1-17-2023

Aircraft Communication Systems - Topologies, Protocols, and Vulnerabilities

Tyler Przybylski

Niroop Sugunaraj

Prakash Ranganathan
University of North Dakota, prakash.ranganathan@und.edu

A Whitepaper On Aircraft Communication Systems - Topologies, Protocols, and Vulnerabilities By Center for Cyber Security Research (C2SR)

Tyler Przybylski, Niroop Sugunaraj*, and Prakash Ranganathan

Abstract

Aviation systems are facing fierce competition driven by private investments promoting the development of new avionics suites (AS). With these new AS comes the need for a faster and larger bandwidth requirement for next-generation communication systems. The legacy military (MIL) standard 1553 communication system (e.g., 1Mbps) can no longer keep up with the surge in bandwidth demand requirements. The new communication systems need to be designed with a system architecture background that can enable simplistic integration with Information Technology (IT) controlled ground-networks, military, and commercial payloads. To facilitate a seamless integration with communication architecture, the current system is highly dependent on the Ethernet based IEEE 802.3 standard. Using a standard protocol cuts down on cost and shortens time for accessibility. However, it introduces several other new problems that developers are actively working through. These problems include a loss of redundancy, lower reliability, and cyber-security vulnerabilities. The cyber-security vulnerabilities that are introduced by IEEE 802.3 Ethernet are one of the larger concerns to military defense programs, and other aviation companies. Impacts of these new communication protocols are quantified and presented as cost, redundancy, topology, and vulnerability. This review paper introduces four communication protocols that can replace heritage systems. These protocols are

*Corresponding Author
Email address: niroop.sugunaraj@und.edu (Niroop Sugunaraj)

presented and compared against each other in redundancy, reliability, topology and security vulnerabilities in their application on aircraft, space launch vehicles and satellites.

Keywords: IEEE 802.3 Ethernet, Ethernet, EtherCAT, TTEthernet, AFDX, Launch Vehicle, Aircraft, Topology, Redundancy, Avionics.

---

1. Introduction

Aerospace systems are rapidly transitioning to advanced communication systems based on the IEEE 802.3 Ethernet standards [1]. In this paper, we broadly define aerospace systems that include aircraft systems, spacecraft systems, and launch vehicle systems. This transition is occurring as the legacy avionics that these aerospace systems are dependent on reaching their limits in terms of performance, component throughput and design complexity [2]. Due to this realization, design companies that build these aerospace systems have either worked out methods to adopt the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard as an aerospace communication standard or built their own proprietary system based on IEEE 802.3. The four leading aerospace communication technologies are: 1) IEEE 802.3 Ethernet, 2) Avionics Full Duplex Switched Ethernet (AFDX), 3) EtherCAT, and 4) Time Triggered Ethernet (TTE). The engineering applications of these four new technologies are discussed in this paper along with the ways to implement them on aircrafts, satellites and launch vehicles. The implementation details include topologies, redundancy, reliability, vehicular applications, and ground support applications. Each technology has its own software protocol that allow for the best understanding of the technology and how security threats can and are introduced. An introduction to the types of tools and software suites that can be used to implement, design, and troubleshoot is presented.

This paper is organized as follows: section II provides a background on aerospace companies that are affected by competition, section III introduces the technology that these companies need to implement next generation avionics into their launch vehicles, section IV presents the ground to airborne network that avionics need to be designed for, section V introduces the four new IEEE 802.3 Ethernet based protocols, section VI provides an overview of open source tools that can be used for development of these protocols, and section VII gives an review of the cyber security threats that must be

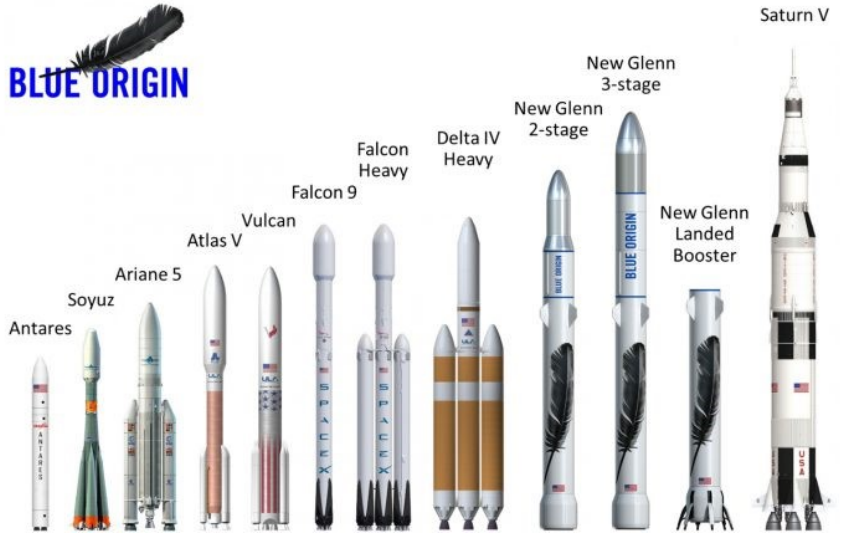

Figure 1: United Sates and Russian rocket size and comparison (blueorigin.com).

thought through during development with these next generation protocols.

1.1. Background

This paper mainly focuses on the way these new communication applications can be implemented for the space launch industries that has direct ties to the aircraft and satellite industries. The strictest applications of these technology are driven by the launch vehicle industry. These launch vehicle industries comprise of government run or funded agencies such as the National Aeronautical and Space Administration (NASA) and the European Space Agency (ESA), as well as private companies like the heritage United Launch Alliance (ULA) and Arianespace to the newer companies such as Space Exploration (SpaceX) and Blue Origin. Each one of these space industry companies focuses on three areas: a launch vehicle (rocket), the payload (satellite), and ground support (launch pad and ground electronics). These three parts must operate perfectly during the duration of a rocket launch, and for aircraft systems, in order for it to be successful and communication system is the critical backbone for these three focus areas to work flawlessly together. The payload and launch vehicle are personalized depending on the application for which they are deployed (e.g., extraterrestrial imagery or remote sensing) requiring tailor-made specifications for each launch mission. Ground system operations are responsible for ensuring that paylods comply

with hazard requirements, pre-mate interface testing, launch vehicle-payload mating (integration), vehicle system tests such as flight simulation and vehicle verification, and if required, a payload propellant loading pad [3]. The U.S. launched its first small launch vehicle (SLV) in 1958 [4]. However, the most notable endeavor was taken in 1990 when an SLV called Pegasus was air-launched by the US to place payloads in low-earth orbit (LEO). Subsequent Pegasus launches in the following decades carried payloads in the 400 – 1000 lbs range. Mission-specific details about the Pegasus can be found in this user guide [5] produced by Orbital ATK.

These space system companies, as well as aircraft companies, are in an era of fierce competition [6] leading to the development of new launch vehicles, aircraft, and satellite constellations. The development of these new systems drives a need for next generation avionics and with that the need for a new communication system that has higher bandwidth and performance. This communication system should also benefit from being standardized as historically, space system companies have developed their own protocol for launch vehicle deployment based on specific use-cases; this results in a myriad of non-standardized technologies. The potential cost savings through a standardized approach will be significant [7]. A typical satellite system consists of 7 subsystems, namely: 1) command and data handling; 2) communications; 3) electrical power; 4) propulsion; 5) thermal control; 6) altitude control; and 7) structure and mechanics. A communications subsystem is designed to transmit/receive electromagnetic (EM) signals, modulate or demodulate the transmitted/received signals, handle inter-subsystems communications such as telemetry (collection and transmission of mission data, spacecraft health, and spacecraft status) or tracking (identifying satellites' current and following locations), satellite timekeeping, onboard computer health monitoring, power monitoring, etc. New communications systems also come with new cyber security vulnerabilities that can affect the performance of the aerospace system and/or its payload [1]. From a security standpoint, the above-mentioned aerospace systems are each governed and controlled by agencies that develop security guidelines and standards meant to protect both the developer and customer. Aircraft systems, such as commercial and military airplanes, are regulated by the Federal Aviation Administration (FAA) [8]. Military airplanes can often be governed by military standards such as military spec (MIL-SPEC) documents and National Security System (NSS) requirements. All spacecraft systems and launch vehicle systems are strictly regulated by the federal government whether commercial or govern-

ment. If the mission, being a spacecraft or launch vehicle, is specifically a national security mission, it must strictly follow all of the guidelines laid out by the Committee on National Security Systems (CNSS) and Instruction (CNSSI) [9]. Additionally, agencies like the Consultative Committee for Space Data Systems (CCSDS) and Aerospace Industries Association (AIA) [10] have published documents that list recommendations to secure space system architectures [11], well known cryptographic algorithms to allow for inter-operability among missions that use the same algorithm(s) [12], and critical security controls [13]. Spacecrafts may use the same communication frequencies and it thus becomes necessary to support secure communications. Inter-operability by using standard cryptographic algorithms will 1) secure data produced by instruments and packages that are from multiple vendors; 2) reduce costs for space missions that utilize the same cryptographic algorithm; and 3) reduce the chances of any corrupt data that could be a consequence of intentional (e.g., malicious attackers) or unintentional (e.g., transmission errors) circumstances.

