

Solving Cyber Security on Avionics Databusses

The need for Cyber Security is well-known today, more than ever, and affects everyone's daily life. With that being said, it is surprising that some of the most sensitive data out there is barely protected at all. I am referring to Avionics Databusses, found on every major [Military and Commercial] aircraft flying today.

PBA.pro: Turnkey solution for Cyber Security Testing on Avionics Databusses.
 Michael J. Randazzo, Director of Applications Engineering

In addition, as more avionics types of buses are being deployed and interconnected [in both new and updated aircraft] there is an increasing concern that these vulnerabilities in security might allow unauthorized access to devices communicating on these busses.

The most concerning bus is MIL-STD-1553, which was designed before the term "Cyber Security" was even invented. The concern is that this bus, which was designed with no infiltration protection, could be easily corrupted or manipulated if any unintended data made it on to the databus.

There are already multiple government and private industry organizations studying the problem with the goal of establishing suitable methods to assure complete aircraft databus cyber security.

As a result of these efforts, AIM has developed a suite of tools that can be utilized to interface with MIL-STD-1553 [and other protocols, i.e. ARINC429, ARINC664/AFDX, Ethernet, CANBus] equipment to analyze, attack, detect and remove potential security vulnerabilities.

Vulnerability Detection

Since there are thousands of fielded avionics computers using MIL-STD-1553 today, the most logical initial approach would be to see if any vulnerabilities exist. More simply put, "can the computer be made to do something it's not supposed to."

PBA.pro contains a concurrent real-time 1553 Bus Monitor (BM), so all 100% of the data that is on the bus can be recorded and post-analyzed at any time. Depot, lab or rugged units are available to support all aspects of flight test.

In addition, recorded data can be always be replayed to reproduce any scenario.

The issue with just looking at "Raw" 1553 data is that most 1553 data requires further decoding (such as a scale factor) to determine its true meaning to perform a "credibility analysis".

PBA.pro handles this with ease by including a Database Manager (ICD) component, which can decode and interpret the raw 1553 data in its true Engineering Unit

(EU). Once the Engineering Unit is decoded, PBA.pro can then scan the recorded data and verify that every bit of data is valid, comprehensible and documented (See Figure 1).

PBA.pro has the ability to perform real-time or post-time credibility analysis in the following areas:

- EU is within ICD Range and valid.
- Undocumented ICD Data detected on bus.
- EU Rate is valid and within tolerance
- 1553 Errors detected on bus

Table 1: Data credibility analysis.

Index	Time (s)	Offset (s)	Alias	ID	Type	Source	TransType	Result	ModeCode	Bus
12	1304176.25	56.7807620000	16.000	0000	1553	MIL	Bi-TerM	1	1	Pa
13	1304176.25	56.7867620000	16.001	0006	1553	MIL	Bi-TerM	1	1	Pa
14	1304176.25	56.8127620000	16.000	000F	1553	MIL	Bi-TerM	1	1	Pa
15	1304176.25	56.8387620000	16.000	0000	1553	MIL	Bi-TerM	1	1	Pa
16	1304176.25	56.8647620000	16.000	0001	1553	MIL	Bi-TerM	1	1	Pa
17	1304176.25	56.8907620000	16.001	0002	1553	MIL	Bi-TerM	1	1	Pa
18	1304176.25	56.9167620000	16.000	0003	1553	MIL	Bi-TerM	1	1	Pa
19	1304176.25	56.9427620000	16.000	0004	1553	MIL	Bi-TerM	1	1	Pa
20	1304176.25	56.9687620000	16.000	0005	1553	MIL	Bi-TerM	1	1	Pa
21	1304176.25	56.9947620000	16.001	0006	1553	MIL	Bi-TerM	1	1	Pa
22	1304176.25	57.0207620000	16.000	0007	1553	MIL	Bi-TerM	1	1	Pa
23	1304176.25	57.0467620000	16.001	0008	1553	MIL	Bi-TerM	1	1	Pa
24	1304176.25	57.0727620000	16.000	0009	1553	MIL	Bi-TerM	1	1	Pa
25	1304176.25	57.0987620000	16.000	000A	1553	MIL	Bi-TerM	1	1	Pa
26	1304176.25	57.1247620000	16.000	000B	1553	MIL	Bi-TerM	1	1	Pa
27	1304176.25	57.1507620000	16.000	000C	1553	MIL	Bi-TerM	1	1	Pa
28	1304176.25	57.1767620000	16.000	000D	1553	MIL	Bi-TerM	1	1	Pa
29	1304176.25	57.2027620000	16.000	000E	1553	MIL	Bi-TerM	1	1	Pa
30	1304176.25	57.2287620000	16.000	000F	1553	MIL	Bi-TerM	1	1	Pa
31	1304176.25	57.2547620000	16.000	0000	1553	MIL	Bi-TerM	1	1	Pa
32	1304176.25	57.2807620000	16.001	0001	1553	MIL	Bi-TerM	1	1	Pa
33	1304176.25	57.3067620000	16.000	0002	1553	MIL	Bi-TerM	1	1	Pa
34	1304176.25	57.3327620000	16.002	0003	1553	MIL	Bi-TerM	1	1	Pa

Figure 1: Verifying EU in-range data.

