1553 Network and Cyber Security Testing

Cage Code: 4RK27 ● NAICS: 334119

Alta Data Technologies LLC

4901 Rockaway Blvd, Building A

Rio Rancho, NM 87124 USA

(tel) 505-994-3111 ● www.altadt.com

CUSTOMER NOTES:

Document Information:

Rev A0 Release Date: October 9, 2020

Note to the Reader and End-User:

This document is provided for information only and is copyrighted by Alta Data Technologies. While Alta strives to provide the most accurate information, there may be errors and omissions in this document. Alta disclaims all liability in document errors and any product usage. By using an Alta product, the customer or end user agrees (1) to accept Alta's Standard Terms and Conditions of Sale, Standard Warranty and Software License and (2) to not hold Alta Members, Employees, Contractors or Sales & Support Representatives responsible for any loss or legal liability, tangible or intangible, from any document errors or any product usage.

The product described in this document is not US ITAR controlled. Use of Alta products or documentation in violation of local usage, waste discard and export control rules, or in violation of US ITAR regulations, voids product warranty and shall not be supported. This document may be distributed to support government programs and projects. Third party person, company or consultant distribution is not allowed without Alta's written permission.

Contact:

We welcome comments and suggestions. Please contact us at 888-429-1553 (toll free in US) or 505-994-3111 or visit our web site for support submit forms at www.altadt.com or email us at alta.info@altadt.com or alta.support@altadt.com.

Table of Contents

Introduction 4
- Approaches to Resiliency 4
- The MIL-STD-1553 Threat Space 5

The Alta Toolset 6
- AltaView 6
  - Bus Monitor 6
  - Message Snapshot Viewer 7
  - Current Value Viewer 9
  - Signal Viewer 9
  - Bus Controller 11
  - Remote Terminal 12
- AltaAPI and AltaCore-1553 12
  - Control Blocks and the Common Data Packet 13
  - Interrupts 13
  - Signal Generator 13
- AltaRTVal 14

Conclusion 14

Introduction

Cyber security refers to the protection of network-connected systems from unauthorized access. A military or commercial-derivative aircraft contains complex avionics; a system of systems. These embedded electronics are connected using various communication networks, and are always an amalgam of new and old designs. Legacy systems and networks pose especially unique challenges for cybersecurity policy, one of which is the MIL-STD-1553 multiplex data-bus communication protocol. First released in 1973, the MIL-STD-1553 protocol continues to be the command-and-control backbone for mission critical weapons systems on military aircraft. It remains in use today because it is deterministic, fault tolerant, and time-tested; but it was not designed to address contemporary cybersecurity issues, and so acts as an entry point for cyber threats.

Approaches to Resiliency

To implement a complete, robust cybersecurity policy for 1553-based systems, we would ideally revise the protocol to include modern-day capabilities like authentication, encryption, and partitioning. However, this is impractical because it would not address the massive installed base of 1553 systems in operation; nor would it fully address newly designed platforms (F-35 Joint Strike Fighter, for example) that tend to use systems that couple modern networks with legacy 1553-based systems. MIL-STD-1760, last updated in 2007, is an aircraft-store interconnection spec that includes 1553 as a method of communication, and adds a checksum to 1553 messages. It is an improvement over 1553's word parity only check, but does not provide the protection needed for modern cyber threats.

Instead, increasing the cyber resiliency of legacy embedded systems is a piecewise process of introducing new components to support artificial intelligence/machine learning (AI/ML) algorithms. These algorithms provide anomaly and intrusion detection, logging, warning, and possibly mitigation. There are two main approaches, both of which have difficult tradeoffs to manage.

The first approach is to introduce new hardware modules running cyber software applications, either in a distributed or centralized manner, to act as traffic cops for each subsystem. This has enormous impact to system failure rate, failure modes, installation, vehicle weight and maintenance activities. The second approach is to modify the software/hardware of each existing subsystem, thereby making each unit more capable. This too has enormous impact through the ensuing qualification and test activities that need to occur for flight acceptance. Some industry efforts are focused on developing high technology-readiness levels (TRL) for these approaches.

The Aviation Cyber Initiative, chartered by the U.S. Departments of Defense, Homeland Security and Transportation, has a mission to reduce cybersecurity risks and improve cyber resilience in the aviation ecosystem. A major goal of the charter is to advance cyber research, development, test and evaluation (RDT&E) by enabling collaboration between government and its national labs with private industry and research groups. Funding for cyber efforts is on an upward trend, through Small Business Innovation Research (SBIR) programs and other contract vehicles.

Extensive test and evaluation are required to compile platform data, characterize systems, and develop solutions. Some vulnerabilities are common to all 1553-based systems, and many are unique and application-specific.