Each of these governing bodies develops guidelines that follow the three tenets of information technology: confidentiality, integrity and availability. Confidentiality is defined as "ensuring information is accessible only to those authorized to have access" [1]. This is one of the most important tenets for government missions involving spacecraft and launch vehicles. "Integrity is defined as data has a complete or whole structure and availability is defined as proportion of time a system is in a functioning condition" [1]. Applying these tenets is a work in progress as each regulation authority is still actively working on how to appropriately develop a one size fits all guideline for the four new communication protocols. Along with introducing these new communication systems and their implementations, this paper also discusses vulnerabilities and security threats that these government agencies and private companies need to be concerned with when developing and implementing these new communication systems.

1.2. Contributions

The contributions of this paper are listed below:

- A review of the 4 most prevalent communication protocols in the launch vehicle industry, namely etherCAT, ethernet, AFDX, and TTE. Background information on these protocols and recommendations based on unique protocol characteristics are given.

- Cyber threats and vulnerabilities for each of the previously mentioned protocols are examined to the best of our knowledge. Countermeasures for possible threats are identified and elaborated wherever possible.

- Protocol evaluation for each of the 4 technologies based on speed, topology, open-source support, redundancy, reliability, etc. will help in selecting the appropriate protocol based on the application.

2. Results

2.1. Aerospace Companies & Research and Development

There are a limited number of companies that contain complete resources to perform research and development (R&D) on all aerospace systems presented in this paper. Lockheed Martin, Boeing, and Airbus all have formed conglomerates that develop aircraft, satellites, missiles, rockets, and human space capsules.

This paper describes the requirements and applications of a communication system for launch vehicle companies such as United Launch Alliance (ULA), SpaceX, and Blue Origin. The product line and goals of each of these companies vary slightly but each has the same goal: make the United States and the world's access to outer space simpler so all of mankind can reach space [14]. This may be done by developing cheaper products and continued reliability. ULA is one of the most heritage launch providers in the United States as it is a combination of Lockheed Martin and The Boeing Company [15]. The rocket line up of United Launch Alliance consists of the Atlas V, Delta II, Delta IV, and Delta IV heavy [14]. The heritage of these rockets can be traced back to America's first space flights way back in the 1950s. ULA is also working on developing a new launch system called Vulcan Centaur which was recently chosen by the US Space Force to be used for US national security space missions from 2021 through 2024 [16]. The Vulcan Centaur is an upgrade to ULA's Delta IV and Atlas V launch systems. Payload fairing (the nose cone housing that protects the spacecraft from atmospheric pressure and heat during launch and ascent) for the Centaur comes in two configurations: 15 metres or 21 metres. Centaur's upper stage is powered by two engines while its boosters are powered by two other engines, each of which produce 550,000 lbs of thrust and are fueled by liquid hydrogen/liquid oxygen. The Centaur can have 0 - 6 solid rocket boosters (SRBs) that provide additional thrust to the spacecraft to escape earth's gravitational force.

These solid rocket boosters separate from the external spacecraft tank and descend to earth where they are retrieved, refurbished, and reused for future launches. SpaceX currently flies the Falcon 9, a rocket whose first flight was in 2006, and recently had their first flight for the Falcon Heavy in 2018. Blue Origin has two projects, both are aimed at space tourism and space exploration. The first is New Shepard, a small one stage rocket designed to take paying tourists to the Karman Line, the boundary of outerspace at 62 miles high. The second project is New Glenn, a two or three stage rocket, that is still in the development stage and set to have its first launch in the fourth quarter of 2022, but whose physical size hasn't been seen since the early days of the Saturn V project. The size and shapes of all of the rockets are shown in Fig. 1 (courtesy of Blue Origin).

All these companies have ambitious, visionary ideas for the future of space exploration and have begun announcing their R&D programs and what you can expect from them in the next 5 to 30 years. In order to complete them, they need to develop cheaper, more robust avionics which includes abandoning the long utilized 1553 communication protocol for a faster, higher bandwidth protocol. One such approach that has gained much traction since the early 2000s is integrated modular avionics (IMA). This architecture presents a smaller form factor and a partitioned environment that encapsulates different critical subsystems to work on a shared resource platform and is applicable to military (missiles) [17] and civilian (flights) use-cases [18]. Boeing's 777 airliner is one of the most widely known aircrafts that makes use of the Aircraft Information Management System (AIMS) (developed jointly by Boeing and Honeywell) which is based on IMA. Using IMA, the AIMS module cabinet provides means through which resources such as power, output ports, processing requirements, etc. are shared by the software backend which unifies the airplane's functions in a single monolith [19]. Now, Boeing's 787, Airbus' A350/A380, and COMAC's C919 have fully incorporated IMA systems. Space systems are now looking to architectures that are based on the IMA concept [20][21].

ULA has recently announced their vision of the future of space, called Cislunar1000. This vision expects that in 30 years, 1000 people will be living and working in outerspace. ULA plans on making this vision possible through the introduction of Advanced Cryogenic Evolved Upperstage (ACES) which is based on a technology called the Integrated Vehicle Fluid (IVF) [22]. This new upperstage allows for long duration time on orbit missions, something that is not possible today [23]. More recently in November and December

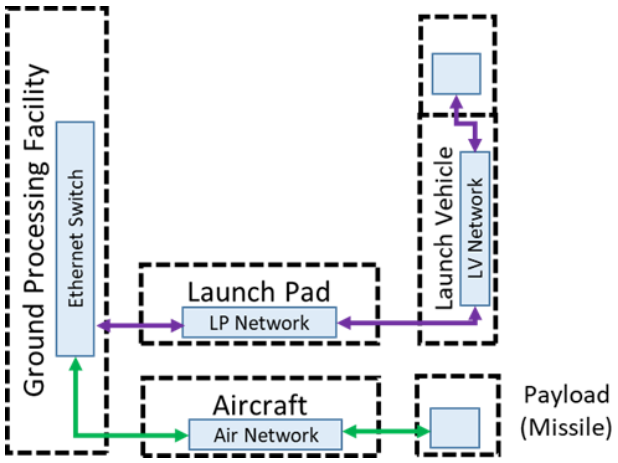

Figure 2: Aerospace communication systems.

of 2020, ULA had its 141st and 142nd launches respectively. Two rockets (Delta IV and Atlas V) carrying payloads of "critical national security" were launched as part of missions for the National Reconnaissance Office (NRO) [24].

SpaceX has already begun ushering in an era of new space technologies by advancing the technologies of its Falcon 9 boosters and Dragon capsule. This company is attempting to accomplish this by landing the booster on either land or on a barge after it has separated from the second stage. SpaceX's newest vision involves reducing the cost of going to Mars from 10 billion per person to the median cost of a house in the United States. Their proposal on how to do this is a fully reusable, distributed launch system that consists of refilling on orbit [25]. As of 2021, SpaceX launched its heavyweight Falcon 9 rocket into LEO carrying satellite for SpaceX's Starlink constellation [26].

Blue Origin has been more secretive with what their future plans are for their New Glenn launch system. It is known that the company is all about space tourism based off of the intent of their New Shepard vehicle [27]. Due to the size of New Glenn, it can be assumed that it has the capability to launch almost an entire space station at once or transporting payloads to the moon. New Glenn is being designed to be reused much like the SpaceX vehicles [28].

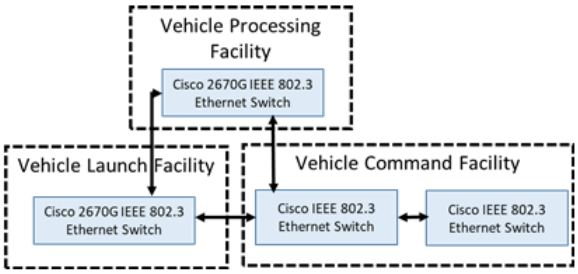

Figure 3: Launch vehicle and aircraft ground support network.

2.2. Aerospace Communication Architecture

The architecture for the launch vehicles of the Blue Origin, ULA, and SpaceX is relatively similar and related to the three key components introduced earlier: launch vehicle, payload (satellite), and ground support as shown in Fig. 2. Ground support for aerospace applications is used to command and collect telemetry from launch vehicle, aircraft, or satellite before liftoff, at which time the link is disconnected making command go in a closed loop control with the flight computer and telemetry over boarded by a wireless system. When command goes internal as closed loop, the vehicles communication protocol becomes critical as it is the physical link that is carrying data from the flight computer (the "brains" of the rocket), to all of the end items that perform functions critical to the success of the vehicle mission, be it a satellite, launch vehicle, or aircraft. Finally for the satellite or payload (missile), it most often has its own communication network, that is often linked to the launch vehicle or aircraft to provide statusing and updates prior to its deployment. Once deployed, its network becomes its own closed loop system helping it complete its mission [29].