Intrusion Simulation

Once the “expected and accepted” data is known, it’s time to see how a 1553 Unit-Under-Test (UUT) reacts to unexpected anomalies.

PBA.pro has the ability to inject many electrical errors (See Table 2) that violate the MIL-STD-1553 specification, with the intention to determine how a UUT reacts.

In addition to the above, PBA.pro can simulate a multiple BC or duplicate RT scenario or even inject 1553 messages during detected Bus Idle (dead) time.

CMD/DATA SYNC INVERSE
WORD/BIT COUNT CHANGES
PARITY ERROR INSERTION
MANCHESTER BIT FAULTS
ZERO CROSSING ERRORS
PARITY ERROR INSERTION

Table 2: Data credibility analysis.

MIL-STD-1553 COMPLIANCE TESTING

Although it is expected that a deployed (flying) 1553 UUT is already compliant to the MIL-STD-1553 specification, there have been exceptions and equipment has been found to fail.

PBA.pro has a completely automated off-the-shelf **SAE 4111/4112 Test Plan Suite**. These tests [published by the Society of Automotive Engineers (SAE)] are designed to validate that a 1553 Remote Terminal UUT meets all electrical and protocol requirements of the MIL-STD-1553 specification.

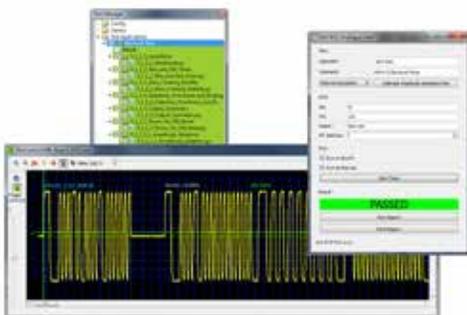


Figure 2: 1553 RT Validation Testing.

PLATFORM-LEVEL ANALYSIS.

Some of the capabilities already mentioned involve PBA.pro and a single UUT. But, in reality an Avionics databus is an interaction of many subsystems. Those interactions create another cyber security concern, requiring testing at the full system level and the vulnerabilities that come with it.

PBA.pro is a modular multi-protocol solution, supporting numerous bus types and multiple bus instances. Below is a list of some of the more popular protocols supported by PBA.pro (See Table 3).

MIL-STD-1553/1760
AFDX*/ARINC-664/EDE
FIBRE CHANNEL (FC-AE)
ARINC-429
10/100/1000 ETHERNET
CANBus* / ARINC-825

Table 3: PBA.pro protocol sampling.

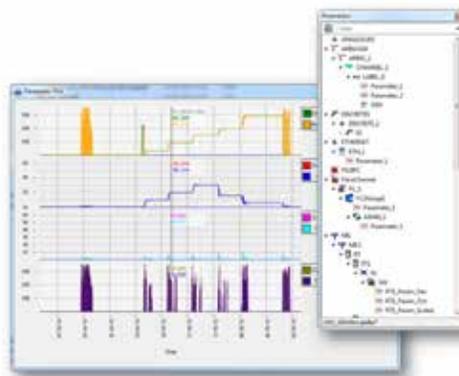


Figure 2: 1553 RT Validation Testing.

Beyond MIL-STD-1553, AIM has a suite of tools that are just as focused for other Avionics Protocols. Comprehensive Monitoring and inline data modification capabilities are currently available for ARINC-429, ARINC-664/AFDX*, 10/100/1000 Ethernet, ARINC825/CANBUS and Fibre Channel protocols.

PBA.pro is an invaluable tool to assist engineers analyze and develop methods to assure the cyber security of any Avionics databus. From laboratory to real-time flight analysis, PBA.pro offers a time-saving and powerful solution.

PICO

SURFACE MOUNT
(and thru-hole)
**Transformers
& Inductors**

Size
does
matter!



from low-profile

.18"ht.

- Audio Transformers
- Pulse Transformers
- DC-DC Converter Transformers
- MultiPlex Data Bus Transformers
- Power & EMI Inductors



VISIT OUR EXCITING
NEW WEBSITE
www.picoelectronics.com

See Pico's full Catalog immediately
www.picoelectronics.com

800 431-1064

Fax 914-738-8225

E Mail: info@picoelectronics.com



143 Sparks Ave. Pelham, N.Y. 10803-1837





Delivery - Stock to one week