This is where Alta Data Technologies can help, with critical tools for development, analysis, simulation, and validation. The armed services and private sector partners rely on Alta's track record of innovation and quality to advance cyber RDT&E.

The MIL-STD-1553 Threat Space

The 1553 bus topology consists of a dual-redundant serial bus connected to all terminals in the system using stubs. There are three types of terminals: Bus Controller (BC), Remote Terminal (RT) and Bus Monitor (BM). The BC uses a combination of preprogrammed scheduling and on-demand transactions to initiate all exchanges between itself and RTs, as well as RT to RT transactions. An RT can be configured as a backup BC to provide failover capability.

A BM, which is incapable of transacting on the bus, can be physically independent from – or embedded within – a BC or RT as an observer. The BM can provide insight as to whether a terminal is malfunctioning by virtue of its 1553 bus activity.

Attacks require the introduction of some type of malware to an aircraft. Transmission can occur through aircraft supply chains, ground support systems such as maintenance computers and data loaders, and over-the-air through radio receivers and data links. Malware could then infect one of various onboard computers, such as mission control, engine control, navigation, displays and weapons. Operating systems, sensors and weapons that implicitly trust incoming commands could allow the malware to spread and implement offensive operations.

Cyber attacks performed by a compromised terminal on 1553 bus can include the following:

- Replacement of data in otherwise valid messages
- Insertion of new messages during unused bus time (dead bus time)
- Flooding the bus with new or ‘retry’ messages to achieve denial of service
- Suppressing scheduled messages
- Changing the state (enable/disable) of a terminal or backup controller

The Alta Toolset

Alta Data provides a suite powerful analysis tools for developers to characterize the behavior of their 1553 architectures at the physical layer and protocol layer.

- ***AltaView*** is a graphical user interface used to view and simulate network activity and perform data analysis.
- ***AltaAPI*** is a layered, modular ANSI C-based software tool kit for fast and efficient application development for communication with the AltaCore.
- ***AltaCore*** is an FPGA-based protocol engine with a common data structure for all 1553 message types and advanced signal generation capabilities.
- ***AltaRTVal*** is a software tool used to perform protocol tests on remote terminal hardware to simplify production validation. The tests are specified by the SAE AS4111 RT Validation Test Plan and the SAE AS4112 RT Production Test Plan.

AltaView

Let’s take a look at AltaView’s three main functions: Bus Monitor, Bus Controller, and Remote Terminal.

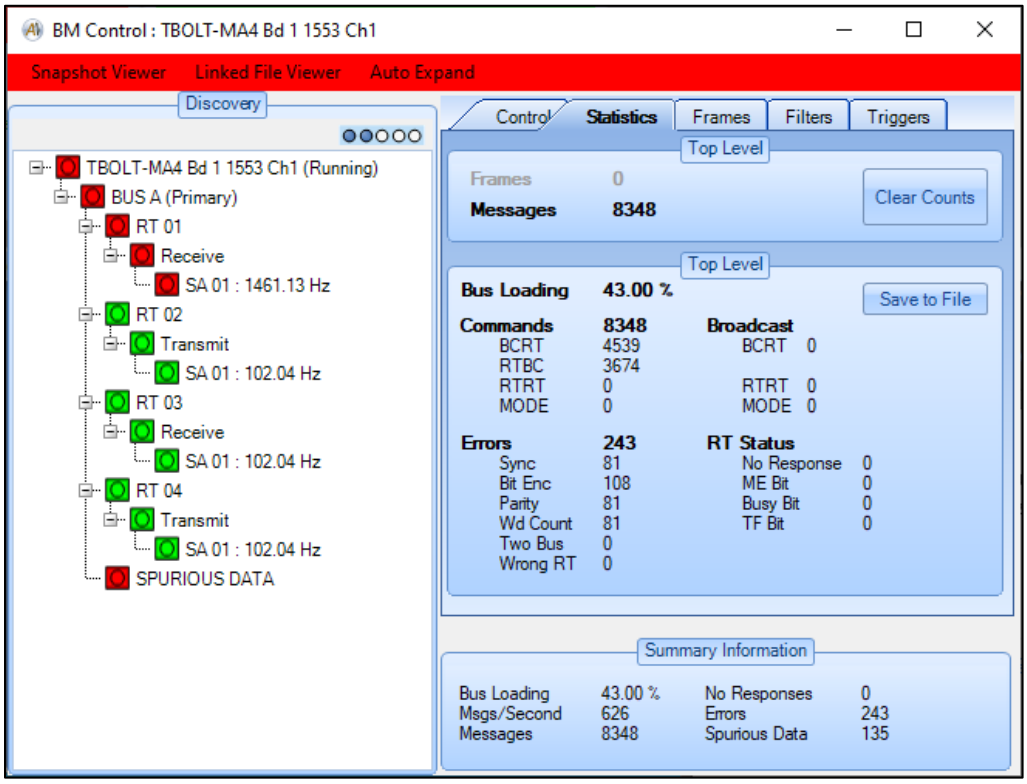
Bus Monitor

The AltaView Bus Monitor captures all activity on the 1553 bus. The Discovery window provides color-coded message detection and statistics for:

