Matthew Preston
Georgia Institute of Technology OMSCY CS6727 Practicum Project Proposal

Lowering Avionics Bus Trust: Moving ARINC 429 Bus Architecture Towards Zero Trust.

Section 1: Problem Statement

In avionics, bus architectures such as ARINC 429, MIL-STD-1553 and ARINC629, play critical roles for aircraft computer communication. Designed in the 1960s and 70s, these systems are robust and reliable, but are no longer resilient to modern cybersecurity threats. With respect to the project of ARINC 429, the problem with these bus architectures is that they are inherently the opposite of zero-trust. If an adversary gains access to the bus, they can potentially issue unchecked commands to line replaceable units (LRUs) in cyber-physical systems, leading to catastrophic kinetic effects. This practicum aims to explore and develop solutions to enhance the security of the ARINC 429 bus architecture by engineering and enforcing zero trust security measures, thereby mitigating the risk of unauthorized access and malicious commands.

Section 2: Problem Relevance and Motivation

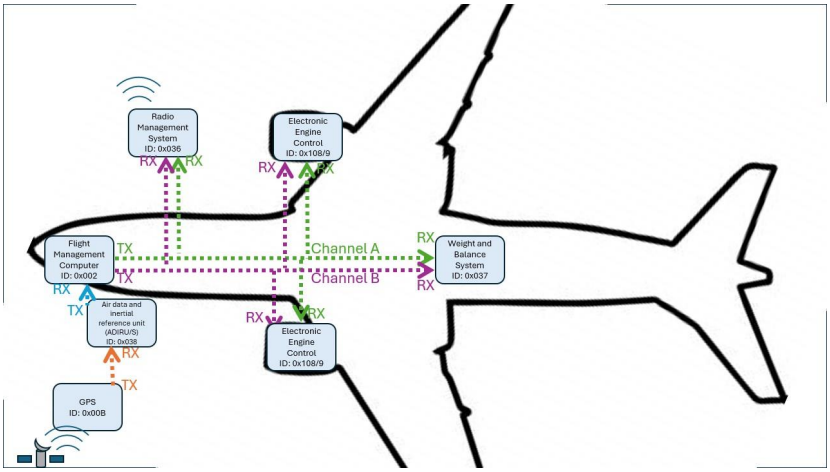
In 2022 The White House commanded government agencies to move towards zero trust cybersecurity principles. This policy was stated in Executive Order 14028 and explained further in White House Memorandum M-22-09. Therefore, it is safe to say that the US Government is interested in securing its technologies by applying a Zero-Trust framework to subcomponents of US Government systems. Due to the potential of a cyber-attack having kinetic effects that could cause loss of life and negatively impact multimillion dollar assets that civilian avionic groups and airplane passengers rely on, the safety and security of aircraft components is further underscored. Furthermore, other governments and organizations around the world have airplanes with the same or similar technologies.

The limited 11-week timeline and somewhat limited resources available will drive the scope of this problem. Because of its use in DoD systems and the defense industry, MIL-STD-1553 is likely of most interest to the US Government, which makes it more sensitive and prevents one from obtaining pertinent data. Therefore, this project will focus on the civilian equivalent: ARINC 429. ARINC 429 is mostly used in civilian aircraft such as the Boeing B737, B747, and B767, the AirBus A320, and A340, and the McDonnel-Douglas MD-11, but it is also used in military systems that derive from similar civilian aircraft. The aviation industry’s reliance on legacy systems underscores the impact of this security problem.

