SITAL
TECHNOLOGY

# Cyber Attack Emulation for MultiComBox

# Table of Contents

## Contents

## The Need

Cyber Resilience for avionic databus networks is a growing need, especially in military grade systems. An effort directed by the US DoD and in joint collaboration of the US NAVY, USAF and US ARMY has been progressing for several years to determine courses of action and the identification of appropriate cyber resilience technology to meet the cyber security changing landscape.

Advanced avionics databus such as AFDX has basic built in cyber resilience mechanisms but the majority of the avionics databuses today are MIL-STD-1553B/1760, ARINC 429 (and it's derivatives) and Fiber Channel. These older protocols are not designed to offer cyber resilience and may serve as a vesicle to deploy harmful cyber attacks, distort munitions accuracy and overall flight readiness.

## Technology Overview

Sital Technology's MultiComBox has been elevated to emulate various cyber-attacks for multi-drop bus protocols such as MIL-STD-1553B.

Development groups of aerospace products that would request to protect their products from cyber-attacks may use the cyber-attack emulation mode to purposefully attack their product and networks under development, to better understand their weaknesses and enhance their counter measures and cyber resilience playbooks.

In addition to the cyber attack emulation module, Sital Technology develops communication protocol engines for MIL-STD-1553B/1760 and related multi-drop busses with embedded cyber security capabilities.

For example:

The Secured 1553 is the world's first FPGA based IP core for MIL-STD-1553B with built in cyber security features and the GRIP 2.0-CS is the a stand alone USB to 1553 device with cyber/anomaly event monitoring and notifications.

The Secured 1553 and Grip 2.0-CS are out of scope for this document.

This document describes the supported attack types and how to program the MultiComBox to engage.

MultiComBox can be configured to work in Cyber-attack mode by means of setting up configuration register 2 (address 48) bits 11..8. These bits provide setting up to 15 different attacks. 0 is the default which defines no attack.

## Supported Attacks

Currently the MultiComBox supports BC related attacks and offers new attack features via firmware updates (issued 2-3 times a year for licensed members).

The existing controls of the BC mode remain and can be used to characterize the attack. Some controls, such as frame length are used differently from the way they are used in the BC programming.

## Attack type 1: Time/Periodic Triggered

The Time/Periodic type of attack follows these steps:

1. Wait for predefined period of time.
2. Wait for bus idle on both bus A and B.
3. Transmit all frame messages to the bus based on the frame rate parameters.

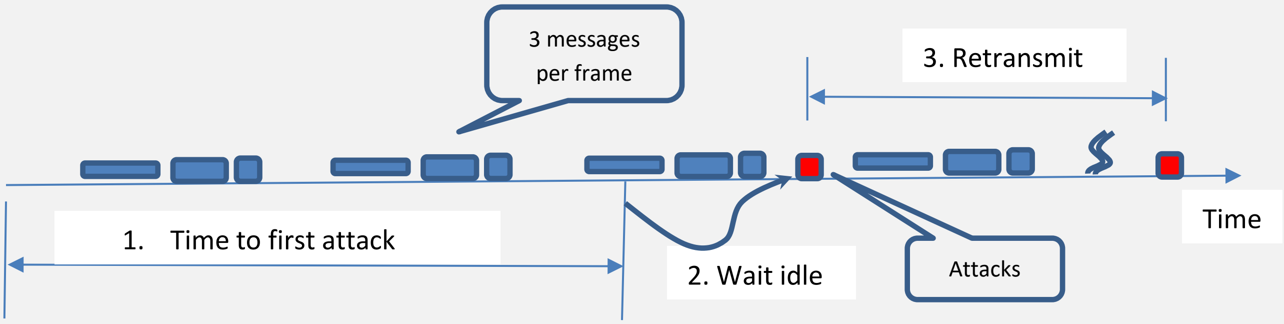
The time triggered attack allows the attacker to delay an attack, and then be persistent with it.

Resources: the frame length counter is used for the delay. 16 bits, two resolutions, one with LSB=65 milliseconds second with LSB=100 us. Maximum delay for LSB=65 ms is 65ms X 64K => 4295 seconds which are 71 minutes => 1 hour and 10 minutes.

Rate of attack: Message gap counter of all messages in the frame. This is typically 16 bits gap of micro seconds, up to a total of 65 ms.