- Message frequency for each Remote Terminal and Subaddress
- Overall bus loading (%)
- Message and error counts
- Presence of spurious data

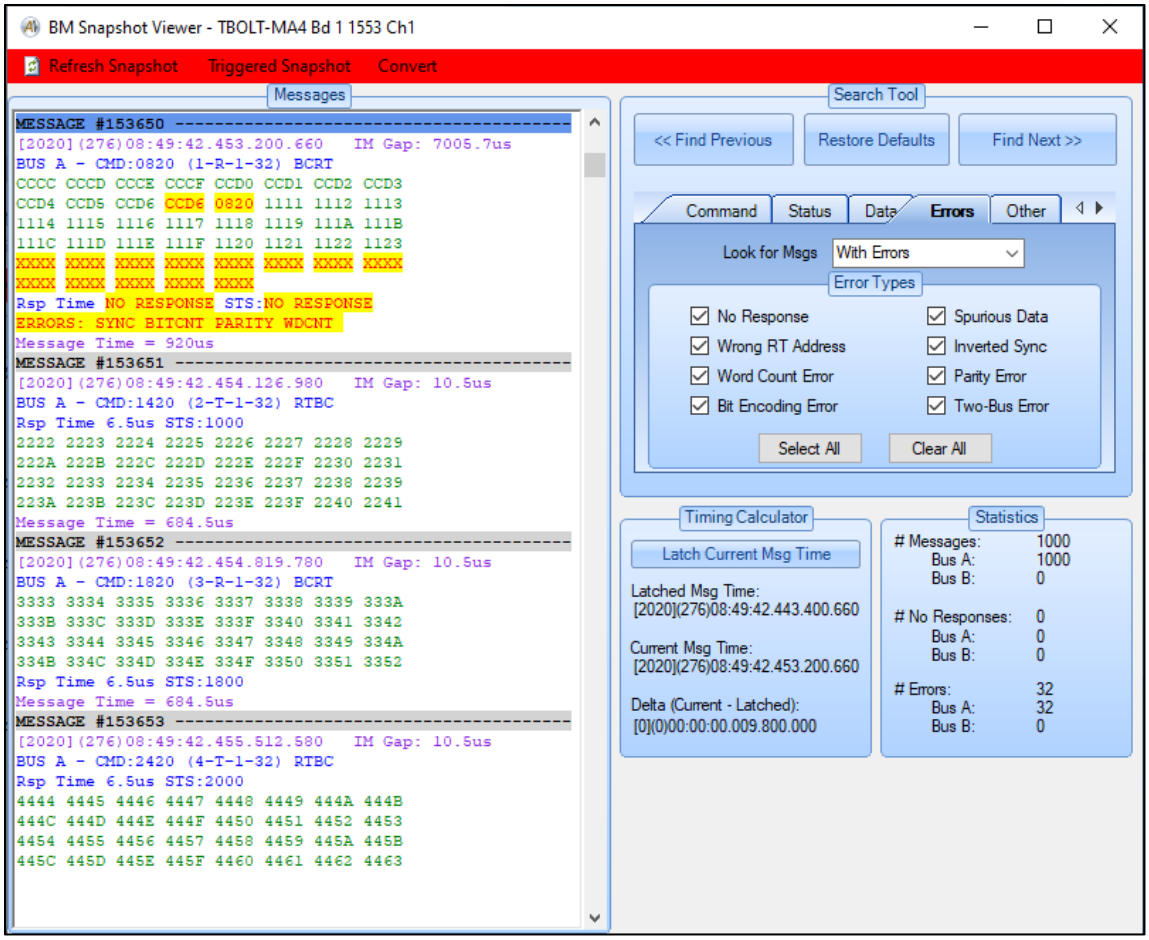
Because a 1553 system runs on a deterministic, periodic schedule, each message is expected to occur at a fixed frequency (with the exception of aperiodic messages). That makes message frequency a key indicator of overall system health, and a change in frequency of one or multiple messages can be used as a form of intrusion detection. Duplicate messages from a compromised BC or RT would increase the overall message frequency, while suppressed messages would decrease message frequency.