Section 3: System and Threat Modelling

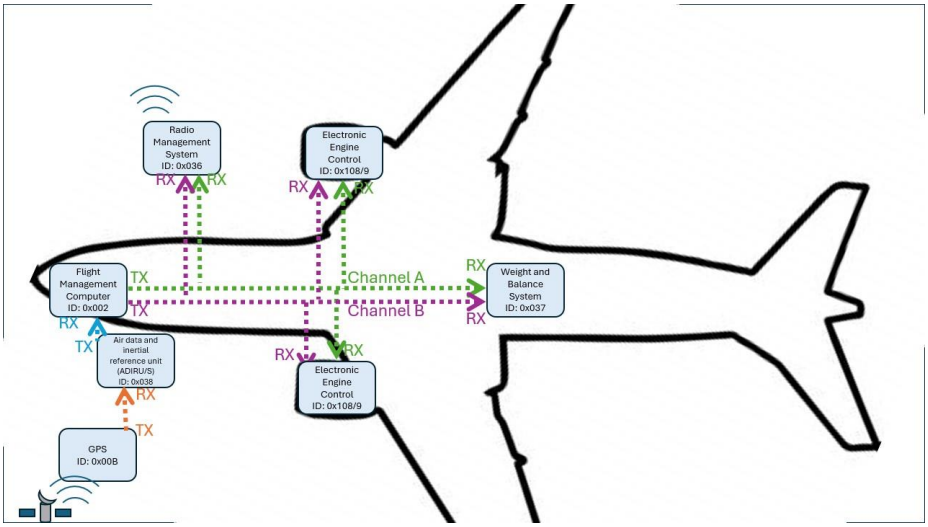
ARINC 429 protocol allows for one transmitter per bus with 20 receivers. In a simplified example, some of the LRUs on the bus are the flight management system, autopilot system, communication systems and navigation systems. ARINC 429 specification slots out 0x341 (833) types of Equipment IDs for LRUs.

This simplified example of an ARINC 429 bus on an airplane could look like the following:



In this system model, the Flight Management Computer is both a receiver and transceiver, as it is a computer with the appropriate ARINC 429 RX and TX chips. Therefore, it is receiving on one bus to get positional, altitude, heading, etc. data to present to the pilots in the cockpit, while broadcasting/transmitting on two other lines. These two lines are redundant for safety reasons. They allow the pilot to control the plane's motion from the cockpit consoles and controls which are physically interfacing with the Flight Management Computer.

The most likely type of attacker against systems with ARINC 429 would be a nation-state actor who is looking to gather intelligence or physically damage critical infrastructure. Below is the threat model with an example attack, using MITRE's ATT&CK Matrix (ICS version, since it maps better to cyber physical systems; https://attack.mitre.org/matrices/ics/).



In this attack, an attacker compromises a traditional IT asset, in this case a maintenance laptop from the airline company. The attack model is short because of the inherent trust of the ARINC 429 bus. They then use the control of the laptop to

propagate and exploit the flight management computer. From there they can set a logic bomb that activates while the plane is running to mess with the engines or other actuators on the bus. Using the bus is easy since the attacker can use ARINC 429 design documents to send valid commands on the buses to the engines as there are no checks for confidentiality or identity.

Nation-state actors are motivated to exploit and affect the critical infrastructure of the competitors. One simple motivation would just be to gather intelligence on ARINC 429 bus data to try to reverse engineer and steal the technology behind the LRUs to artificially prop up their nation's economy. A particularly chilling motivation could also be targeted assassinations with plausible deniability. For example: taking out a political leader in a rival country that wants to pass policies and legislation that hinders your own country's industries or international power. The only evidence left behind would be the flight management computer if it survives, and the laptop. The ARINC 429 bus does not leave any record or log of commands, so there would be less data to autopsy. An attack like this would be much harder to assign any attribution, than something more kinetic like a surface to air missile. One other motivation, which is more moderate, would be as part of a campaign of deepening a rival nation's political instability. For example, implanting a logic bomb that does not cause catastrophic failures but rather grounds a fleet or acts as maintenance nuisances across the airline industry would weaken a nation's public trust in one of their transportation institutions. Combined with coordinated attacks on other parts of infrastructure like the energy grid, water facilities, etc., this would foment a larger effect of distrust from the public.