Ground systems are often comprised of IEEE 802.3 Ethernet as it is a cheap and simple standard that allows them to build a massive switched network that is often needed for support of launch vehicles, satellites and aircraft as seen in Fig. 3. These extensive networks are needed as there are often multiple processing facilities that the vehicles move through during a launch campaign or vehicle processing. This switched network allows for rapidly moving the data between the centers, as well as, to the data storage facilities and operators on console. This IEEE 802.3 network is often copper cabling at the vehicle interface and is then switched to a fiber interface to allow for miles long runs back to command and storage facilities.

A launch vehicle network is often used for closed loop control and for mov-

ing telemetry. This closed loop control network interfaces with the ground system prior to launch and then transitions internally prior to liftoff. After liftoff, the reliability of the network becomes critical for communicating commands from the flight computer to the end items used to control the rocket. This launch vehicle network in the past has been 1553 or a version of RS422. This meant that it was not compatible with the ground network and needed to be converted to a different protocol [30]. If one of the four communication protocols presented in this paper is used, it can be linked to the ground network without additional processing, which should be avoided as it is another possible point for faults and problems. The goal of a launch vehicle network should be to keep it simple, minimizing the protocols used in order to avoid interoperability issues that can arise from avionics components created by different vendors and thus utilizing differently coded network stacks. When implementing any of the protocols presented in this paper, it is best to keep it to the simple switched network presented within.

Aircraft network operates similar to the launch vehicle network; however, it is not necessarily a closed loop system to the same level that a launch vehicle is. With the aircraft, external commands can be sent by the means of wireless protocols and executed by means of human interaction through the pilot. The aircraft network is still the network that is tasked with transferring messages and telemetry by the means of the physical link. The AFDX protocol that is presented in this paper is a protocol that was developed initially for the use in aircraft, by an aircraft manufacturer.

Finally, the satellite/payload network is a unique network that needs to be designed with high reliability as this is the "mission" critical network. In the case of a satellite, they are often designed to operate for decades in outer space, meaning that the closed loop network has to be designed to last for the duration of the mission. The network must also be designed to integrate with the launch vehicle network during the launch portion of the mission to get critical telemetry and commands to the satellite. When on the ground, the satellite needs a network to interface with the ground to load mission parameters before launch. Like launch vehicles, this has often been time synchronized RS422 [31], but lately has been moving more towards one of the protocols presented in this paper.

For all three "airborne" networks: launch vehicle, aircraft and satellite, a key requirement in their topology is redundancy. After these networks disconnect from the ground, they become independent and with reliability a crucial factor in the success of the mission. To achieve this reliability

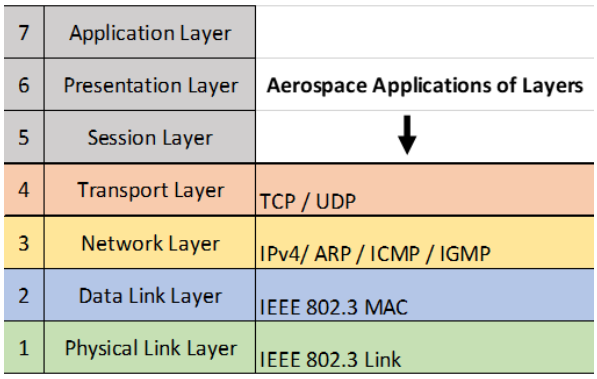

Figure 4: IEEE 802.3 Ethernet OSI layer model.

redundancy must be built into both the hardware topology of the system and into the protocol stack of the communication network. The widely used, heritage 1553 communication protocol had redundancy built into its topology design with an A and B bus for each bus controller [32]. All four of the protocols presented in this paper are based off IEEE 802.3 Ethernet which was built as a commercially distributed system, not as a replacement for 1553. As presented in the following section, each protocol has its ability to meet the airborne and ground network requirements, but to do so, developers need to be aware of the protocol design and how to compensate for some of their short falls at a system level.

2.3. Communication Protocols

2.3.1. IEEE 802.3 Ethernet Standard

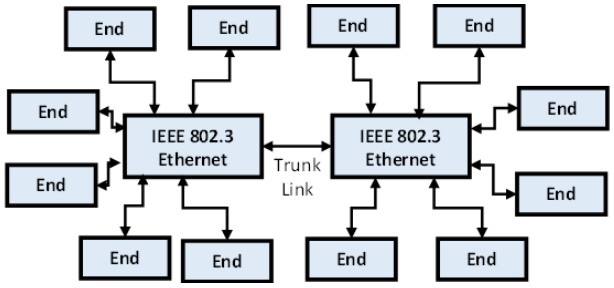

Figure 5: IEEE 802.3 Ethernet switched star topology.

Ethernet is the backbone of the Internet that everybody uses without even thinking due to its simplicity and ease of configuration. First developed

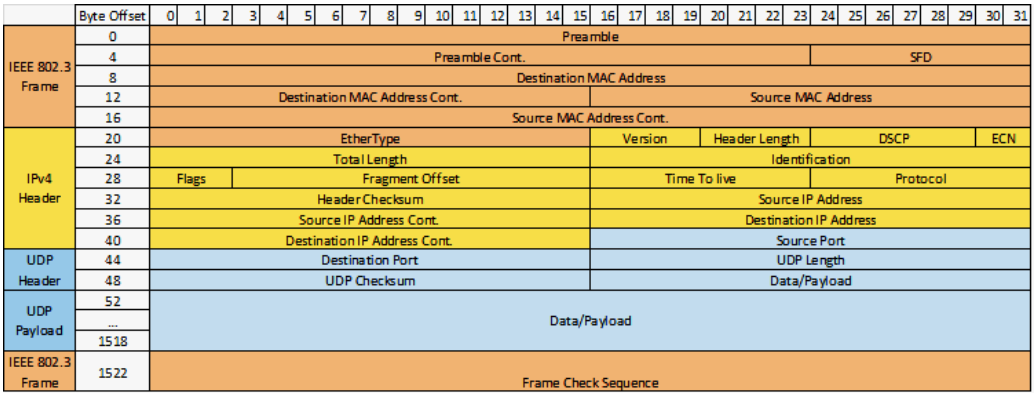

Figure 6: An IEEE 802.3 based Ethernet frame with UDP protocol.

as a 3 Mbps network allowing up to 256 users, Ethernet was hoped to be a flexible, decentralized and low cost technology [33]. This technology quickly grew into a 10 Mbps network, than a 100 Mbps network, a 1 Gbps network and to what can be used today as a 10 and 40 Gbps network [34].

This rapid growth is facilitated due to its wide adoption as an IEEE standard 802.3. Because of its rapid adoption, a working group was formed to be in charge of the standard and keep pace with the changes. The Internet Engineering Task Force (IETF) was established to oversee the implementation and standardization of the Internet Protocol (IP) [35]. This task force has developed thousands of Request For Comments (RFC) to govern the use of the IP protocol [33]. These RFCs are the guidelines to developing system protocol stacks to ensure interoperability between developers. RFCs standardize IPv4 protocols such as ICMP which is commonly used for Ping messages, IGMP multicast network requirements, and User Datagram Protocol (UDP) requirements [35].

The Ethernet protocol can theoretically be defined by the first two layers of the Open Systems Interconnection (OSI) network stack (Physical Link and Data Link layers) [36], as shown in Fig. 4. For the simplicity and purposes of this paper, only layers one (Physical Link) and two (Data Link) are discussed. Ethernet's physical layer is defined by the cabling it uses and the type of devices that can be deployed on the network. Ethernet typically uses a full-duplex set of twisted pair cables (CAT 5, CAT 6, CAT 6a, or CAT 7) which can have speeds of 1 or 10 Gbps. Such cabling is most commonly done in a star configuration as this configuration allows for direct communication devices and switches while reducing packet collisions.

Ethernet's data layer primarily handles the Media Access Control (MAC) sublayer where devices equipped with networking capabilities, typically by an internal network interface card (NIC), are identified by hardware addresses to identify the source and destination addresses of packet transmissions. This star configuration utilizes Ethernet switches to form a mesh network [33].

Aerospace applications of the 802.3 standard are often based off of the 100BaseTx design, also known as Fast Ethernet. Gigabit links can be used for interfaces from the airborne Ethernet switch to the ground switch, but for all airborne-to-airborne links, 100BaseTx is best used as it is a simpler MLT-3 signal than the Gigabit PAM-5 signal [34]. Using 100BaseTx in a switched network star topology, shown in Fig. 5, allows for the implementation of physical redundancy in the airborne system. This is possible as to meet criticality requirements, most avionics boxes are designed to be physically redundant, having either an 'A' and 'B' side, or channel 1 and channel 2 side [37]. By adding in Ethernet switches the two sides can be physically separated into two separate but functionally equivalent networks. This can create single string, single fault tolerant, or dual redundant system based off of the way the physically separated networks are connected to the end items.

The protocol implementation of 100BaseTx Ethernet uses layer 2 MAC addressing schemes, layer 3 IP version 4 (IPv4) EtherType (0x0800), and layer 4 UDP or Transmission Control Protocol (TCP). Each layer of this packet or frame contains its own Cyclic Redundancy Check (CRC) totaling three for each packet. This triple check allows for verification of messages to ensure that no bits were flipped during transmission of the messages. This error checking is critical in ensuring any side of the physical network is working and healthy at all times. A typical Ethernet IPv4 UDP packet looks as shown in Fig. 6.

