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

Matthew Preston Video Update 1 Group 4

Overview

- Activities from the past week
- Ideas for upcoming week
- Areas for feedback

Activities from the past week

- Research on bus architecture
- Research on bus security solutions
- Creation of System and Threat model
- Creation of first LRU & and flight simulation *

Research

Label (octal value) - Stated Function of Packet								SDI		Data																SSM	P
								Source / Dest ID		Equip ID			Discrete, Binary Coded Decimal, or Binary Data														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

8	7	6	5	4	3	2	1	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Label								SDI		LSB			Data															MSB	SSM		P

ARINC 429 Word Transfer Order

Source: ARINC 429 Specification Tutorial, B. Waldmann

ARINC 429 Word Example - Full Authority Engine Control B

Parity bit -> 12 "1"s = 0

Label (octal value) - Stated Function of Packet								SDI		Data																SSM	P
								Source / Dest ID		Sign	Binary Data - % from –5% to 105%																
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0

0o375

Dead bits (unused)

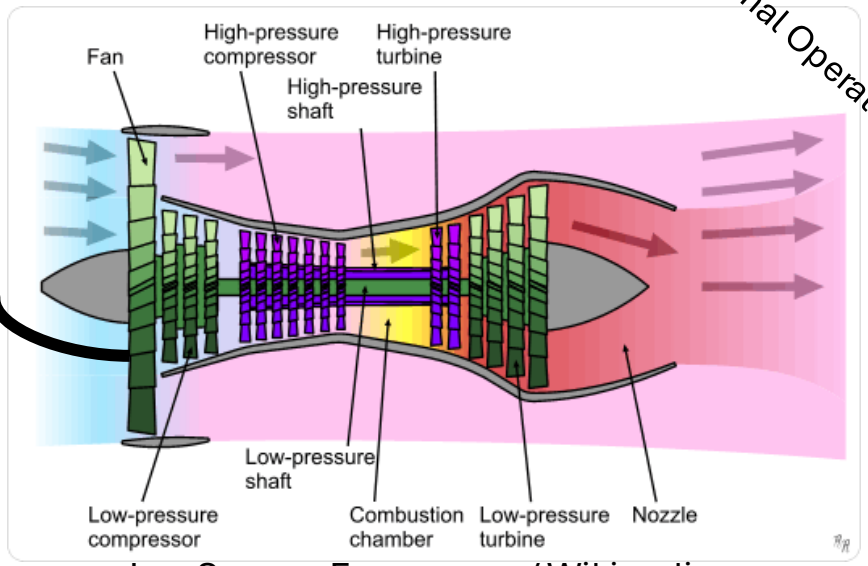
+ 70 %

Normal Operations

Flight Management Computer

(ARINC 429 bus)

Img Source: SITAL Technologies ARINC -429 IP with Cyber and Wirefault Protection Catalogue Page