While there are no known public attacks like this, there are examples of attacks and research on bus architectures and avionics:

- "Exploiting the MIL-STD-1553 avionic data bus with an active cyber device" is a research paper that details ways to guard against spoofing and DoS attacks on 1553 buses with their own hardware-in-the-loop devices loaded with their own custom defense software. (Source: https://www.sciencedirect.com/science/article/pii/S0167404820303709#sec0006)
- "Hardware Fingerprinting for the ARINC 429 Avionic Bus" is a conference paper that implements an intrusion detection system for ARINC 429. Thier threat model guards against rogue devices added onto the bus, letting operators know to remove said devices, while mine deals with compromised bus devices. The difference is that in their threat model, they identify hardware devices and therefore have some sort of quasi-identification/authentication of device scheme, while my solution will investigate a more traffic-based monitoring system. Their defense, according to the paper, is good at detecting rogue devices, but compromised devices themselves which are still going to send malicious commands seem to pass unchecked. (Source: https://link.springer.com/chapter/10.1007/978-3-030-59013-0_3)
- "Investigating CAN Bus Network Integrity in Avionics Systems" is a research blog that briefly talks about CAN bus defenses against crafted packets. All packets were manually analyzed by human operators after the fact, and not on any system. (Source:

https://www.rapid7.com/research/report/investigating-can-bus-network-integrity-in-avionics-systems/)

Section 4: Deliverables and Project Plan

I expect to develop and deliver the following by the conclusion of this practicum:

Part 1: Demonstration of Vulnerability/ARINC 429 Weakness.

1. A simulated environment with visualization and code-based interfacing tools of an ARINC 429 bus. This would be an extension of current free and open-source resources for ARINC, such as pyARINC 429 (https://github.com/aeroneous/PyARINC 429). Current ARINC 429 simulation is non-existent.
2. A simple hack/attack implemented on this simulation that can demonstrate the impact of various scenarios. It will assume compromise of the plane to ARINC 429 components – as one should with a Zero Trust mindset. For example, assuming the ARINC 429 transceiver component has been compromised, the hack would then be getting that component to send out valid commands with catastrophic effects, like turning the engines off or putting the plane into a downward trajectory. Points 1 and 2 combine to a digital twin that includes malicious commands for the simulated ARINC 429.

Part 2: Defending ARINC 429 Against Attacks:

3. A rules-based intrusion detection unit for ARINC 429 data frames. This solution would have expected behaviors coded in, allowing it to show what the bus should look like devoid of an attacker at any moment, and allowing a human to be a manual monitor of the bus. Additionally, it could allow for an add-on machine-learning agent that stops malicious commands. This machine-learning add-on would be sorting each bus command into categories of effects (or plane behaviors) and then flagging and stopping dangerous ones. Each part of the defense will be evaluated on its reliability and minimal impact on system robustness, and computing/resource needs.

From NIST Special Publication 800-207, there are seven basic tenets of zero trust. In my model and defense, I plan to address some of them:

1. “All data sources and computing services are considered resources.” In my model, I am considering LRUs, external connections and the bus itself as resources (logically speaking) to fly a plane.
2. “All communication is secured regardless of network location.” This tenet will be addressed by Part 2 above.
3. “Access to individual enterprise resources is granted on a per-session basis.” This is not addressed by my defense or models. There is no plans to add privileging or least privilege to ARINC429 and its connected components. Additionally, there is no plan to limit access to any LRU to the bus as per necessary, since availability is critical in the model.
4. “Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other

behavioral and environmental attributes." This is addressed similarly as tenet 2, with the rules-based IDS system that I will implement, itself can changed based on needs of the operators.

5. "The enterprise monitors and measures the integrity and security posture of all owned and associated assets." As part of the IDS, monitoring of the bus is required. However, it will not continuously monitor LRUs continuously for vulnerabilities in their software.
6. "All resource authentication and authorization are dynamic and strictly enforced before access is allowed." This will not be addressed by my model or defenses.
7. "The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture." I plan to incorporate logging bus traffic as part of the defense functionality.

References:

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- https://github.com/aeroneous/PyARINC 429
- https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- https://whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- https://www.swri.org/podcast/ep64
- https://www.astronics.com/avionics-databus-tutorials
- https://www.aim-online.com/wp-content/uploads/2019/07/aim-tutorial-oview429-190712-u.pdf
- https://www.instructables.com/Interfacing-Electronic-Circuits-to-Arduinos/
- https://attack.mitre.org/matrices/ics/
- https://web.archive.org/web/20201013031536/http://read.pudn.com/downloads111/ebook/462196/429P1-17_Errata1.pdf