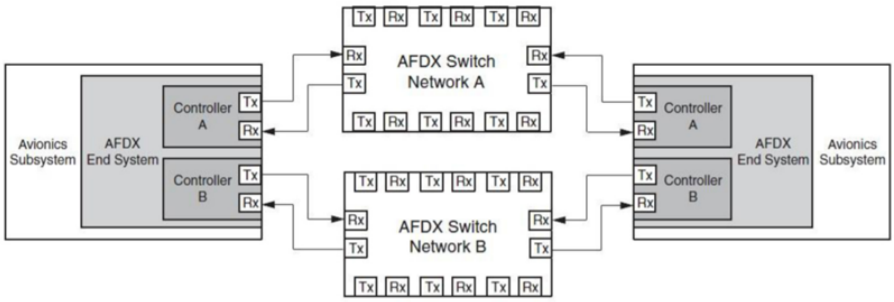

Figure 7: AFDX redundant star topology.

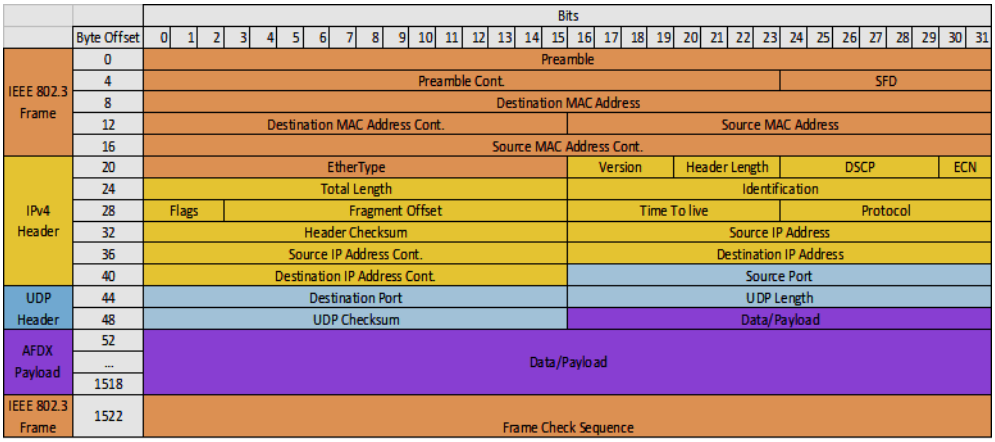

Figure 8: AFDX frame.

Implementation of the standard in a star topology means the introduction of an Ethernet switch. The Ethernet switch connects nodes to each other through multiple ports, introducing another layer of software called "switching fabric" [33]. This switching fabric is a store-and-forward mechanism, requiring that the complete packet be scanned in before the switch acts on the information. The switch learns who is on each port by resolving MAC addresses to IP addresses using the Address Resolution Protocol, EtherType (0x0806). This is a unique feature that does not exist in the following three protocols discussed in this paper. The switch also introduces the ability to create a Virtual network or VLAN. These are used to separate physical networks into multiple logical networks, such as separating control commands from telemetry commands [33].

Even though Ethernet was developed as a commercially distributed protocol not designed for the redundancy and criticality requirements needed for use in aerospace systems, it can be adapted pretty easily to meet the requirements. The network designer needs to be fully aware of the protocols mentioned above and develop controlling software to make it all work as one fluent system. A couple companies have realized some of the down falls of standard Ethernet and developed additional protocols built into the standard layers of IEEE 802.3 Ethernet. The next three presented protocols are all based off of standard Ethernet with either patented or standardized add-ons.

2.3.2. Avionics Full Duplex Switched Ethernet

Avionics Full Duplex Switched Ethernet (AFDX) was developed to be a safety critical network using a reliable redundancy management mechanism to provide aircraft a reliable network [2]. AFDX is an Ethernet-based technology that was created by Airbus and has since been used by Boeing and other commercial aerospace companies [36]. Built on the Ethernet technology, AFDX offers higher available bandwidth and provides a deterministic performance that is done through a "virtual link" (VL) concept [2]. AFDX was developed to help solve some of the real-time deterministic characteristics that the IEEE 802.3 standard is missing. The topology design of AFDX is based off of a two independent and redundant network schemes, shown in Fig. 7. This network scheme consists of three main elements, similar to IEEE 802.3 Ethernet: the end systems (ES), switches, and physical links. The end items are connected to the switches via a redundant, full duplex physical links natively creating a dual redundant system. The physical interface uses the IEEE 802.3 PHY chips capable of speeds of 100Mbps or 1Gpbs. The network is applied in a star topology, shown in Fig. 7, which allows for the network to be scalable, much like 802.3 Ethernet [2].

To form a star topology, the AFDX network utilizes switches like 802.3 Ethernet, however these AFDX switches have added features beyond 802.3 Ethernet [2]. These switches implement the unique features of AFDX that allow for meeting the crucial timing requirements needed for airborne systems. These switches are store and forward and allow for parallel processing.

The AFDX communication frame is fully compliant with the IEEE 802.3 standard [38]. AFDX specifies the use of the IP, and uses UDP, allowing for more determinism in a control network. Determinism refers to the capability of an AFDX switch to determine the time taken by any data packet to reach its destination and perform packet scheduling thus preventing packet collisions. Within the AFDX frame, both the IP and UDP layer implement a Cyclic Redundancy Check (CRC) allowing for extra security and safety [29]. AFDX also implements the standard IEEE 802.3 MAC addressing scheme. An example of a AFDX frame, taken is shown in Fig. 8 [38].

A software, protocol advantage that AFDX has natively designed into is systems is a redundant transmission mechanism. This feature is where AFDX starts separating itself from IEEE 802.3 Ethernet. Every AFDX frame that is transmitted on the network has a duplicate copy sent on each network. This means that the message would go out network A and Network B as shown in

Fig. 8. The end item processes the messages from both networks and does a compare of the messages to ensure that they are the same. If they are not, the end items know which network is not functioning properly and can shut it down. This topology is similar to what was proposed in the IEEE 802.3 Ethernet section, however the difference is that it is built into each physical redundant side of the avionics boxes [39]. Therefore, the designer can opt to not physically duplicate the boxes depending on the criticality of the design, which in some cases can save development time and money.

AFDX has solved some of the timing and redundancy shortcomings that are present in IEEE 802.3 Ethernet by implementing a proprietary layer on top of the standard Ethernet. If a designer would choose to use this system in their airborne architecture, they would not be able to natively talk with the ground system as standard Ethernet switches do not work with the AFDX [38]. This limitation can be fixed through a processing unit that converts from AFDX to Ethernet, however this can add a layer of cost to the program. A previously listed limitation to this deterministic system was inaccuracy in packet transmission timing due to delay otherwise known as jitter [40]. However, the ARINC-664 Part 7 specification for AFDX communication link maximum jitter is specified by two formulae that are classified as requirements for the network and this enhances its reliability [41].

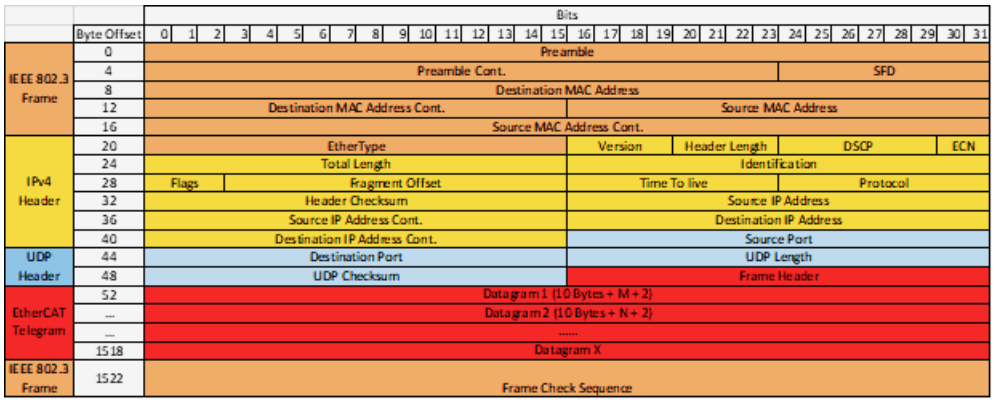

Figure 9: EtherCAT frame.