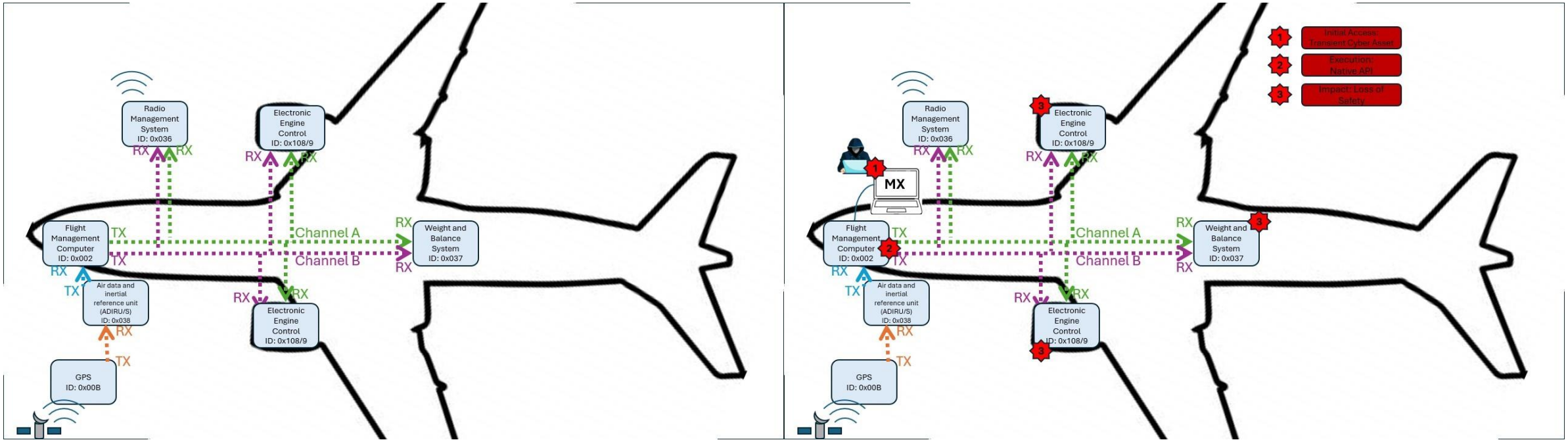
Img Source: Emoscopes / Wikipedia

```
applicable_labels_BCD = {
        0o046: 'BCD', # Engine Serial No. (LSDs) -> BCD
        0o047: 'BCD', # Engine Serial No. (MSDs) -> BCD
    }

applicable_lables_DISC = {

        0o270: 'DISC', # Discrete Data #1 -> DISC
        0o271: 'DISC', # Discrete Data #2 -> DISC
        0o272: 'DISC', # Discrete Data #3 -> DISC
        0o273: 'DISC', # Discrete Data #4 -> DISC
        0o274: 'DISC', # Discrete Data #5 -> DISC
        0o275: 'DISC', # Discrete Data #6 -> DISC

        0o350: 'DISC', # Maintenance Data #1 -> DISC
        0o351: 'DISC', # Maintenance Data #2 -> DISC
        0o352: 'DISC', # Maintenance Data #3 -> DISC
        0o353: 'DISC', # Maintenance Data #4 -> DISC
        0o354: 'DISC', # Maintenance Data #5 -> DISC

    }

applicable_lables_BNR = {
        0o114: 'BNR', # Selected Ambient Static Pressure -> BNR
        0o127: 'BNR', # Fan Discharge Static Pressure -> BNR
        0o130: 'BNR', # Selected Total Air Temperature -> BNR
        0o133: 'BNR', # Selected Throttle Lever Angle -> BNR
        0o134: 'BNR', # Throttle Lever Angle -> BNR
        0o137: 'BNR', # Selected Thrust Reverser Position -> BNR
        0o155: 'BNR', # Maintenance Data #6 -> DISC
        0o156: 'BNR', # Maintenance Data #7 -> DISC
        0o157: 'BNR', # Maintenance Data #8 -> DISC
        0o160: 'BNR', # Maintenance Data #9 -> DISC
        0o161: 'BNR', # Maintenance Data #10 -> DISC
        0o203: 'BNR', # Ambient Static Pressure -> BNR
        0o205: 'BNR', # Mach Number -> BNR
        0o211: 'BNR', # Total Fan Inlet Temperature -> BNR
        0o244: 'BNR', # Fuel Mass Flow -> BNR
        0o260: 'BNR', # LP Turbine Discharge Temperature -> BNR
        0o261: 'BNR', # LP Turbine Inlet Pressure -> BNR
        0o262: 'BNR', # HP Compressor Inlet Total Pressure -> BNR
        0o263: 'BNR', # Selected Compressor Inlet Temperature (Total) -> BNR
        0o264: 'BNR', # Selected Compressor Discharge Temperature -> BNR
        0o265: 'BNR', # Selected Compressor Discharge Temperature -> BNR
        0o267: 'BNR', # HP Compressor Inlet Temperature (Total) -> BNR

        0o300: 'BNR', # ECU Internal Temperature -> BNR
        0o301: 'BNR', # Demanded Fuel Metering Valve Position -> BNR
        0o302: 'BNR', # Demanded Variable Stator Vane Position -> BNR
        0o303: 'BNR', # Demanded Variable Bleed Valve Position -> BNR
        0o304: 'BNR', # Demanded HPT Clearance Valve Position -> BNR
        0o305: 'BNR', # Demanded LPT Clearance Valve Position -> BNR
        0o316: 'BNR', # Engine Oil Temperature -> BNR
        0o321: 'BNR', # Exhaust gas Temperature (Total -> BNR
        0o322: 'BNR', # Total Compressor Discharge Temperature -> BNR
        0o323: 'BNR', # Variable Stator Vane Position -> BNR
        0o324: 'BNR', # Selected Fuel Metering Valve Position -> BNR
        0o325: 'BNR', # Selected Fuel Metering Vane Position -> BNR
        0o327: 'BNR', # Compressor Discharge Static Pressure -> BNR
        0o330: 'BNR', # Fuel Metering Valve Position -> BNR
        0o331: 'BNR', # Selected HPT Clearance Valve Postion -> BNR
        0o335: 'BNR', # Selected Variable Bleed Valve Position -> BNR
        0o336: 'BNR', # Variable Bleed Value Position -> BNR
        0o337: 'BNR', # HPT Clearance Valve Position -> BNR
        0o341: 'BNR', # Command Fan Speed -> BNR
        0o342: 'BNR', # Maximum Allowed Fan Speed -> BNR
        0o343: 'BNR', # N1 Command vs. TLA -> BNR
        0o344: 'BNR', # Selected Actual Core Speed -> BNR
        0o345: 'BNR', # Selected Exhaust Gas Temperature (Total) -> BNR
        0o346: 'BNR', # Selected Actual Fan Speed -> BNR
        0o347: 'BNR', # LPT Clearance Valve Position -> BNR

        0o360: 'BNR', # Throttle Rate of Change -> BNR
        0o363: 'BNR', # Derivative of Thrust vs. N1 -> BNR
        0o372: 'BNR', # Actual Fan Speed -> BNR
        0o373: 'BNR', # Actual Core Speed -> BNR
        0o374: 'BNR', # Left Thrust Reverser Position -> BNR
        0o375: 'BNR' # Right Thrust Reverser Position -> BNR
}
```