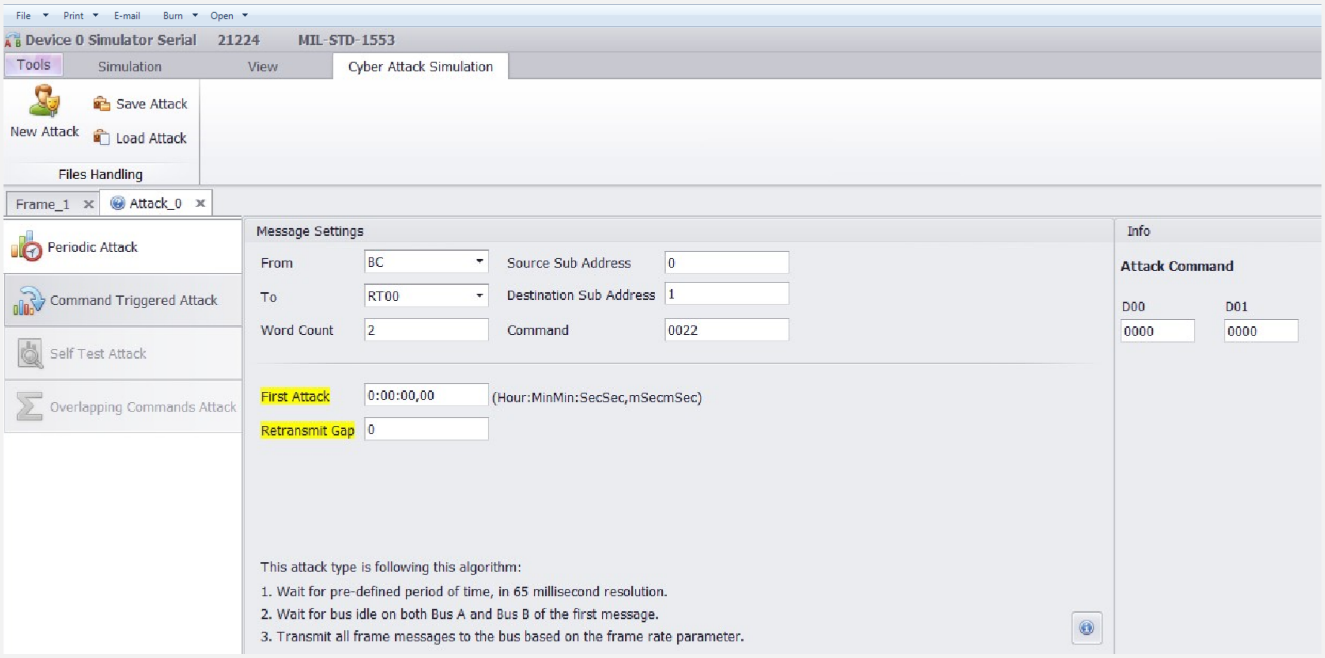
Example attack: Wait for 10 minutes, and then transmit broadcast reset time tag every 65 milliseconds.

In this case there would be a frame with one message with message gap time set to 0xFFFF, and frame length counter set to 10x60x(1000/65) = 9230.



*Time/Periodic Triggered Attack*

Set attack type to 1 to enable this type of attack.



Device 0 Simulator Serial 21224 MIL-STD-1553

| | | | |
|---|---|---|---|
| From | BC | Source Sub Address | 0 |
| To | RT00 | Destination Sub Address | 1 |
| Word Count | 2 | Command | 0022 |

First Attack 0:00:00,00 (Hour:MinMin:SecSec,mSecmSec)

Retransmit Gap 0

Attack Command

| D00 | D01 |
|---|---|
| 0000 | 0000 |

This attack type is following this algorithm:

1. Wait for pre-defined period of time, in 65 millisecond resolution.
2. Wait for bus idle on both Bus A and Bus B of the first message.
3. Transmit all frame messages to the bus based on the frame rate parameter.

*MultiComBox Periodic Attack Window*

# Attack type 2: Command Triggered

The command trigged attack follows these steps:

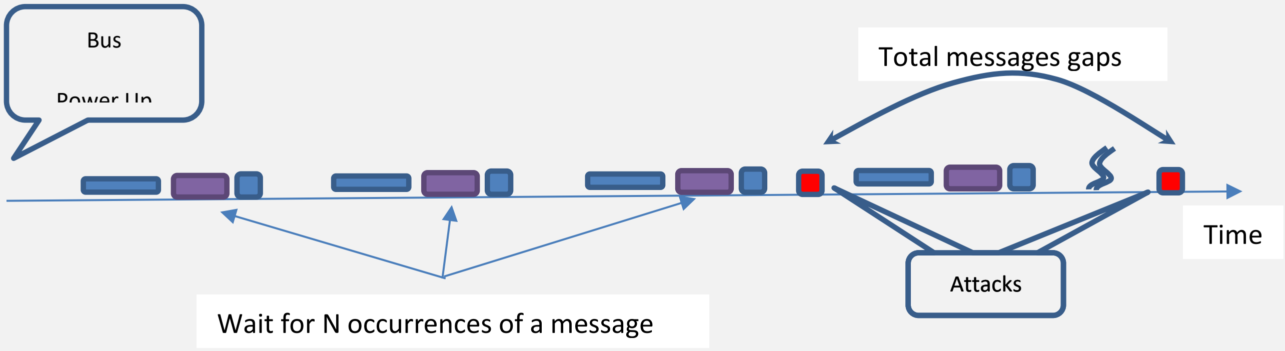
1. Wait for BC to transmit a defined command for N times.
2. Wait for destination buses idle, and transmit frame (without frame delay).