2.3.3. EtherCAT

EtherCAT is a technology that was developed based on the IEEE 802.3 standard to be a real-time, Ethernet like, protocol and introduced to the pub-

lic in 2003 [42]. EtherCAT works as Master and Slave network in a way that is similar to the legacy 1553 MIL standard communication protocol, where transmission of a frame can only be initiated by the EtherCAT master, thus making it the controller [43]. The Master and Slave EtherCAT ports use a standard IEEE 802.3 RJ45 PHY and MAC layer, capable of speeds up to 200Mbps. The protocol implementation for the master and slave is an EtherCAT specific FPGA or ASIC [44][33]. Both the master and slave systems use a 100uS clock which limits the jitter. The EtherCAT protocol allows slaves to read and write frames on-the-fly, meaning that there is no store-and-forward delay, unlike 802.3 Ethernet and AFDX [25]. Due to this on-the-fly method and combined with the use of full duplex, the latency is only what is caused because of the hardware. EtherCAT payloads are embedded in a standard Ethernet frame using the EtherType identifier of (0x88A4) [42]. As shown in Fig. 9, this single Ethernet frame is capable of transporting several EtherCAT payloads, known as datagrams, and as a result, the protocol overhead that IEEE 802.3 Ethernet has is largely omitted. In this Ethernet frame, the standard source and destination fields are populated with the addresses of the sending and receiving devices [25].

The topology design for EtherCAT networks is flexible and can be line, tree or star [42]. Each topology allows for up to 65,535 devices in one segment with a master. However, the most used topology is the line, or daisy chain topology. Since each EtherCAT slave contains two ports, the Master connects the port one of the first slave. Then port two of the first slave is connected to port one of the second slave and so forth [43] as shown in Fig. 10. This removes the requirement for a switched network which would cause excess latency. However, implementation as a line topology means that the redundancy is limited to single fault tolerance, one of the lowest levels of redundancy.

EtherCAT was originally designed for automation technology such as robotics and has recently been reviewed for use in avionics systems. Its similarities to 1553 with no switched network mean that there is a risk for increased cabling needs, and if there are many slaves in the network, that latency can add up as it is not point to point making messages move through each slave to get to the end item. The implementation of this protocol also does not support an IEEE 802.3 Ethernet system that would be used on the ground network. Therefore, use of this protocol in an airborne network requires separate processing to interface with the ground system.

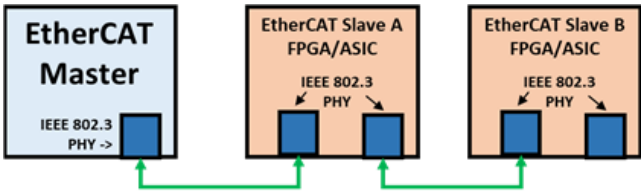

Figure 10: EtherCAT line architecture.

2.3.4. Time Triggered Ethernet

Time-Triggered Ethernet (TTE) is the final communication protocol that is based on the IEEE 802.3 Ethernet standard. TTE was developed by a European company TTTech with academia involvement for use in avionics applications and industrial automation [43]. The technology was developed to have a reliant communication protocol that had microsecond accuracy.

TTE introduces three Quality of Service (QoS) message types to aid in the real-time requirements: time-triggered, rate-constrained which is AFDX, and best-effort. Time-triggered is the highest priority of the three message types and is sent only at predefined times for critical applications. Rate-constrained guarantees bandwidth, but is not synchronized thus increasing jitter. Rate constrained is a form similar and often the same as AFDX. Finally best-effort is the lowest level QoS and is used for non-critical applications due to having no latency guarantees [45] .

Time-Triggered Ethernet added a time synchronization service which is called Time-Triggered (TT) frames. This method works between the use of senders, receivers, and switches. The switch is the key component to the technology, implementing the TT protocol [32]. It knows the time-triggered windows and can hold frames based off of when they were sent by the sender and when they must be received by the receiver. This is synchronous messaging due to the known window timing. There are other non-IEEE 802.3 Ethernet protocols like the Controller Area Network (CAN) bus and synchronous RS-422, however TTE is the only Ethernet based protocol that introduces this synchronous ability and works on preset periods and phases within which sender and receiver nodes operate [46].

Similar to AFDX, TTE implements the standard IEEE 802.3 MAC and full duplex PHYs for Layer 1 and Layer 2 needs that are capable of 10Mbps, 100Mbps, or 1Gpbs. This implementation is specific to the sender and receiver. However at the switch, the proprietary hardware and software is used in order to implement the timing protocols [32].

Of the four IEEE 802.3 Ethernet protocols presented, TTE is the only one that implements synchronous communication for some developers, this is a peace of mind protocol similar to the long lived, legacy 1553 which makes them comfortable in using it. TTE switches also have built-in mechanisms to contain errors that may critically affect the system(s) they belong to. This is an additional factor that improves the protocol's reliability [47]. However, since it is a tightly-controlled proprietary protocol, like AFDX, it can become costly trying to implement this protocol. This protocol may be the best choice for use on satellites. This is due to the development cycle of satellites often being a one-time design, meaning that cost is usually not an issue unlike recurring designs such as launch vehicles and aircraft.

3. Discussion

3.1. Communication Protocol Evaluation Tools

There are many open sourced and licensed tools that are available to capture and construct packets for all the listed protocols in this paper (please see Fig. 11). One of the most widely used and supported open-sourced packet capture tools is Wireshark. This tool works on both Linux and Windows machines and utilizes Tcpdump to create packet capture (PCAP) files. Tcpdump is a network debugging tool that can passively or actively intercept packets on a network. One downside of Wireshark is that its real-time capture capabilities vary based on the performance statistics of the machine it is running on and therefore accuracy down to the millisecond is not always there.

An open source tool designed for Linux called Arkime (formerly called Moloch) can also work with Wireshark as it works with PCAP files to capture and analyze network traffic. Arkime also has an application programming interface (API) for visualization of such data with custom dashboards and protocols like the IEEE 802.3. One of the major benefits of Arkime is that is based on the "ELK" stack (Elasticsearch, Logstash, and Kibana) which allows users to analyze, index, and search multi-modal data regardless of their type while offering speed and flexibility.

Tcpreplay is a tool that allows for the replay of a string of packets captured by Wireshark and stored as a PCAP file. This kind of tool can be useful when data is being captured and an error is discovered. If the transmitted packets are captured, TcpReplay can replay the same string of packets to

determine if the error happens again or if it was a single occurrence. This tool is an open-source tool.

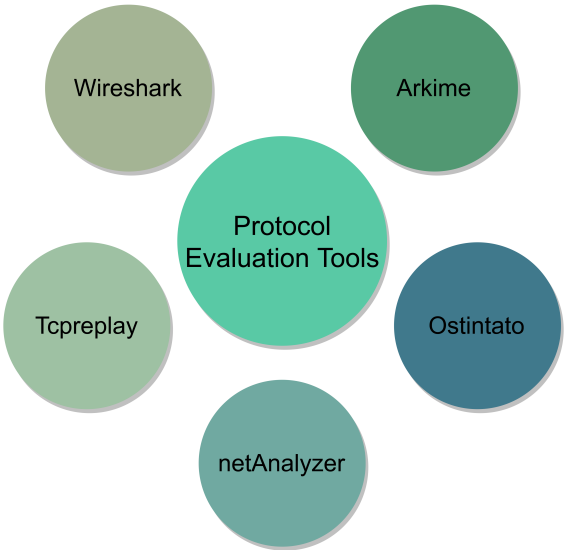

Figure 11: Tools to evaluate aircraft communication protocols.

An open-source packet generation tool that can be used to simulate some of the vulnerabilities mentioned below is called Ostinato. Ostinato allows for a user to construct a packet by filling in text boxes with the required IPv4 and transmit layer information. It then builds the packet and sends out on the wire based on user inputs of packets per second and number of bursts of the packet. This ability also allows for executing DoS attacks discussed below because Ostinato allows for randomizing MAC and IP addresses per packet generated.

If time-sensitive packet capture is required, then netANALYZER real time Ethernet analyzer by Hilscher is the best choice [48]. This device is a passive packet capture device that works for IEEE 802.3 Ethernet and EtherCAT. The device's accuracy is +/- 5ns. This device can plot packet capture real-time in a histogram and can log packet capture files as PCAP files for later dissection in Wireshark and other PCAP tools.

3.2. Protocol Security Threats and Vulnerabilities

As implementation of 21st century communication protocols rapidly expands in the aerospace industry, federal regulation boards and developing

companies IT and Security departments need to adapt and create new governing guidelines for these new protocols. Most recently in the aircraft industry, it has been up to the company IT departments to create guidelines as the FAA has struggled and been slow at adapting and creating new guidelines to mitigate cyber security risk [1]. Current FAA regulations, standards, and guidance do not address cyber security vulnerabilities [8]. For the spacecraft and launch vehicle industries, their designers and company IT are struggling with following often archaic guidelines based off of early 1970s communications protocols and operating systems. This lack of update of requirements does not only apply to communication protocols but to the end item computation systems and the switching devices used to enable the communication protocols.

As the industry shifts from expensive custom built operating systems for the computation systems and switching devices, to a commercial off the shelf (COTS) approach, the number of lines of code (LOC) raises from 50 thousand to 100's of millions lines of code [43]. This creates a logistics and man power nightmare in trying to verify and validate every single line of code within the communication system. As stated in the introduction, keeping in mind the three tenants of security and understanding for each protocol when selecting a communication standard to use is a necessary requirement. One must also be aware of the entire picture when assessing security risks for each protocol, such as not limiting the evaluation to the specific design [37]. For example, a design engineer might be developing a communication network for a space vehicle or launch vehicle. The engineer must remember that when the vehicle is sitting on the ground, the communication bus is most likely be linked to a ground network, introducing vulnerabilities that are not present once the vehicle is off of the ground. This problem is particularly credible for airborne systems that use standard IEEE 802.3 Ethernet.