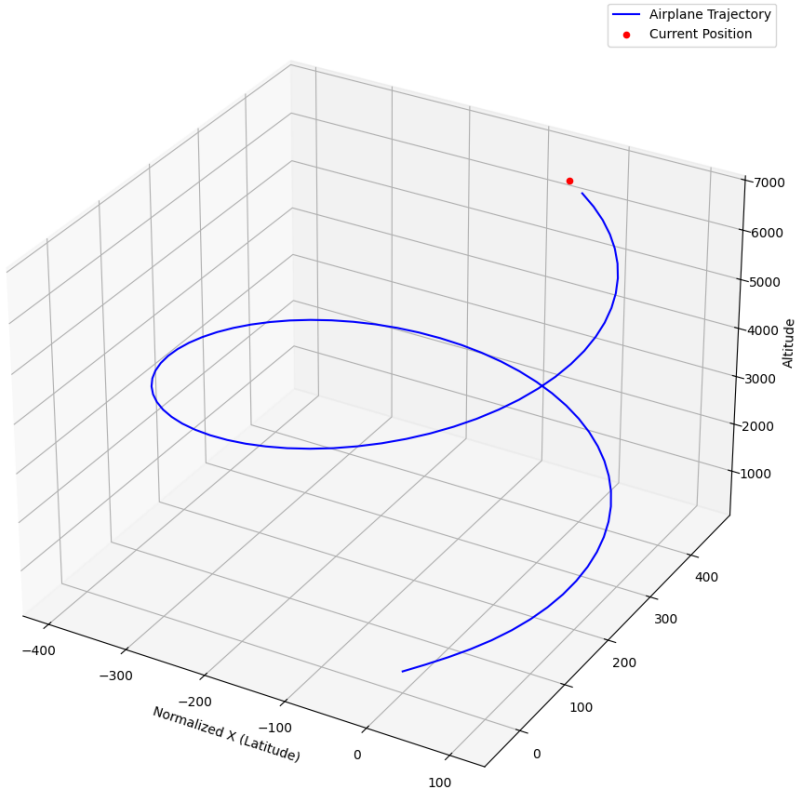
Research

- Many articles calling for more cybersecurity for avionics bus architectures
- White house & Executive branch want to move their assets to zero trust for cybersecurity
- 2 Papers of interest
  - "Hardware Fingerprinting for the ARINC 429 Avionic Bus"
  - "Exploiting the MIL-STD-1553 avionic data bus with an active cyber device"