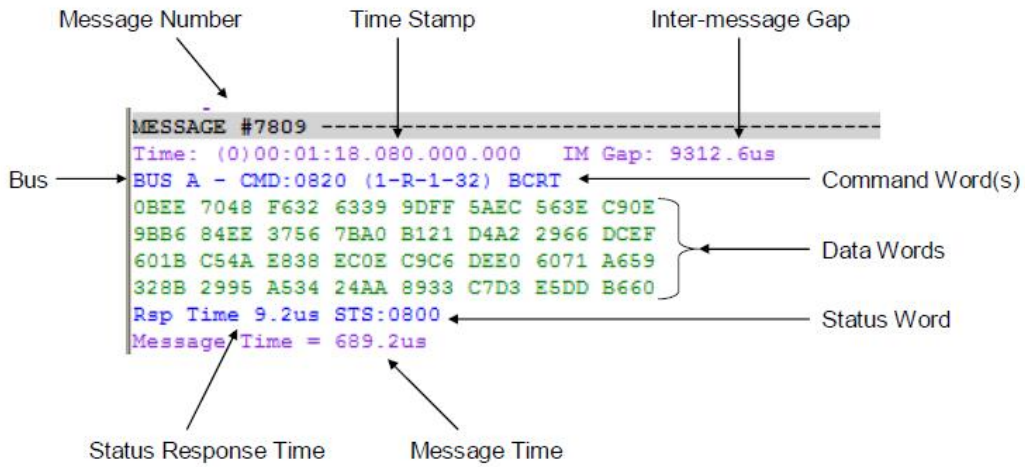
Bus collisions due to scheduling violations and malformed messages would be detected as spurious data and displayed. These attacks would be exposed by increased or decreased bus loading metrics and error counts.



Message Snapshot Viewer

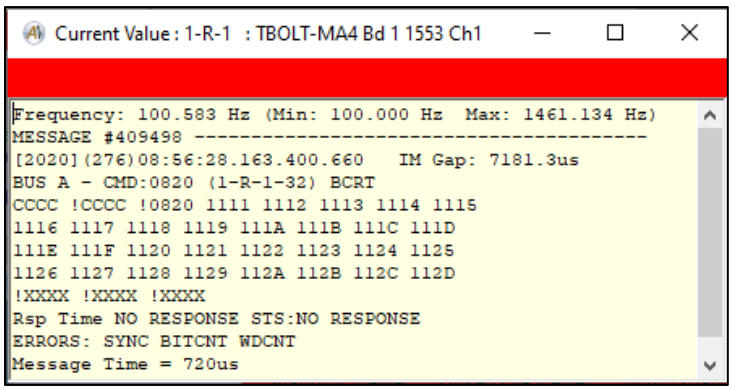
The Message Snapshot viewer provides a log of time-tagged messages and displays all relevant message and timing information. Errors are highlighted for easy identification. Extensive search capability allows messages to be found based on word content, error conditions, and timing parameters. The viewer can be used in real time or offline with previously archived data.


BM Snapshot Viewer - TBOLT-MA4 Bd 1 1553 Ch1
Refresh Snapshot
Triggered Snapshot
Convert
Messages
MESSAGE #153650 ----------
[2020](276)08:49:42.453.200.660 IM Gap: 7005.7us
BUS A - CMD:0820 (1-R-1-32) BCRT
CCCC CCCD CCCE CCCF CCD0 CCD1 CCD2 CCD3
CCD4 CCD5 CCD6 CCD6 0820 1111 1112 1113
1114 1115 1116 1117 1118 1119 111A 111B
111C 111D 111E 111F 1120 1121 1122 1123
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX
Rsp Time NO RESPONSE STS:NO RESPONSE
ERRORS: SYNC BITCNT PARITY WDCNT
Message Time = 920us
MESSAGE #153651 ----------
[2020](276)08:49:42.454.126.980 IM Gap: 10.5us
BUS A - CMD:1420 (2-T-1-32) RTBC
Rsp Time 6.5us STS:1000
2222 2223 2224 2225 2226 2227 2228 2229
222A 222B 222C 222D 222E 222F 2230 2231
2232 2233 2234 2235 2236 2237 2238 2239
223A 223B 223C 223D 223E 223F 2240 2241
Message Time = 684.5us
MESSAGE #153652 ----------
[2020](276)08:49:42.454.819.780 IM Gap: 10.5us
BUS A - CMD:1820 (3-R-1-32) BCRT
3333 3334 3335 3336 3337 3338 3339 333A
333B 333C 333D 333E 333F 3340 3341 3342
3343 3344 3345 3346 3347 3348 3349 334A
334B 334C 334D 334E 334F 3350 3351 3352
Rsp Time 6.5us STS:1800
Message Time = 684.5us
MESSAGE #153653 ----------
[2020](276)08:49:42.455.512.580 IM Gap: 10.5us
BUS A - CMD:2420 (4-T-1-32) RTBC
Rsp Time 6.5us STS:2000
4444 4445 4446 4447 4448 4449 444A 444B
444C 444D 444E 444F 4450 4451 4452 4453
4454 4455 4456 4457 4458 4459 445A 445B
445C 445D 445E 445F 4460 4461 4462 4463
Search Tool
<< Find Previous
Restore Defaults
Find Next >>
Command
Status
Data
Errors
Other
Look for Msgs
With Errors
Error Types
No Response
Wrong RT Address
Word Count Error
Bit Encoding Error
Spurious Data
Inverted Sync
Parity Error
Two-Bus Error
Select All
Clear All
Timing Calculator
Latch Current Msg Time
Latched Msg Time:
[2020](276)08:49:42.443.400.660
Current Msg Time:
[2020](276)08:49:42.453.200.660
Delta (Current - Latched):
[0](0)00:00:00.009.800.000
Statistics
Messages: 1000
Bus A: 1000
Bus B: 0
No Responses: 0
Bus A: 0
Bus B: 0
Errors: 32
Bus A: 32
Bus B: 0


