

PhysiMUX IPS

Intrusion Detection System & Intrusion Prevention System

User Guide

Rev 1.0

Mar 2022



Copyright (C) 2022 by Sital Technology Ltd.

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Sital Technology Ltd.

Table of Contents

1	Introduction	4
1.1	Scope	6
1.2	Audience	6
1.3	Reference.....	6
1.4	Support	6
2	Concept & High Level Workflow	7
3	IPS Application	8
3.1	ISP main window	8
3.2	Event log window	9
3.3	IPS Debug window	10

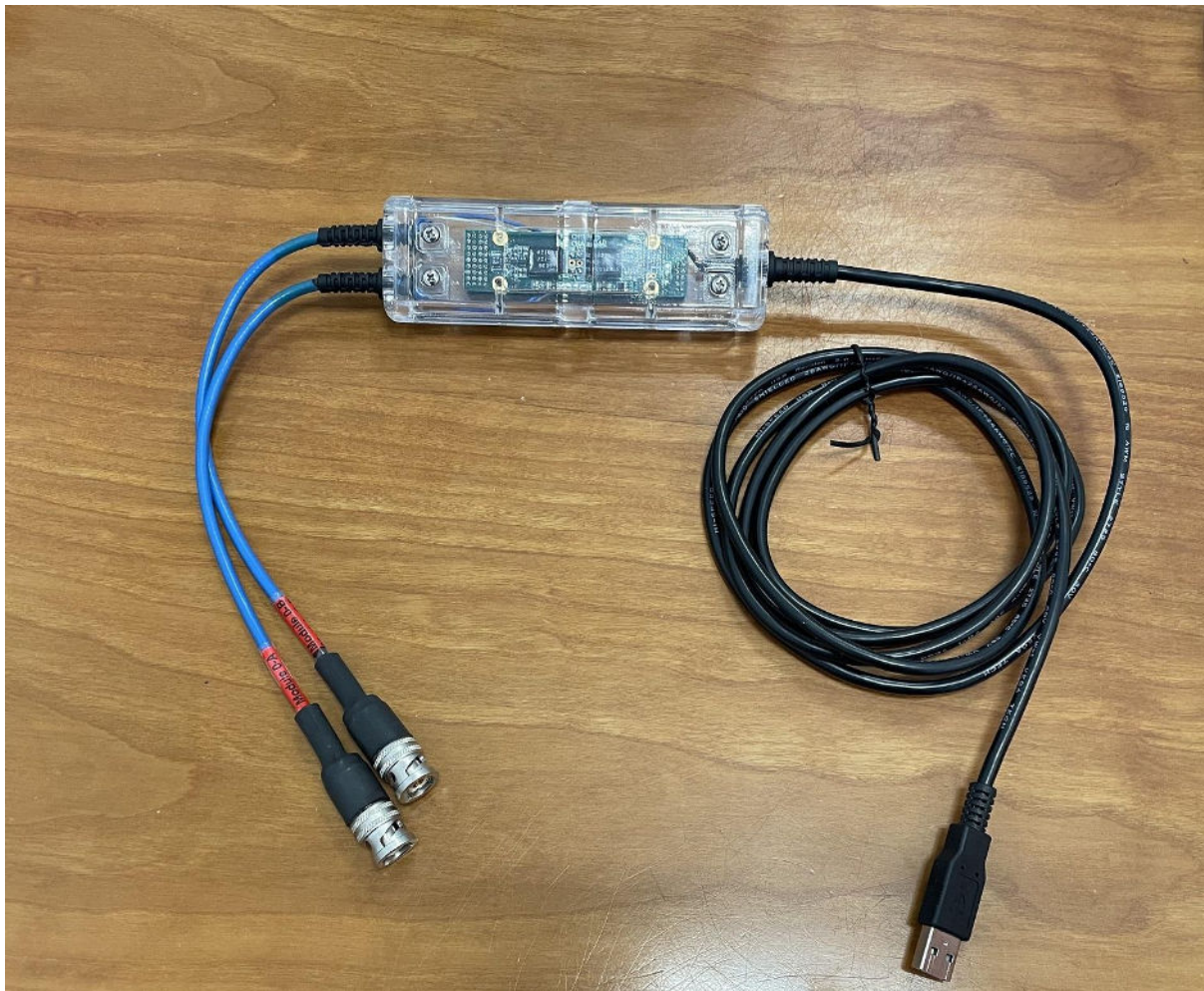
1 Introduction

The PhysiMUX IPS (Intrusion Prevention System) device connects to a dual redundant MIL-STD-1553 bus and to a Windows host computer through a USB connection.