System & Threat Model



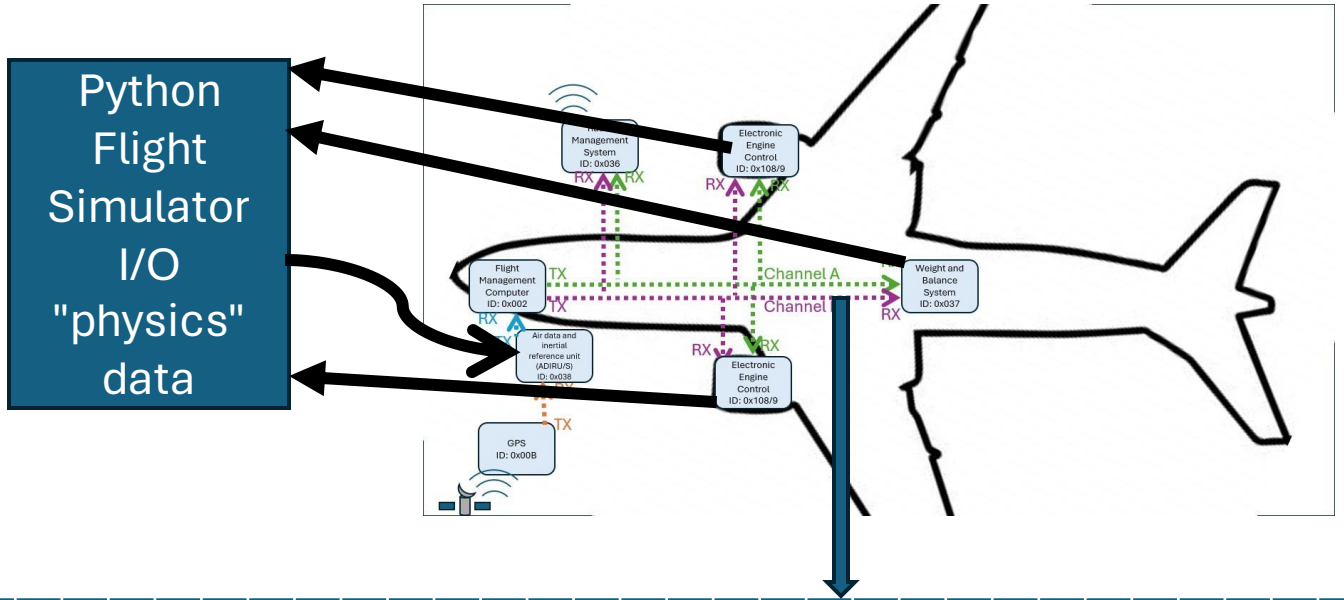
Creation of LRU #1 & Flight Simulator




```
applicable_labels_BCD = {
        0o046: 'BCD', # Engine Serial No. (LSDs) -> BCD
        0o047: 'BCD', # Engine Serial No. (MSDs) -> BCD
    }

applicable_lables_DISC = {

        0o270: 'DISC', # Discrete Data #1 -> DISC
        0o271: 'DISC', # Discrete Data #2 -> DISC
        0o272: 'DISC', # Discrete Data #3 -> DISC
        0o273: 'DISC', # Discrete Data #4 -> DISC
        0o274: 'DISC', # Discrete Data #5 -> DISC
        0o275: 'DISC', # Discrete Data #6 -> DISC

        0o350: 'DISC', # Maintenance Data #1 -> DISC
        0o351: 'DISC', # Maintenance Data #2 -> DISC
        0o352: 'DISC', # Maintenance Data #3 -> DISC
        0o353: 'DISC', # Maintenance Data #4 -> DISC
        0o354: 'DISC', # Maintenance Data #5 -> DISC

    }

applicable_lables_BNR = {
        0o114: 'BNR', # Selected Ambient Static Pressure -> BNR
        0o127: 'BNR', # Fan Discharge Static Pressure -> BNR
        0o130: 'BNR', # Selected Total Air Temperature -> BNR
        0o133: 'BNR', # Selected Throttle Lever Angle -> BNR
        0o134: 'BNR', # Throttle Lever Angle -> BNR
        0o137: 'BNR', # Selected Thrust Reverser Position -> BNR
        0o155: 'BNR', # Maintenance Data #6 -> DISC
        0o156: 'BNR', # Maintenance Data #7 -> DISC
        0o157: 'BNR', # Maintenance Data #8 -> DISC
        0o160: 'BNR', # Maintenance Data #9 -> DISC
        0o161: 'BNR', # Maintenance Data #10 -> DISC
        0o203: 'BNR', # Ambient Static Pressure -> BNR
        0o205: 'BNR', # Mach Number -> BNR
        0o211: 'BNR', # Total Fan Inlet Temperature -> BNR
        0o244: 'BNR', # Fuel Mass Flow -> BNR
        0o260: 'BNR', # LP Turbine Discharge Temperature -> BNR
        0o261: 'BNR', # LP Turbine Inlet Pressure -> BNR
        0o262: 'BNR', # HP Compressor Inlet Total Pressure -> BNR
        0o263: 'BNR', # Selected Compressor Inlet Temperature (Total) -> BNR
        0o264: 'BNR', # Selected Compressor Discharge Temperature -> BNR