Message Number
Time Stamp
Inter-message Gap
MESSAGE #7809 ----------
Time: (0)00:01:18.080.000.000 IM Gap: 9312.6us
Bus
BUS A - CMD:0820 (1-R-1-32) BCRT
Command Word(s)
0BEE 7048 F632 6339 9DFF 5AEC 563E C90E
9BB6 84EE 3756 7BA0 B121 D4A2 2966 DCEF
601B C54A E838 EC0E C9C6 DEE0 6071 A659
328B 2995 A534 24AA 8933 C7D3 E5DD B660
Data Words
Rsp Time 9.2us STS:0800
Status Word
Message Time = 689.2us
Status Response Time
Message Time

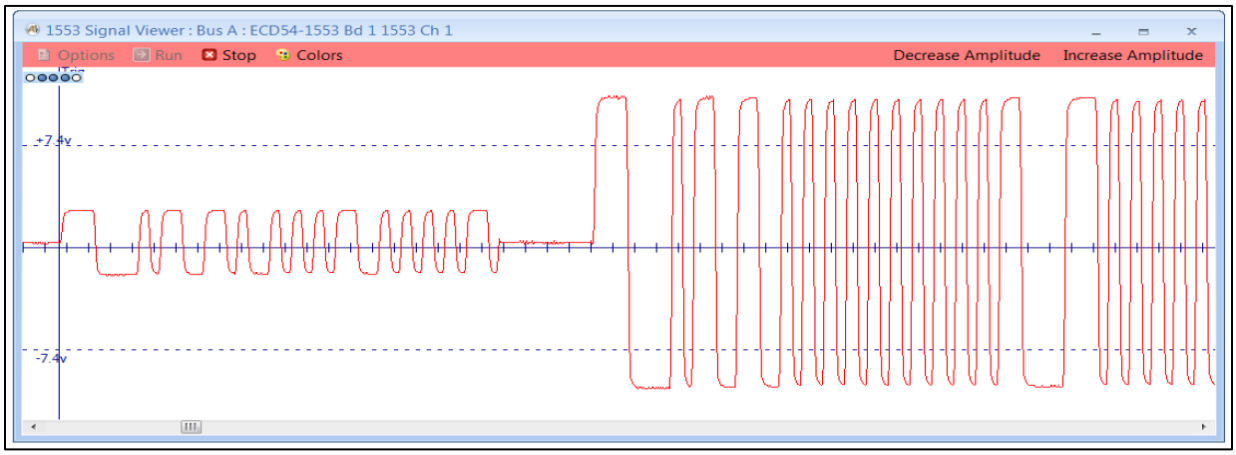
Current Value Viewer

The Current Value viewer provides a watch window for a particular RT and subaddress, including the current, minimum, and maximum message frequency.