With these factors in mind, security vulnerabilities are presented for each communication protocol with mitigation factors suggested.

3.2.1. IEEE 802.3 Ethernet Vulnerabilities

Ethernet is the protocol that the following three discussed protocols are based off of. Because of this, the majority of vulnerabilities related to the frame structure are common between the protocols. However, Ethernet, being an open-sourced switched network introduces vulnerabilities unique to it that the other three protocols fixed through their proprietary nature. Due to the desire for Ethernet to be cheap and easily deployable, security and Ether-

net vulnerabilities have never been a major consideration when designing the standard [33]. The vulnerabilities are tied directly to its easily expandable network, meaning the ARP and MAC table learning are one major introduction of vulnerabilities. This sub-protocol is what allows for the basis of all intrusive Ethernet attacks by allowing an attacker to obtain access to the network [49]. This access can be achieved through either a direct connection to the network or through the use of a malware application. There are multiple ways the attacker can utilize this network access: network access for learning about the topology for a later attack, eavesdropping, manipulation, and disruption [33].

1. **Network Access**: Network access is required to execute all types of attacks discussed in this paper. Access is facilitated by implementation issues and most often not caused directly by the Ethernet standard architecture. An attacker gaining access directly breaks the confidentiality tenet and can lead to the other two tenets being broken after the attacker gains access.
   Unauthorized Joins: Because of the nature of the Ethernet standard protocol being easily expandable, unauthorized joins are one of the easiest ways to join the network [50]. This can be done through obtaining a physical link to the Ethernet switch through connections through a wall socket and disconnecting an end user and using its physical link [17]. This vulnerability can be introduced when an end link is disconnected from an approved computer and the switch does not shut down the link. Solutions to this method are to introduce software at the switch level that limits the way the network can expand [50]. These can be things such as controlling unauthorized connections, doing port shutdowns when appropriate, and implementing hard coded MAC address tables. However, in large networks, hardcoded tables can become nearly impossible to keep up to date. This is a solution for small isolated networks such as launch vehicle or aircraft networks. For the IT ground network, they need to implement additional protections against unauthorized joins.
   VLAN Join: Because Ethernet switches often transmit VLAN advertisements, an attacker can create a computer that looks like an Ethernet switch using virtual software and therefore listens to the VLAN management messages. This establishes this computer as a switch and it can therefore intercept messages. A solution to this is to appropriately

disable this feature and manually add Ethernet switches to the network [33].

Remote Access: Most Ethernet switches have the ability to be remotely accessed through Serial Network Management Protocol (SNMP), telnet, or secure shell (SSH). Using these methods, the attacker can open a remote administration system and gain access to the network [17].

2. **Traffic Confidentiality - Eavesdropping**:
   Once an attacker has gained access to the network, they can begin eavesdropping on the Ethernet packets. Due to the design of the Ethernet frame, lots of information can be gained by just scanning the packets: IP & MAC addresses of end items on networks, VLAN information, and more topology information [17]. One way hackers can eavesdrop is by flooding random MAC addressed Ethernet packets to the switch, thus filling up its buffer. Once that happens, Ethernet switches are designed to broadcast unresolved packets out every port, thus allowing the attacker to eavesdrop [33]. An attacker could also enable the port mirroring feature of the Ethernet switch and passively eavesdrop on all packets that transmit through the switch. Eavesdropping in the network breaks the confidentiality tenant which is one of the main tenants for military applications. It is important to stop and prevent eavesdropping in a launch vehicle, aircraft, and satellite network in order to prevent critical data from getting into the wrong hands.
3. **Traffic Integrity - Manipulation**: Another method for an attacker to modify traffic on the network. If the attacker is able to imitate the user, they can often gain temporary control of an end item in the network. This breaks the integrity tenant that was presented in the security section. One way to do this is called a man in the middle attack. This is done by the attacker directing traffic through its link. If the traffic is not protected by any secure measure, it can be modified and then passed on. As stated in the last sentence, one way to protect from this happening is to encrypt the data and have extra security checks within the packet to know if the data has been manipulated in any way [17]. Preventing manipulation in an aerospace network is critical to keeping control of assets on the network. This can be crucial for launch vehicles and satellites that are sitting on a pad ready for liftoff. For the launch to be successful, everything must be carefully coordinated and if there is manipulation of data in the network. This can cause major problems in the launch sequence.

4. **Denial of Service - Disruption**:
   Unlike the previous vulnerabilities, Denial of Service (DoS) attacks are not meant to gain access and instead are meant to prevent access [17]. These attacks can lead to partial or total loss of service for as long as the attack is sustained prevent launch vehicles from launching, spacecraft from operating, or aircraft from taking flight.

3.2.2. AFDX Vulnerabilities

AFDX is a technology that is based off of IEEE 802.3 Ethernet and therefore has many of the same vulnerabilities as IEEE 802.3. Even though AFDX is a proprietary technology, it lacks one of the advantages that EtherCAT has due to its frame utilizing an EtherType of 0x0800 which is IEEE 802.3 IPv4 protocol. This makes it so that the attacker can access the network, discussed in section II.A.1, in the same manner as the standard. This is important to recognize because any time the item, whether spacecraft, launch vehicle or aircraft, is plugged into an IT ground network, it becomes susceptible to access attacks. The one thing that is not similar to IEEE 802.3 are the switches used in AFDX. Since AFDX was designed to meet critical timing requirements, the AFDX switches look for special delimiters in the AFDX payload, shown in Fig. 4 [45]. This means that the attacker needs to recognize these delimiters and make sure that they are matched in any attempt at spoofing, DoS, or manipulation. The AFDX switches do not use virtual networks and thus are not susceptible to the VLAN join attack discussed in the section above. AFDX is designed for critical timing and to facilitate this has a unique configuration of redundancy built into its topology and its protocol. One way the protocol does this is to send duplicate packets for every message transmitted. If there are no transmission errors the duplicate packet is discarded. This means that the attacker must apply the same manipulation or spoofing to each packet in order not to raise red flags in the system [45].

3.2.3. EtherCAT Vulnerabilites

EtherCAT, in general, is vulnerable to all attacks that exist on IEEE 802.3 Ethernet, however, some attacks may not cause the same damage, but rather interrupt the real time ability that makes EtherCAT unique [24]. The type of Ethernet attack that has the ability to cause the most damage in an EtherCAT network is a man in the middle attack. However, in the application of all four protocols discussed in this paper, it can be argued that a man in

the middle attack poses the same level of threat for all protocols. This is due to the highly sensitive nature of these protocols all being used as a control system and thus if a man in the middle attack occurred, the attacker could theoretically obtain control of the device it hacked [25]. An attack not discussed in the Ethernet section, but that does apply to all Ethernet based protocols, is a Replay-Attack. This is an integrity attack where the attacker records a frame and then later resends it [17]. In EtherCAT, this duplicate packet can cause slaves to execute older commands setting them or the system into an undesired state. This attack is especially damaging in the EtherCAT network because unlike IEEE 802.3 Ethernet, EtherCAT has no way to add extra authentication into its frames [51]. Another type of attack that affects all Ethernet based protocols is MAC address spoofing [52]. Since there is a lack of authorization and authentication observed in EtherCAT communications [53], a MAC address spoofing attack takes the attacker frame and assumes the identity of the EtherCAT master by using its MAC address. By doing so, the attacker has gained full control of the EtherCAT network and can now control all slaves. This was proved by a testbed simulation carried out for etherCAT vulnerabilities in ICS systems where a system admin cannot explicitly tell that MAC-based spoofing has taken place due to the lack of authentication. This can lead to devastating consequences for aerospace applications [54]. This can lead to devastating consequences in the aerospace industry: it can mean loss of mission for a spacecraft or launch vehicle, an untimely launch of a launch vehicle, loss of aircraft control leading to injury or death of the pilot.

Table 1: Next generation aerospace communication protocol evaluation.

Feature\Protocol	**IEEE 802.3 Ethernet**	**AFDX**	**EtherCAT**	**TTEthernet**
Speed (Mbps)	10/100/1000+	100/1000	100/200	100/100/1000
Duplex	Full	Full	Full	Full
PHY	Standard 802.3	Standard 802.3	Standard 802.3	Standard 802.3
MAC	802.3 MAC	802.3 MAC	802.3 MAC	802.3 MAC
Topology	Star	Star	Line	Star
Redundancy	Single String / Single Fault / Dual Redundant (Up to Developer)	Natively Dual Redundant	Single Fault Tolerant	Single Fault/ Dual Tolerant
Proprietary (Cost)	Open Source	Proprietary	Open Source/ Proprietary	Proprietary
Reliability (Timing)	Manageable with Implementation	Manageable with Implementation	Built-in Timing Improvements	QoS Provides Best Timing Options
Ground Support	Yes	Additional Processing Required	Additional Processing Required	Additional Processing Required
Security Vulnerabilities	IEEE 802.3 Vulnerabilities	IEEE 802.3 Vulnerabilities	IEEE 802.3 Vulnerabilities	IEEE 802.3 Vulnerabilities
Open Source Tool Support	Yes	Yes	Yes	Yes

3.2.4. Time-Triggered Ethernet Vulnerabilities

Time triggered Ethernet (TTE) is one of the hardest proprietary protocols for an attacker to gain access on. This is due to the complexity of its protocol

along with the high proprietary nature of the switches that route the traffic [32]. TTE has all the same risks for spoofing, manipulation, and DoS attacks, however because of the structure of the protocol with the three different QOS message types, it becomes extremely difficult for an attacker to accurately spoof all message types accurately. The first QoS type of Time-Triggered poses the biggest challenge for an attacker due to the scheduled timing of the packets [26].