        0o265: 'BNR', # Selected Compressor Discharge Temperature -> BNR
        0o267: 'BNR', # HP Compressor Inlet Temperature (Total) -> BNR

        0o300: 'BNR', # ECU Internal Temperature -> BNR
        0o301: 'BNR', # Demanded Fuel Metering Valve Position -> BNR
        0o302: 'BNR', # Demanded Variable Stator Vane Position -> BNR
        0o303: 'BNR', # Demanded Variable Bleed Valve Position -> BNR
        0o304: 'BNR', # Demanded HPT Clearance Valve Position -> BNR
        0o305: 'BNR', # Demanded LPT Clearance Valve Position -> BNR
        0o316: 'BNR', # Engine Oil Temperature -> BNR
        0o321: 'BNR', # Exhaust gas Temperature (Total -> BNR
        0o322: 'BNR', # Total Compressor Discharge Temperature -> BNR
        0o323: 'BNR', # Variable Stator Vane Position -> BNR
        0o324: 'BNR', # Selected Fuel Metering Valve Position -> BNR
        0o325: 'BNR', # Selected Fuel Metering Vane Position -> BNR
        0o327: 'BNR', # Compressor Discharge Static Pressure -> BNR
        0o330: 'BNR', # Fuel Metering Valve Position -> BNR
        0o331: 'BNR', # Selected HPT Clearance Valve Postion -> BNR
        0o335: 'BNR', # Selected Variable Bleed Valve Position -> BNR
        0o336: 'BNR', # Variable Bleed Value Position -> BNR
        0o337: 'BNR', # HPT Clearance Valve Position -> BNR
        0o341: 'BNR', # Command Fan Speed -> BNR
        0o342: 'BNR', # Maximum Allowed Fan Speed -> BNR
        0o343: 'BNR', # N1 Command vs. TLA -> BNR
        0o344: 'BNR', # Selected Actual Core Speed -> BNR
        0o345: 'BNR', # Selected Exhaust Gas Temperature (Total) -> BNR
        0o346: 'BNR', # Selected Actual Fan Speed -> BNR
        0o347: 'BNR', # LPT Clearance Valve Position -> BNR

        0o360: 'BNR', # Throttle Rate of Change -> BNR
        0o363: 'BNR', # Derivative of Thrust vs. N1 -> BNR
        0o372: 'BNR', # Actual Fan Speed -> BNR
        0o373: 'BNR', # Actual Core Speed -> BNR
        0o374: 'BNR', # Left Thrust Reverser Position -> BNR
        0o375: 'BNR' # Right Thrust Reverser Position -> BNR
    }
```