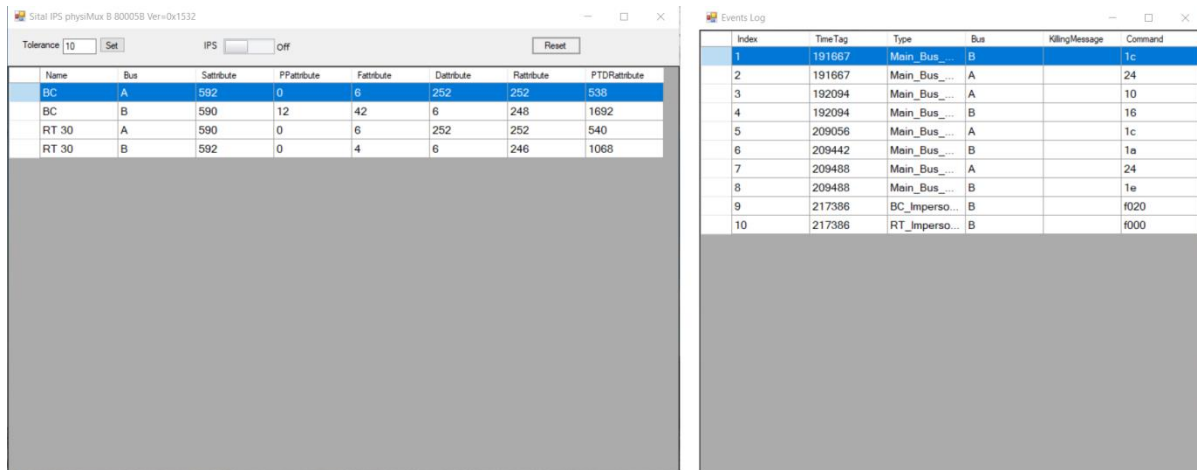
This device constantly monitors the 1553 bus and its data to detect anomalous data and optionally protect the 1553 BC, RT or Monitor terminal against such data.

Anomalous data can be the result of either “spoofing” (impersonation) of a Bus Controller (BC) or Remote Terminal (RT), a denial-of-service attack (DoS), or wiring faults such as open and short circuits or disconnections.

In addition to the detection of anomalous data, PhysiMUX IPS can invalidate messages resulting from impersonation attacks and thereby prevent the damage an attacker is attempting to do.



Sital's IPS (Intrusion Prevention System) Windows PC uses the PhysiCAN's USB 2.0 link to monitor and display the information gathered by the PhysiMUX IPS and present the fingerprinting information (on the left) and the event logger (on the right) with the following image:



The screenshot displays two windows from the Sital IPS software. The left window, titled 'Sital IPS physiMUX B 80005B Ver=0x1532', shows a table of fingerprinting information. The right window, titled 'Events Log', shows a table of system events.

Name	Bus	Sattribute	PPattribute	Fattribute	Dattribute	Rattribute	PTDAttribute
BC	A	592	0	6	252	252	538
BC	B	590	12	42	6	248	1692
RT 30	A	590	0	6	252	252	540
RT 30	B	592	0	4	6	246	1068

Index	TimeTag	Type	Bus	KillingMessage	Command
1	191667	Main_Bus_...	B		1c
2	191667	Main_Bus_...	A		24
3	192094	Main_Bus_...	A		10
4	192094	Main_Bus_...	B		16
5	209056	Main_Bus_...	A		1c
6	209442	Main_Bus_...	B		1a
7	209488	Main_Bus_...	A		24
8	209488	Main_Bus_...	B		1e
9	217386	BC_imperso...	B		1020
10	217386	RT_imperso...	B		1000

2 Scope

The scope of this document is the description of and operating instructions for the application program running on a Windows PC that communicates with the PhysiMUX IPS device through its USB connection.