3.3. Future Trends

The aviation industry has made significant milestones from the first commercial flight in 1914. These milestones (e.g., supersonic/hypersonic aircraft, deployment of CubeSats, and artificial intelligence-based aircraft design strategies) have paved way for the next-generation of aerospace technology to actively investigate areas such as eco-friendly and sustainable fuel sources (i.e., decarbonization), autonomous flight systems, and the potential for smart factories to model a data-driven approach for optimization and visibility into the manufacturing process. Fly-by-wire technology has brought benefits such as lower weights (replacement of heavy mechanical systems with wiring), reduced maintenance costs, improved safety, and precise handling but also opens the possibility for the software-defined networking (SDN) paradigm in addition to a more secure supply chain through artificial intelligence.

3.3.1. Software-defined Networking (SDN)

Software-defined Networking (SDN) allows for centralized network management, control, and monitoring. Additionally, SDN can also accommodate modifications and new changes through network modularity. It is important to note that SDN may not necessarily reduce the hardware complexity in a closed-loop communication system, but rather offloads a majority of the functions to a centralized server [55]. According to Elmasry and colleagues [56], the aviation sector may see approvals from the FAA to move all cockpit communications to commercial infrastructure (i.e., 5G infrastructure or broadband satellites) as long as high-end encryption mechanisms are in place. An additional layer of security can be provided by SDN by separating cockpit and cabin traffic using general purpose processors (GPPs) that relay data from air to ground over secure tunnels. Onboard devices communicate with a ground gateway that establishes security and service policies to meet the aircraft's requirements.

3.3.2. Artificial Intelligence

There are limited standards that exist to regulate cybersecurity in the aviation industry. According to Mirchandani and Adhikari [57], there are several threat vectors that exist for aerospace systems (i.e., space systems and subsystems, space operations, ground services, support infrastructure, etc.), one of which is the supply chain. A standard called the NAS9924 by the Aerospace Industries Association [58] released in 2013 outlines a security baseline for manufacturers supplying components (e.g., COTS) to aerospace and defense companies and is the only publicly known standard for cybersecurity regulation in aviation. In addition to the lack of policies for aerospace cybersecurity, the supply chain is complex and integration of multi-vendor systems from different vendors drastically increases the attack surface. Operational and mission lifespans of space assets can easily last decades and unpatched security vulnerabilities in legacy systems can be exploited [59]. For such threats and vulnerabilities, artificial intelligence-based cognitive computing will enable aerospace and defense customers to supply chain assess data and produce supply risk scoring and supplier performance. Cognitive computing will offer insights and a comprehensive visibility into the supply chain that will allow suppliers to predict and prevent threats. An effective cognitive computing system will require resilient and high fidelity data from supply chain, procurement, manufacturing, and product development processes to produce actionable intelligence that can secure the supply chain [60].

4. Conclusion

The selection of an Ethernet based protocol for use on aerospace systems is dependent on the application-specific implementation. Each of the four protocols presented have their own pros and cons that can be traced back to their implementation. It can be agreed that each of these four protocols meets the main requirements needed for next-generation avionics systems: bandwidth increase, redundancy, reliability, and system integration. TTEthernet stands out to be the most robust of the four protocols when compared on metrics such as redundancy, reliability, and security. Its add-on design to standard IEEE 802.3 Ethernet makes it the best option for highly critical and sensitive applications such as for satellite designs. For aircraft and launch vehicles, the best options are either AFDX or standard IEEE 802.3 Ethernet. It is possible that 802.3 Ethernet could be carefully implemented to have the

same functionality as AFDX without the extra cost of purchasing a proprietary design. Both technologies offer the ability to have full redundancy, methods for reliability, and configuration support with existing Ethernet-based ground systems. Through the implementation of any of these four protocols, the next generation of avionics systems will enable design companies to successfully build and fly their future aircraft, launch vehicle, and satellite programs.

Recommended Citation

Tyler Przybylski, Niroop Sugunaraj, and Prakash Ranganathan. "A Whitepaper On Aircraft Communication Systems - Topologies, Protocols, and Vulnerabilities By Center for Cyber Security Research (C2SR)" (2023). Electrical Engineering Student Publications. 11. https://commons.und.edu/ee-stu/11

References

[1] R. De Cerchio, C. Riley, Aircraft systems cyber security, in: 2011 IEEE/AIAA 30th Digital Avionics Systems Conference, IEEE, 2011, pp. 1C3–1.

[2] M. Li, G. Zhu, Y. Savaria, M. Lauer, Reliability enhancement of redundancy management in afdx networks, IEEE Transactions on Industrial Informatics 13 (2017) 2118–2129.

[3] National Aeronautics and Space Administration (NASA), Space Launch System (SLS) Artemis 2 Secondary Payloads 6U & 12U Potential Cubesat Accommodations, Space Launch System Program (2019). URL: `https://www.nasa.gov/sites/default/files/atoms/files/sls_artemis-2_6u-12u_accommodations_8_1_19.pdf`.

[4] R. D. Launius, D. R. Jenkins, To Reach the High Frontier: A History of US Launch Vehicles, The University Press of Kentucky, 2002.

[5] Orbital ATK, Pegasus® User's Guide (2015) 1–97.

[6] D. L. Sharp, K. Widelitz, FA8811-17-9-0001; Evolved Expendable Launch Vehicle (EELV) Launch Service Agreements (LSA) Request

for Proposals (RFP), 2018. Https://govtribe.com/opportunity/federal-contract-opportunity/fa8811-17-9-0001-evolved-expendable-launch-vehicle-eelv-launch-service-agreements-lsa-request-for-proposals-rfp-fa881116r000x.

[7] H. H. Nguyen, P. S. Nguyen, Communication subsystems for satellite design, in: Satellite Systems-Design, Modeling, Simulation and Analysis, IntechOpen, 2020.

[8] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, B. M. Phares, Cyber Security for Airports, International Journal for Traffic and Transport Engineering 3 (2013) 365–376. doi:10.7708/ijtte.2013.3(4).02.

[9] Commitee on National Security Systems, Security Categorization and Control Selection for National Security Systems This Instruction Prescribes Minimum Standards Your Department or Agency May Require Further Implementation (2014). URL: https://www.cnss.gov.

[10] B. Bailey, R. J. Speelman, P. A. Doshi, N. C. Cohen, W. A. Wheeler, Defending Spacecraft in the Cyber Domain, Technical Report, The Aerospace Corporation, 2019. URL: http://marefateadyan.nashriyat.ir/node/150.

[11] Consultative Committee for Space Data Systems, Report Concerning Space Data System Standards - Overview of Space Communications Protocols (2014) 43. URL: http://public.ccsds.org/publications/archive/130x0g3.pdf.

[12] B. Rashidi, Recommendation for Space Data System Standards, Technical Report August, 2019. doi:10.1049/pbse009e_ch4.

[13] N. Aerospace, S. Nas, National Aerospace Standard 9933 Critical Security Controls for Effective Capability in Cyber Defense (2015) 22209.

[14] B. F. Kutter, F. Zegler, J. Barr, M. Gravlee, J. Szatkowski, J. Patton, S. Ward, Ongoing launch vehicle innovation at United Launch Alliance, IEEE Aerospace Conference Proceedings (2010). doi:10.1109/AERO.2010.5446742.

[15] G. J. Schiller, Innovation at ULA- It really is rocket science, IEEE Aerospace Conference Proceedings (2014) 1–8. doi:10.1109/AERO.2014.6836371.

[16] United Launch Alliance, Vulcan Centaur, 2021. URL: https://www.ulalaunch.com/rockets/vulcan-centaur.

[17] T. Venkata Mani, S. Maitra, P. Bhanusrinivas, K. L. Raja Sekhar, S. Vijaya Lakshmi, R. M. Guptha, Integrated Modular Avionics for Missile Applications, 1st International Conference on Range Technology, ICORT 2019 (2019). doi:10.1109/ICORT46471.2019.9069629.

[18] F. Boniol, New Challenges for Future Avionic Architectures (2013) 1–1. doi:10.1007/978-3-319-00560-7_1.

[19] Honeywell, Airplane Information Management System (AIMS), Avionics, 2022. URL: https://aerospace.honeywell.com/us/en/products-and-services/product/hardware-and-systems/cockpit-systems-and-displays/airplane-information-management-system.

