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

SOLVING CYBER SECURITY ON AVIONICS DATA BUSES

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 Data Buses, found on every major [Military and Commercial] aircraft flying today.

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 buses.

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 protocol] equipment to analyze, attack, detect and remove potential security vulnerabilities.

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

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

Table 1: Data credibility analysis

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

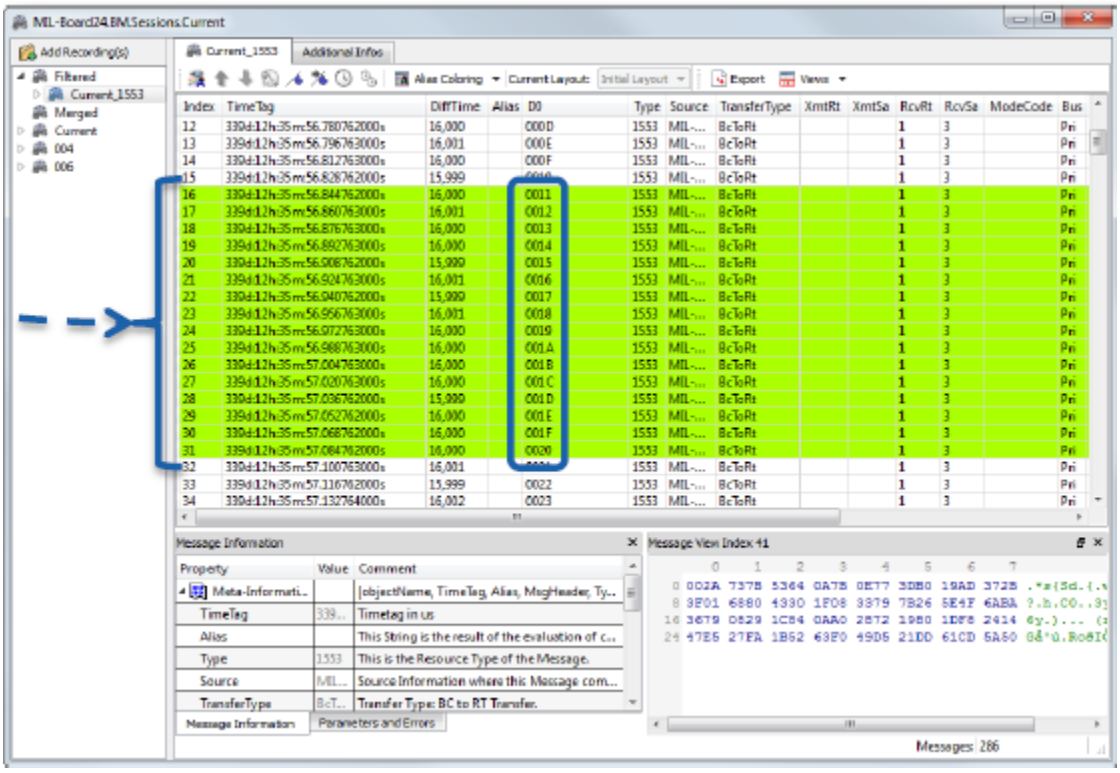

Figure 1: Verifying EU in-range data.

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**	**GAP ERROR INSERTION**
MANCHESTER BIT FAULTS	**ZERO CROSSING ERRORS**	**PARITY ERROR INSERTION**

Table 2: MIL-STD-1553 error injection sampling.

MESSAGE SUPRESSION AND REINSERTION

In order to perform certain penetration attacks, it may be required to suppress a message. Suppressing a message will stop particular data from being received by its targeted destination. PBA.pro can easily target a specific message on the bus and suppress it by disrupting the bus at the appropriate time. This will cause a bus failure and force the destination device to discard that message.

In addition, the same message can then be reinserted in Bus Idle (dead) time as described above.