Ideas for upcoming week

- Finalizing the flight simulator to have positional data to feed into LRUs in the future.
- Create the code that will be the Flight Management Computer LRU simulation.
- Create the code that will be the weight and balance system LRU simulation.



1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

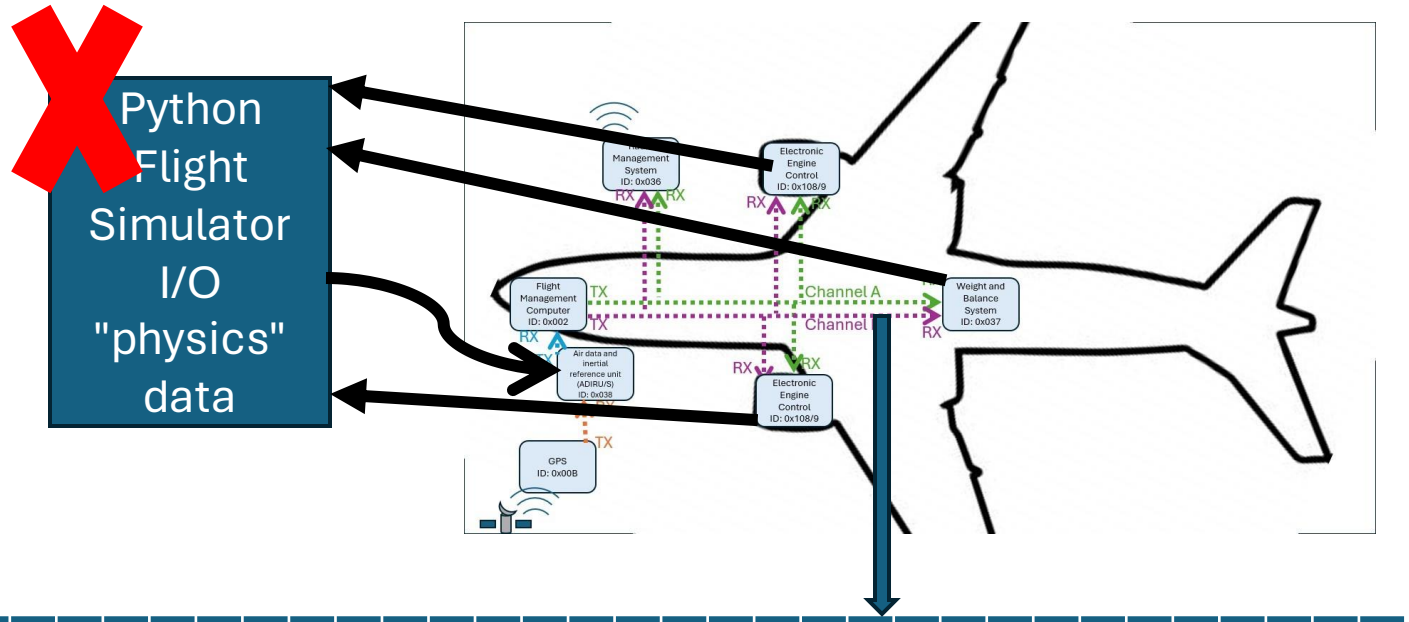
1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

... etc

Areas for Feedback

- Is the flight simulator a good idea or waste of time?
- Is the system model accurate enough for a good testing base?
- Is the threat model too simple?
- Is the threat model too similar to the research paper's?
- Anything else?



IDS

1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

... etc