[20] H. Wang, W. Niu, A review on key technologies of the distributed integrated modular avionics system, International Journal of Wireless Information Networks 25 (2018) 358–369.

[21] I. Kabashkin, V. Filippov, Reliability of software applications in integrated modular avionics, Transportation Research Procedia 51 (2020) 75–81.

[22] M. Holguin, Enabling long duration spaceflight via an integrated vehicle fluid system, AIAA Space and Astronautics Forum and Exposition, SPACE 2016 (2016) 1–5. doi:10.2514/6.2016-5495.

[23] Melissa Sampson and Jeremy Tamsett, Launch Can Do More: Upper-Stage Innovation at ULA Will Create New value for Space, United Launch Alliance (2018). URL: https://www.spacefoundation.org/wp-content/uploads/2019/07/Sampson-Melissa_Cislunar-Economy-and-ACES.pdf.

[24] United Launch Alliance, United Launch Alliance Successfully Launches NROL-44 Mission to Support National Security, 2020.

Https://www.ulalaunch.com/about/news-detail/2020/12/10/united-launch-alliance-successfully-launches-nrol-44-mission-to-support-national-security.

[25] SpaceX, Mars & Beyond: THE ROAD TO MAKING HUMANITY MULTIPLANETARY, 2021. URL: https://www.spacex.com/human-spaceflight/mars/.

[26] A. Thompson, SpaceX launches another 60 Starlink satellites into orbit and sticks rocket landing, 2021. Https://www.space.com/spacex-starlink-23-satellite-mission-launch-rocket-landing.

[27] G. Martin, NewSpace: The Emerging Commercial Space Industry, Technical Report, NASA Ames Research Center, 2017.

[28] J. P. Bezos et al., Sea Landing of Space Launch Vehicles and Associated Systems and Methods 2 (2014) 1–10.

[29] J. Alvarez, B. Walls, Constellations, clusters, and communication technology: Expanding small satellite access to space, in: 2016 IEEE aerospace conference, IEEE, 2016, pp. 1–11.

[30] E. Blasch, P. Kostek, P. Pačes, K. Kramer, Summary of avionics technologies, IEEE Aerospace and Electronic Systems Magazine 30 (2015) 6–11.

[31] L. Wang, P. Chen, X. Jiang, Z. Chen, B. Liu, A design of sounding rocket video processing system based on wavelet transform compression algorithm, 2013 IEEE 3rd International Conference on Information Science and Technology, ICIST 2013 (2013) 870–873. doi:10.1109/ICIST.2013.6747679.

[32] C. Xu, L. Zhang, Z. Ling, M. Xu, D. Wang, TTEthernet for launch vehicle communication network, in: Proceedings of the 29th Chinese Control and Decision Conference, CCDC 2017, volume 77, 2017, pp. 5159–5163. doi:10.1109/CCDC.2017.7979411.

[33] T. Kiravuo, M. Sarela, J. Manner, A survey of ethernet LAN security, IEEE Communications Surveys and Tutorials 15 (2013) 1477–1491. doi:10.1109/SURV.2012.121112.00190.

[34] IEEE Standard for Information technology, IEEE 802.3cc-2017 - IEEE Standard for Ethernet - Amendment 11: Physical Layer and Management Parameters for Serial 25 Gb/s Ethernet Operation Over Single-Mode Fiber, 2018. URL: https://standards.ieee.org/standard/802{_}3cc-2017.html.

[35] University of Southern California, INTERNET PROTOCOL -DARPA INTERNET PROGRAM: PROTOCOL SPECIFICATION, 1981. URL: https://tools.ietf.org/html/rfc791.

[36] R. Neuhaus, A Beginner's Guide to Ethernet 802.3 (2005) 1–26. URL: https://www.analog.com/media/en/technical-documentation/application-notes/EE-269.pdf.

[37] A. B. Kisin, E. T. Gorman, G. P. Rakow, SpaceAGE bus: Proposed electro-mechanical bus for avionics intra-box interconnections, IEEE Aerospace Conference Proceedings (2012). doi:10.1109/AERO.2012.6187221.

[38] P. Vdovin, V. A. Kostenko, Organizing message transmission in afdx networks, Programming and Computer Software 43 (2017) 1–12.

[39] T. Schuster, D. Verma, Networking concepts comparison for avionics architecture, AIAA/IEEE Digital Avionics Systems Conference - Proceedings (2008) 1–11. doi:10.1109/DASC.2008.4702761.

[40] L. Abdallah, J. Ermont, J.-L. Scharbarg, C. Fraboul, Reducing afdx jitter in a mixed noc/afdx architecture, in: 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), IEEE, 2018, pp. 1–4.

[41] GE Intelligent Platform, AFDX / ARINC 664 Protocol Tutorial, Network (2010) 24.

[42] EtherCAT Technology Group, EtherCAT - the Ethernet Fieldbus, 2003. URL: https://www.ethercat.org/en/technology.html.

[43] R. Cummings, K. Richter, R. Ernst, J. Diemer, A. Ghoshal, Exploring Use of Ethernet for In-Vehicle Control Applications: AFDX, TTEthernet, EtherCAT, and AVB, 2012. URL: https://www.sae.org/publications/technical-papers/content/2012-01-0196/.

[44] R. L. Alena, J. P. Ossenfort IV, K. I. Laws, A. Goforth, F. Figueroa, Communications for integrated modular avionics, IEEE Aerospace Conference Proceedings (2007). doi:10.1109/AERO.2007.352639.

[45] P. Grams, Time-Triggered Ethernet for Aerospace Applications (2013).

[46] S. Vitturi, C. Zunino, T. Sauter, Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G, Proceedings of the IEEE 107 (2019) 944–961. doi:10.1109/JPROC.2019.2913443.

[47] I. Alvarez Vadillo, A. Ballesteros, M. Barranco, D. Gessner, S. Djerasevic, J. Proenza, Fault Tolerance in Highly Reliable Ethernet-Based Industrial Systems, Proceedings of the IEEE 107 (2019) 977–1010. doi:10.1109/JPROC.2019.2914589.

[48] Hilscher, netANALYZER real time Ethernet analyzer, box, 2021. URL: https://www.hilscher.com/products/product-groups/analysis-and-data-acquisition/ethernet-analysis/nanl-b500g-re/?

[49] D. Robinson, C. Kim, A cyber-defensive industrial control system with redundancy and intrusion detection, 2017 North American Power Symposium, NAPS 2017 (2017). doi:10.1109/NAPS.2017.8107186.

[50] A. O. Bakhtin, V. S. Sherstnev, I. L. Pichugova, V. V. Dudorov, Detection of an unauthorized wired connection to a local area network by solving telegraph equations system, 2016 International Siberian Conference on Control and Communications, SIBCON 2016 - Proceedings (2016). doi:10.1109/SIBCON.2016.7491804.

[51] A. GRANAT, H. HÖFKEN, M. SCHUBA, Intrusion Detection of the ICS Protocol EtherCAT, DEStech Transactions on Computer Science and Engineering N/A (2017) 113–117. doi:10.12783/dtcse/cnsce2017/8885.

[52] H. Zhao, Z. Li, H. Wei, J. Shi, Y. Huang, SeqFuzzer: An industrial protocol fuzzing framework from a deep learning perspective, Proceedings - 2019 IEEE 12th International Conference on Software Testing, Verification and Validation, ICST 2019 (2019) 59–67. doi:10.1109/ICST.2019.00016.

[53] K. O. Akpinar, I. Ozcelik, Methodology to Determine the Device-Level Periodicity for Anomaly Detection in EtherCAT-Based Industrial Control Networks, IEEE Transactions on Network and Service Management 4537 (2020). doi:10.1109/TNSM.2020.3037050.

[54] K. Ovaz Akpinar, I. Ozcelik, Development of the ECAT Preprocessor with the Trust Communication Approach, Security and Communication Networks 2018 (2018). doi:10.1155/2018/2639750.

[55] K. Sampigethaya, Software-defined networking in aviation: Opportunities and challenges, in: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), IEEE, 2015, pp. 1–21.

[56] G. Elmasry, D. McClatchy, R. Heinrich, K. Delaney, A software defined networking framework for future airborne connectivity, in: 2017 Integrated Communications, Navigation and Surveillance Conference (ICNS), IEEE, 2017, pp. 2C2–1.

[57] S. Mirchandani, S. Adhikari, Aerospace cybersecurity threat vector assessment, in: ASCEND 2020, 2020, p. 4116.

[58] A. I. Association, NAS9924, 1st Edition, February 28, 2013 - CYBER SECURITY BASELINE, 2013. URL: https://global.ihs.com/doc_detail.cfm?document_name=NAS9924&item_s_key=00601403#abstract-section.

[59] G. Falco, Cybersecurity principles for space systems, Journal of Aerospace Information Systems 16 (2019) 61–70.

[60] K. Butner, D. Lubowe, Welcome to the cognitive supply chain, IBM Institute for Business value (2017) 1–21. URL: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03836USEN.