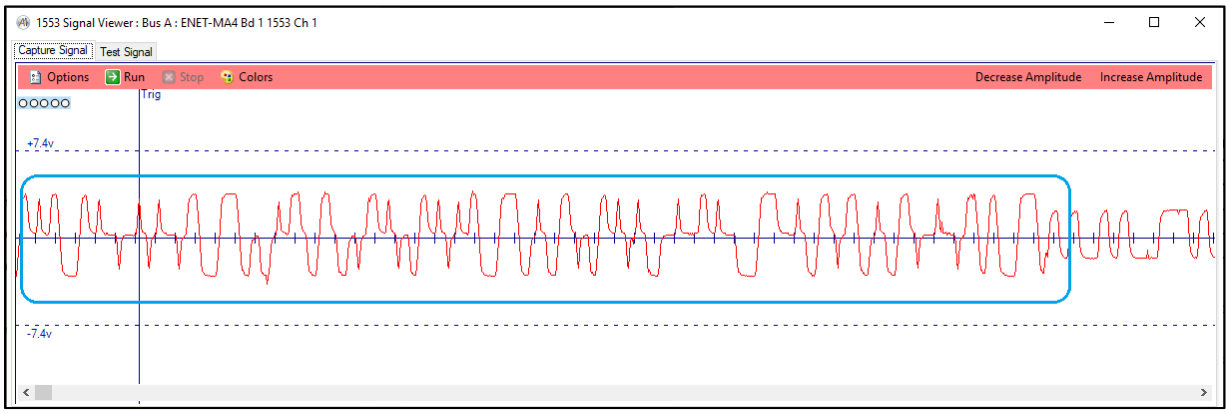


Signal Viewer

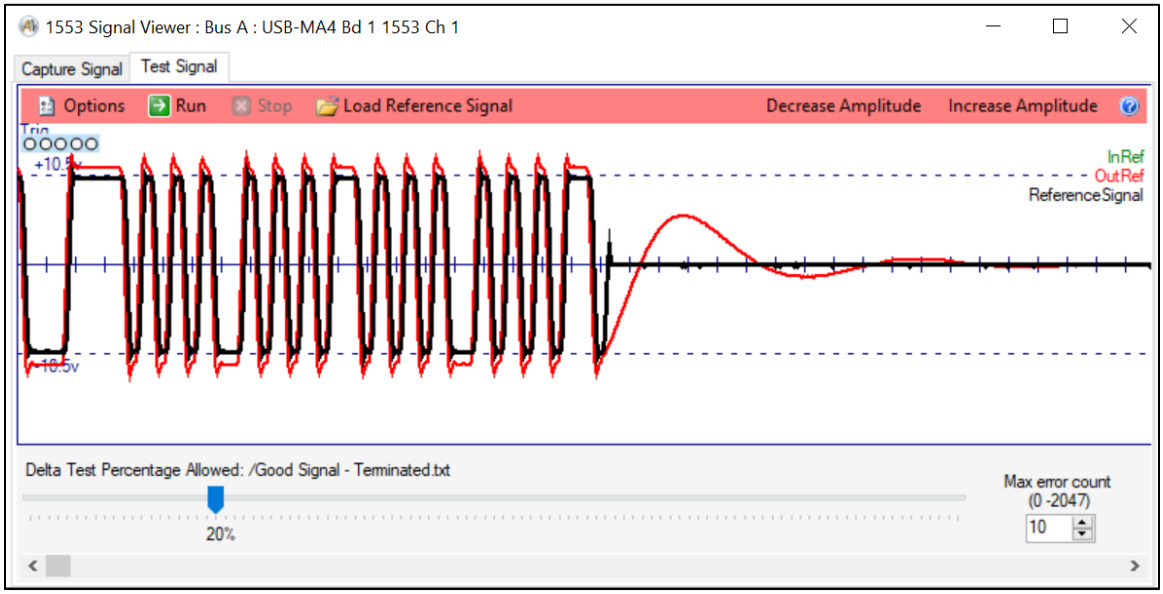
The Signal Viewer is an industry-first unique feature that uses the analog-to-digital converter on the front-end of Alta's 1553 interface hardware to display electrical signal waveforms. The time base is 50 nanoseconds per sample, and the voltage can be scaled. Sample data can be exported to other formats for additional analysis. Various trigger options are available. This is useful for detecting signal presence, amplitude levels, and signal integrity.



Signal Viewer will also display bus collisions associated with spurious data. This can indicate that a terminal is not transacting according to the predetermined BC schedule.