2.1 Audience

The principle audience for this document is engineers with requirements for MIL-STD-1553 bus cyber-security solutions.

2.2 Reference

The PhysiMUX IPS software was developed based on “SnS1553 HSID V4 IPS.pdf” – This document describes the Hardware/Software Interface document of the PhysiMUX IPs hardware.

2.3 Support

If you have any question or require further assistance, use any of the following methods to contact Sital customer support:

- By Email: support@sitaltech.com
- By Phone: +972-9-7633300
- By Fax: +972-9-7663394

3 Concept & High-Level Workflow

The PhysiMUX IPS (Intrusion Prevention System) device connects to High-Level a dual redundant MIL-STD-1553 bus and to a Windows host computer through a USB connection. Please do not connect through a USB hub. Instead, always connect the PhysiCAN device directly to a PC or laptop port.

An FTDI driver should be installed on the PC or laptop computer. This is provided with the installation).

Sital's IPS application program communicates with the PhysiMUX IPS device through the FTDI USB driver.

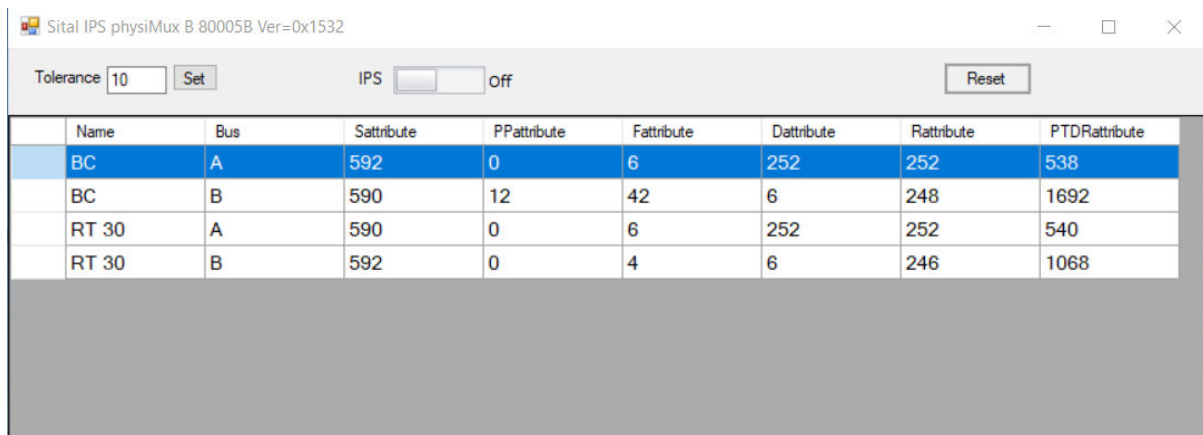
4 IPS Application

Unzip the software package to any directory. The files in the software package folder include some GUI DLL files, Sital_USB.dll and IPS.EXE as well as this document.

Start the application by running IPS.exe

If the device is not connected or the communication between the device and the Application is disconnected, an error message will appear in the window.

