordinate multiple ports in time will allow the simulation of various ports with Virtual Links coordinated in time.
Error injection associated with traffic generation is important to see how the End System will behave under various error conditions. The types of error injection include the following.

- Frame level errors (Cyclic Redundancy Check (CRC), wrong byte alignment, size)
- Incorrect Virtual Link identifiers
- Incorrect sequencing of frames

One of the most important tests of the traffic generator for the network is the measurement of network latencies. This test involves placing an accurate time-stamp in the payload portion of a frame. The receiving End System, which does not know where the frame came from, or the path used to get there, can look at this time stamp and determine the amount of time it took to traverse the network. The traffic generator can introduce the time stamp at the UDP layer to measure the time through the software. Ideally, the time stamp should be placed right before the physical frame transfer occurs. Then a true measure of the network efficiency is available. This type of test is important to monitor in new systems, and behavioral changes made to older systems. It is also an important measure of the times associated with the redundant paths of the network.

Traffic monitoring is the ability to look at and capture all frames of data traversing the network. The ability to monitor traffic in chronological order, including interframe gap times is important for measuring the network’s efficiency. A complete analysis of the network can be accomplished by looking at the traffic over time. This information will yield how the traffic over the network is shaped (i.e., data being transmitted at a higher rate than necessary, or an End System being prohibited from transmitting data). It is equally important for measuring an End Systems’ adherence to Virtual Link Bag specifications.

For monitoring tests, the monitor needs to have programmable capture modes. This provides the ability to begin capturing data based on an event. The event can be an error condition, a specific Virtual Link, or even a portion of data embedded within the payload. Programmable capture enables trapping infrequent errors so that network behavior that prompts these errors can be analyzed and repaired.

The monitor operational tests need to have the capability of storing data for long captures over time. A test system that can buffer data and store onto a disk file for later review is vital. Archived disk files can be analyzed in detail, post operation. The archives of multiple files allow comparisons of network behavior that can occur over time, or when new End Systems or capabilities are added.

Traffic monitoring is the ability to look at and capture all frames of data traversing the network. The ability to monitor traffic in chronological order, including interframe gap times is important for measuring the network’s efficiency. A complete analysis of the network can be accomplished by looking at the traffic over time. This information will yield how the traffic over the network is shaped (i.e., data being transmitted at a higher rate than necessary, or an End System being prohibited from transmitting data). It is equally important for measuring an End Systems’ adherence to Virtual Link Bag specifications.

RECEIVE OPERATIONS

The receive operational testing consists of receiving frames from a Switched Ethernet port just like an End System. These tests can be conducted by simulating the receiver End System, or by “shadowing” the actual receiving End System. Shadowing simply means
connecting to the same physical port connection as the receiver End System, and acquiring the incoming frames simultaneously with the receiver End System.

For receiver testing, the only data frames that are received are based on Virtual Link identifiers. This is different from the monitoring tests described previously where every frame is captured. The intent of receive operations testing is to test and gather Virtual Link frame information for a particular port. Each incoming frame is checked for errors (CRC, frame size, byte alignment), and statistics are kept of these errors conditions.

The receive operation tests look at the higher layers of the protocol stack, and will simulate the reception of frames and data destined for a UDP application. The ability of the application to look at the data contained within the payload to verify its integrity is an important test function. Due to the critical nature of the data passed in avionics applications, it is very important to test the actual received data as well as verify that it was delivered.

The final purpose of the receive operations is the evaluation of the time stamp that can be embedded within the data payload. Receiving the time stamp (as provided by the traffic generator) and computing the elapsed time from the time sent provides valuable insight to network health and efficiency.
CONCLUSION

Switched Ethernet has become a common network architecture in avionics applications. The Commercial Standard ARINC664 and the aircraft vendor specific implementation called AFDX define the topology and implementation of the Switched Ethernet network. This standard developed for avionics communications specifically address reliability and determinism. These are key requirements for avionics communications. Designing and implementing test procedures to verify and monitor the behavior of End-Systems and the Switched Ethernet network requires doing more than just examining the protocol.

Testing and analysis are required for the data payload of transferred frames. Tests must be developed that require traffic generation, chronological monitoring, and simulating End Systems receiving Ethernet frames. These tests go beyond just checking the integrity of the data, but also must look at timing the data flow and efficiency of the network. In addition, the tests must also look at the robustness of the End System and its application tasks ability to interact with the Switched Ethernet network. Testing the Switched Ethernet for avionics goes beyond the simple protocol testing. The efficiency and health of the data traversing the network is more important than the simple measurement of protocol faults that occur over time.

REFERENCES


[9] IEEE 802.1p, Local and Metropolitan Area Networks: Media Access Control Level Bridges: Traffic Class Expediting and Dynamics Multicast Filtering.