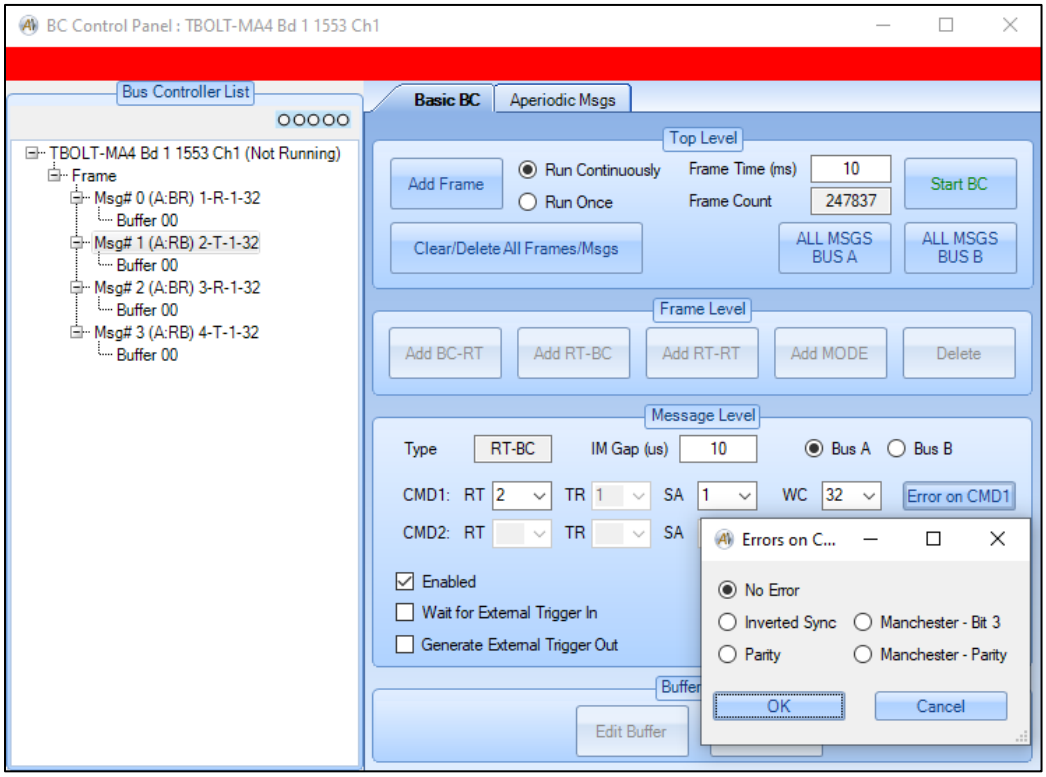


Electrical characterization of a 1553 network is a potential method for providing anomaly and intrusion detection. Signal Viewer's comparison tool allows a recorded reference signal to be compared with current bus waveforms to help detect any physical changes to the network, such as a modified terminal or bus termination.



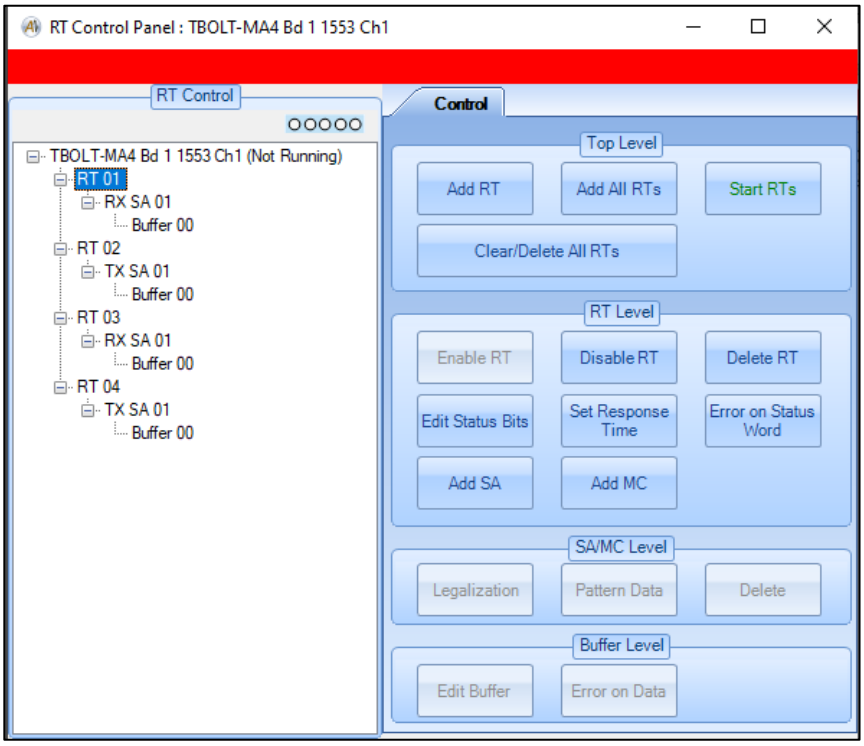
Bus Controller

The AltaView Bus Controller provides advanced control of scheduling and messages. Errors can be injected into message timing, message parameters, sync polarity, data parity, and other message bits. Aperiodic (on-demand) messaging allows messages to be injected during dead bus time. Multiple BCs can be run (on separate hardware channels) to inject messages and cause bus collisions.



Remote Terminal

AltaView allows the simulation of up to 32 RTs (per 1553A), or 31 RTs (per 1553B) simultaneously. Each RT supports modification of status bits, error injection, and word count legalization. Multiple data buffers can be used to vary data content. Various RT responses can be used to simulate system behavior in the presence of compromised RTs.