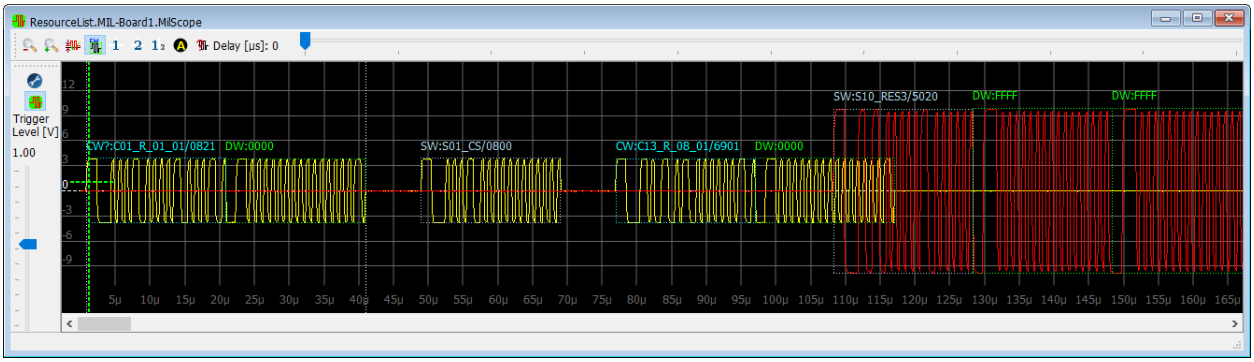

Figure 2: 1553 Message Suppression

PBA.pro: Turnkey solution for Cyber Security Testing on Avionics Data Buses

Michael J. Randazzo, Director of Applications Engineering

MIL-STD-1553 COMPLIANCE TESTING

Although is it 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.

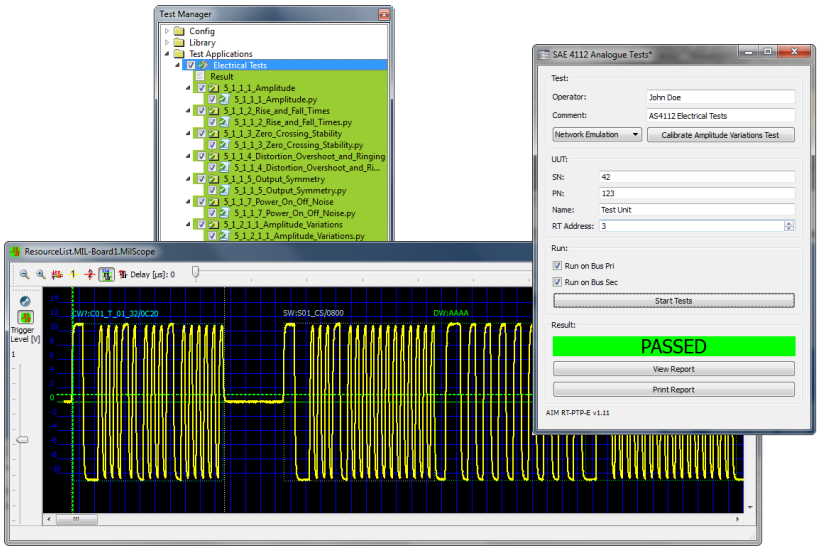

Figure 3: 1553 RT Validation Testing

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

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-Layer-2)**
ARINC-429	**10/100/1000 ETHERNET**	**CANBus® / ARINC-825**

Table 3: PBA.pro protocol sampling.

To simplify the complex analysis of multiple systems, PBA.pro includes a **Scripting Component**, which can tackle repetitive or time-consuming tasks with ease. All scripting is done with the popular Python® language, allowing easy integration with other tools, such as LabVIEW® and MATLAB.

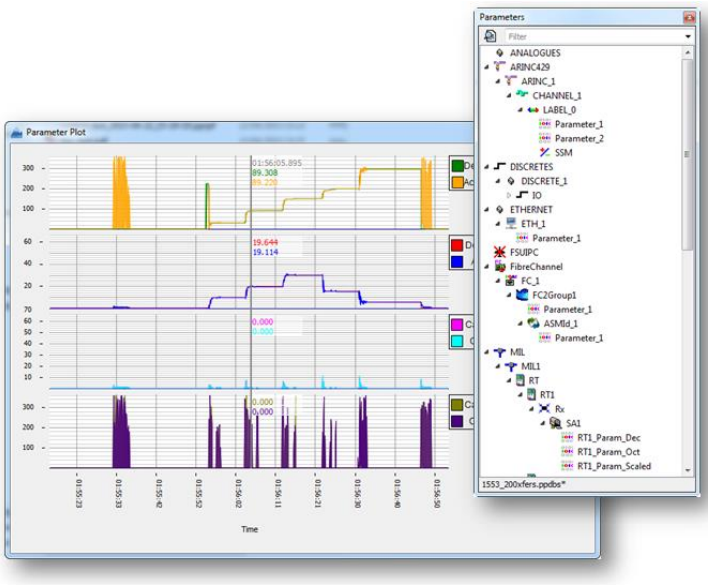

Figure 4: Verifying data across multiple Data Buses and protocols.

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

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.

AIM-USA

Seven Neshaminy Interplex, Suite 211

Trevose, PA 19053

Phone: 1-267-982-2600

Email: supportusa@aim-online.com

Web: www.aim-online.com