4.1 ISP main window

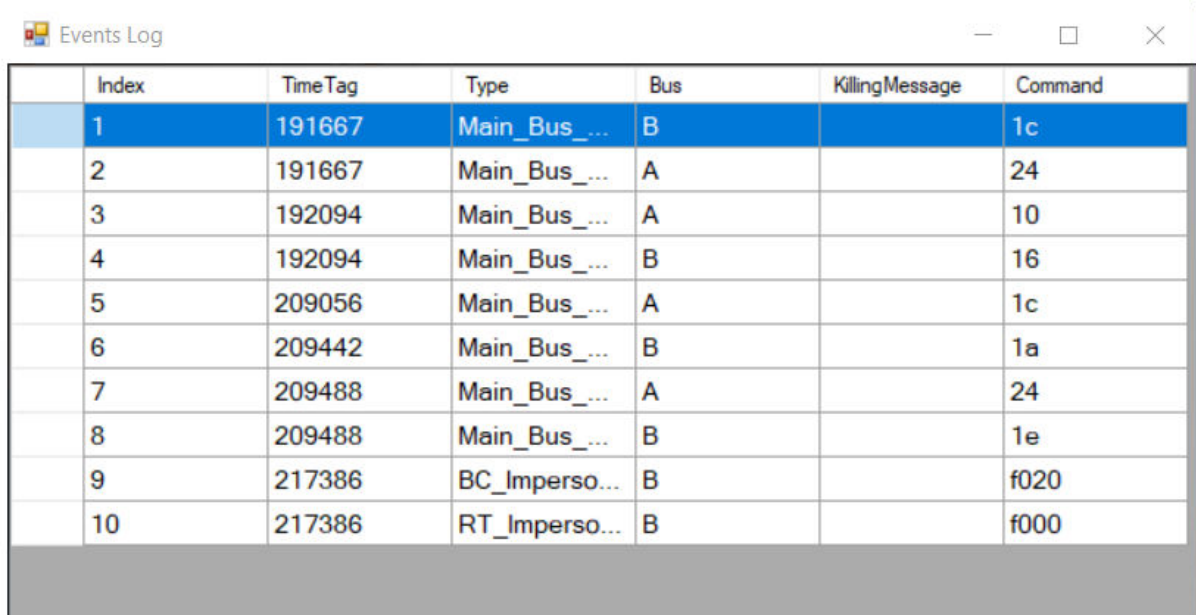


Name	Bus	Sattribute	PPattribute	Fattribute	Dattribute	Rattribute	PTDRattribute
BC	A	592	0	6	252	252	538
BC	B	590	12	42	6	248	1692
RT 30	A	590	0	6	252	252	540
RT 30	B	592	0	4	6	246	1068

- The Windows Title shows the version number of the device.
- The Table shows the parameters (attributes) for each terminal on the bus. The parameters include the S attribute, PP attribute, F attribute, D attribute, R attribute and pTDR attribute. Each attribute is a unique characteristic for each terminal on the bus. The IPS determines the attribute data by monitoring and averaging data collected during the approximate 4-second learning period following power-up. Thereafter, it maintains and occasionally updates the attribute (parameter) values. These values are used occasionally to determine if a violation has occurred. The table can be sorted by name or bus. This is done by clicking on the column title.
- Tolerance – Following the learning period, the attribute values for all received messages are compared against the set of stored attribute values for the respective BC or RT. For each received message, if the difference between the received and expected value(s) of one or more attributes exceeds the tolerance value limit, the IPS will determine that the message is anomalous.
- Reset button – resets the device and clears its memory. In addition, the table and Log events table will be cleared.
- IPS ON/OFF button – when the IPS is running (ON), it will invalidate messages that are determined as being anomalous.

- The data of this table is saved to a log file in .csv format. The file is located in the running folder under Logs directory. It is saved every 5 minutes.