AltaAPI and AltaCore-1553

The AltaAPI is a properly modeled OSI layer 3 package that is easy to program and very portable across OS platforms. It is a C-based library of functions that provides programmatic control of AltaCore-1553, a firmware-based protocol engine resident on all Alta hardware products.

AltaCore-1553 has the industry's most advanced 1553 offload engine controls, as well as full protocol engine error injection and signal generation tools. It also has a unique packetizing engine, utilizing Common Data Packets, that enable BC, RT and BM functions to see the exact same encoder/decoder controls and results. No other 1553 product on the market today has this.

Together, they provide maximum flexibility and capability for the 1553 interface. The AltaAPI enables a deeper level of error injection and electrical signal control than does AltaView.

Control Blocks and the Common Data Packet

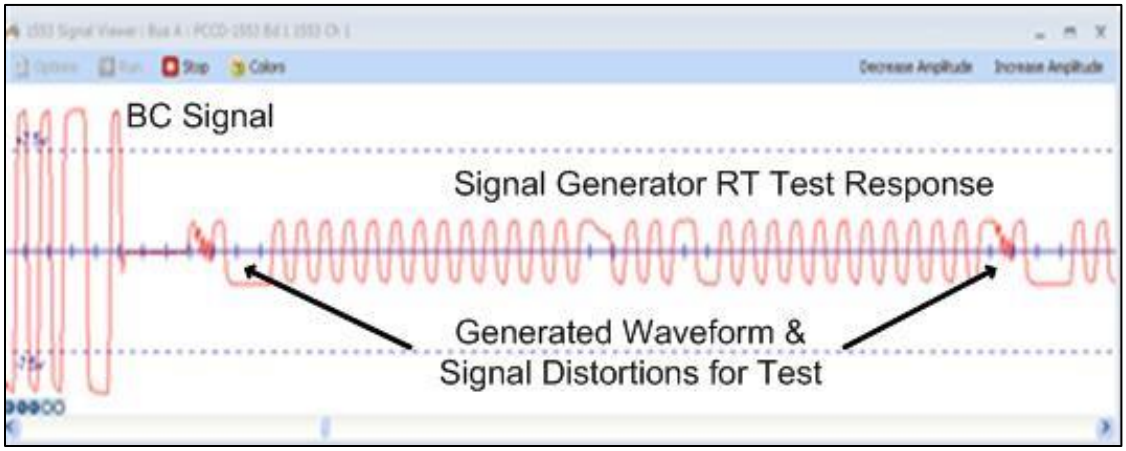
A key API memory structure is the Control Block. Control Blocks for the BC and RT allow for error injection and detection in command words and status words, as well as control of timing and interrupt behavior. Another key API memory structure is the Common Data Packet (CDP). Each CDP contains information for one 1553 message. The CDP controls error injection and detection, interrupts, and time tags down to the individual data word level, and even word-level gap timing. This information allows BC, RT or Monitor applications to have a complete snapshot of message status.

Interrupts

Interrupts can be used to warn an application of various events that could signify cyber intrusion. For example, not all mode codes, RTs, or RT sub-addresses are used in a given system. A BM can monitor these and generate an interrupt if a cyber intrusion tries to leverage them for communication. The interrupt counter can be used to track messages and the BM message counter can be used for total traffic count.

Signal Generator

The Signal Generator is an industry-first unique feature that provides precise control over the 1553 hardware transceiver output. It is a waveform generator that bypasses the standard 1553 encoder and allows words to be constructed at a bit-level that is 50 times the resolution of a normal 1553 signal. This can be used to create signal distortion, malformed message words and timing violations, which are key for creating fuzzing tests. Triggering events can be used to strategically activate the signal generator (between a BC command and RT response, for example).



AltaRTVal

AltaRTVal implements the protocol tests for both the SAE AS4111 RT Validation Test Plan and the SAE AS4112 RT Production Test Plan to simplify RT design and production validation. Some fielded systems containing 1553 Remote Terminals have never gone through this formal design verification testing. This potentially leaves these systems open to security threats. Most RT systems are old and use integrated circuits that were presumably validated. However, there are application-specific features that can affect compliance and introduce vulnerabilities. RT Validation can expose these deficiencies.

AltaRTVal software runs on Alta hardware to generate the protocol tests and provides a comprehensive automated test report.

Conclusion

The aerospace and defense industry can get the most out of their cybersecurity RDT&E efforts by leveraging the capabilities of ***AltaView, AltaAPI, AltaCore,*** and ***AltaRTVal.*** Alta's software suite provides unparalleled features for cybersecurity analysis. Alta is dedicated to providing the best possible avionics products, support and service.