This attack allows the attacker to wait for a particular event on the 1553 bus in the form of a specific message, count N such occurrences, and then transmit the preplanned frame to the bus.

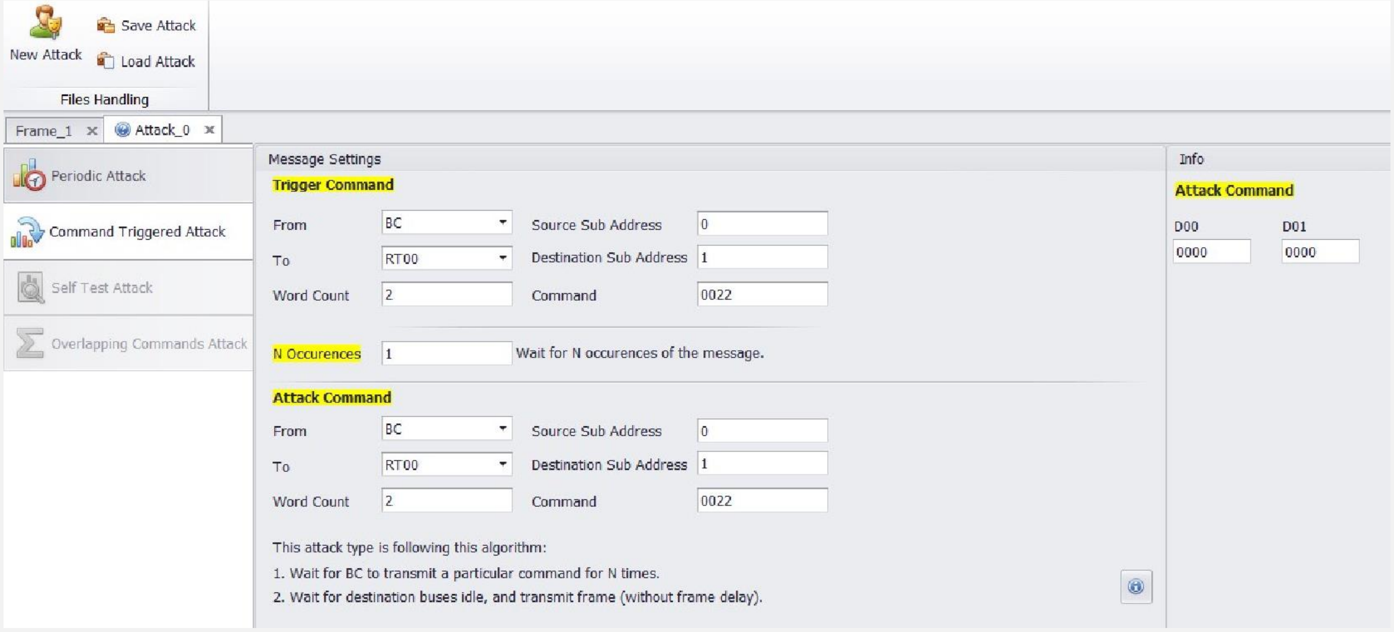
Resources: the frame length counter is used for N. N can be in the range of 0 to 64K. 0 would transmit without delay, 1 would indicate right after first occurrence of trigger message, 2 would wait for 2 such occurrences…

The Sync pattern register (0x46) defines the triggering command.

The attacker chooses to wait for an event such as a particular station (RT) becoming armed and replying to the bus. When that event happens, the attack includes transmitting predefined messages to that particular RT, to damage its operation.



*Command Triggered Attack*



**Trigger Command**

From: BC
Source Sub Address: 0
To: RT00
Destination Sub Address: 1
Word Count: 2
Command: 0022

N Occurences: 1 Wait for N occurences of the message.

**Attack Command**

From: BC
Source Sub Address: 0
To: RT00
Destination Sub Address: 1
Word Count: 2
Command: 0022

This attack type is following this algorithm:

1. Wait for BC to transmit a particular command for N times.
2. Wait for destination buses idle, and transmit frame (without frame delay).

Info – **Attack Command**

| D00 | D01 |
|---|---|
| 0000 | 0000 |

*MultiComBox Command Attack Window*