4.2 Event log window



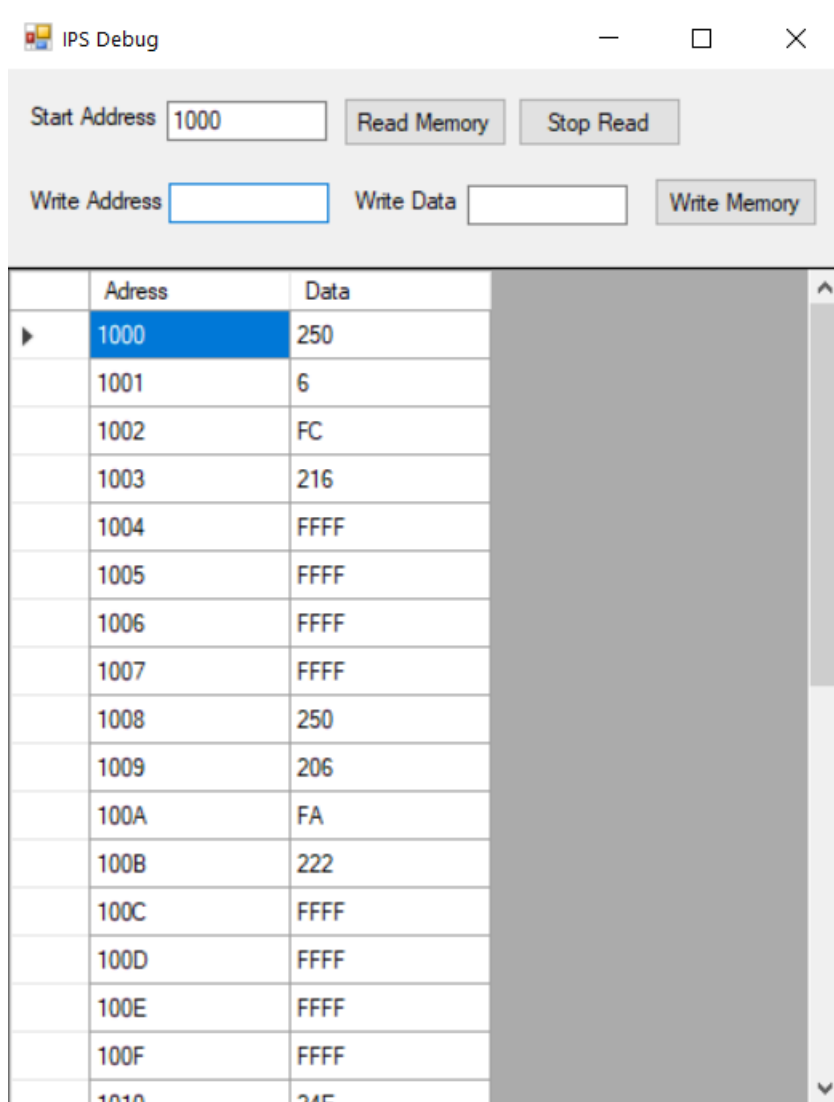
Index	Time Tag	Type	Bus	KillingMessage	Command
1	191667	Main_Bus_...	B		1c
2	191667	Main_Bus_...	A		24
3	192094	Main_Bus_...	A		10
4	192094	Main_Bus_...	B		16
5	209056	Main_Bus_...	A		1c
6	209442	Main_Bus_...	B		1a
7	209488	Main_Bus_...	A		24
8	209488	Main_Bus_...	B		1e
9	217386	BC_Imperso...	B		f020
10	217386	RT_Imperso...	B		f000

This window shows the events that were detected by the PhysiMUX IPS device.

The table can be sorted by clicking on the column title (double click to return to default).

- Time Tag (device time) of detection – number of microseconds since reset or power-up.
- The type of event : BC_Impersonation, RT_Impersonation, Bus_DoS, RT_DoS, Main_Bus_Wiring_Disconnection_Error, Main_Bus_Wiring_Short_Error, Stub_Short_Error.
- Bus – Identifies the bus the message was sent over.
- KillingMessage – If PhysiMUX IPS invalidated this message, a “V” will appear.
- Command – Identified the command where this event (anomaly) was detected. The format is 16-bit hex representation of the 1553 Command or Status word.
- The Events are saved in a Log file in csv format. The file is located in the running folder under Logs directory.

4.3 IPS Debug window



Start this window by pressing Ctrl+Shift+D on the keyboard when the focus is on main window.

This window shows the content of the device memory.

- Start Address – The Address in hex from which to start reading.
- Read Memory button – Start reading the memory continuously (every 500 milliseconds). For each such instance of this operation, 32 bytes are read.
- Stop Read button – Stop the reading thread. The displayed data will remain.
- Write Address – The address in hex to which we want to write data.
- Write Data – The data in hex to be written.
- Write Memory button – Initiates the memory write command.