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

Matthew Preston
Georgia Institude of Technology
ithub.com/PrestonMatt/GATech_MS_Cybersecurity_Practicum_InfoSec_Summer24 mpreston9@g
mspreston98@gmail.com

Abstract

In avionics, bus architectures such as ARINC 429, MIL-STD-1553 and ARINC 629, 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.

Keywords – Cybersecurity, Avionics, ARINC 429, Zero Trust, Cyber Physical Systems, Bus Architectures, Internal Defense System (IDS)

1 Introduction

TODO: Include problem statement, justification (/Problem relavance and motivation), resource constraints, initial ideas for design, and the three goals to touch upon: 1. creating ARINC429 Sim, 2. Creating ARINC429 Attack, and 3. Creating ARINC 429 IDS.

2 Model and Threat Model

TODO: Include graphics of the model of the plan that the simulator was based on, explain it, explain some differences and simplifications made with the sim vs. a real world plane, and explain the threat model and various attacks that could happen, and how they could be achieved.

3 Simulation

TODO: Detail all the work done with creating the ARINC 429 simulation from the ground up in python, and try to relate each component and functionality to its real world counterpart.

4 Attack Explanation

TODO: detail the attack here, further if necessary from the Threat model. Specifically show the code that creates the attack.

5 IDS Explanation

TODO: Explain the IDS algorithm, complexity, and functionality. Now would also be a good time to justify why this is the best solution in terms of something like an IPS or redesigning the ARINC bus.

6 IDS Evaluation

TODO: Explain the evaluation plan for the IDS. Then show and document the code and results of the eval plan.

7 Lessons Learned

TODO: Explain lessons learned in this project, and where I could have done better.

8 Future Work

TODO: Explain what future research could be done, and how future researchers could use my ARINC 429 simulation and IDS in the future, or extend their features / real word likeness.

Appendix Include graphs, self refrences, etc. Bibliography is already completed below.

References

R. Vincent. 28 Nov. 2023, *Arinc-429 RX Implementation in LabVIEW FPGA.*, NI Community. https://forums.ni.com/t5/Example-Code/Arinc-429-Rx-Implementation-in-LabVIEW-FPGA/ta-p/3507624

aeroneous. 17 Jul. 2018, *PyARINC429.*, Discover PyARINC429, a simple Python module for encoding and decoding ARINC 429 digital information. https://github.com/aeroneous/PyARINC429

Peña, Lisa and Shipman, Maggie. Feb. 2024, *Episode 64: Zero-Trust Cybersecurity for Vehicles.*, Technology Today Podcast, Southwest Research Institute, https://www.swri.org/podcast/ep64

Sital Technology. Accessed May 2024, *ARINC-429 with Cyber and Wirefault Protection.*, ARINC-429 Solutions. Sital Technology, https://sitaltech.com/arinc-429/

Sital Technology. Accessed May 2024, *Understanding Cyber Attacks on MIL-STD-1553 Buses*, Sital Technology, https://sitaltech.com/understanding-cyber-attacks-on-mil-std-1553-buses/

Alta Data Technologies LLC. 19 Jan. 2021, *1553 Network and Cybersecurity Testing*, Alta Data Technologies LLC, https://www.altadt.com/wp-content/uploads/dlm_uploads/2020/10/1553-Network-and-Cybersecurity-Testing.pdf

Tilman, Bill. 14 Dec. 2021, *Why You Need to Secure Your 1553 MIL-STD Bus and the Five Things You Must Have in Your Solution.*, Abaco Systems, https://abaco.com/blog/why-you-need-secure-your-1553-mil-std-bus-and-five-things-you-must-have-your-solution

Waldmann, B. Jul. 2019, *ARINC 429 Specification Tutorial.*, Avionics Databus Solutions, Version 2.2, AIM Worldwide, https://www.aim-online.com/wp-content/uploads/2019/07/aim-tutorial-oview429-190712-u.pdf, https://www.aim-online.com/products-overview/tutorials/arinc-429-tutorial/

KIMDU. 26 Jun. 2023, *ARINC-429 tutorial: A Step-by-Step Guide.*, KIMDU Technologies, https://kimdu.com/arinc-429-tutorial-a-step-by-step-guide/

United Electronic Industries/AMETEK. 26 Jun. 2023, *ARINC-429 Tutorial & Reference.*, Understanding ARINC-429, United Electronic Industries/AMETEK, https://www.ueidaq.com/arinc-429-tutorial-reference-guide

Biden, Joesph R. Jr. 12 May 2021, *Executive Order on Improving the Nation's Cybersecurity.*, Briefing Room, Presidential Actions, The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cyber

Rose, Scott; Borchert, Oliver; Mitchell, Stu; and Connelly, Sean. Aug. 2020, *Zero Trust Architecture.*, NIST Special Publication 800-207, National Institue of Standards and Technology, U.S. Department of Commerce, https://doi.org/10.6028/NIST.SP.800-207

Young, Shalanda D. 26 Jan. 2022, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.*, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, Version M-22-09, Executive Office of the President; Office of Management and Budget, https://whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Ballard Technology. 26 Jan. 2022, *Avionics Databus Tutorials.*, Astronics AES, https://www.astronics.com/avionics-databus-tutorials

maewert. Accessed May 2024, *Interfacing Electronic Circuits to Arduinos.*, Circuits; Arduino, Autodesk Instructables, https://www.instructables.com/Interfacing-Electronic-Circuits-to-Arduinos/

Airlines Electronic Engineering Committee. 17 May 2004, *ARINC Specification 429 Part 1-17: Mark 33 – Digital Information Transfer System (DITS).*, ARINC Document, Aeronautical Radio Inc., https://read.pudn.com/downloads111/ebook/462196/429P1-17_Errata1.pdf, https://web.archive.org/web/20201013031536/https://read.pudn.com/downloads111/ebook/462196/429P1-17_Errata1.pdf

D. De Santo, C.S. Malavenda, S.P. Romano, C. Vecchio. 2021, *Exploiting the MIL-STD-1553 avionic data bus with an active cyber device.*, Computers & Security, Volume 100, 2021, 102097, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102097, https://www.sciencedirect.com/science/article/pii/S0167404820303709

Gilboa-Markevich, N., Wool, A. 2020, *Hardware Fingerprinting for the ARINC 429 Avionic Bus.*, In: Chen, L., Li, N., Liang, K., Schneider, S. (eds) Computer Security – ESORICS 2020. ESORICS 2020. Lecture Notes in Computer Science(), vol 12309. Springer, Cham. https://doi.org/10.1007/978-3-030-59013-0_3

Kiley, Patrick. 30 Jul. 2019, *Investigating CAN Bus Network Integrity in Avionics Systems.*, Rapid7, https://www.

rapid7.com/research/report/
investigating-can-bus-network-integrity-in-avionics-systems/