Avionic Databus Cyber Protection

- **Real-time detection of UN-AUTHORIZED TRANSMITTING SOURCES**
- **Cyber protection against Message Spoofing and DDOS for mission critical avionic systems**

Available for Evaluation

- Real-time detection of message spoofing
- Protect the entire network from a single location
- Support after-production modifications
- Fully Upgradable
- SPI Interface to CPU
- C level API

Real-Time
Detection (IDS) and Prevention (IPS)

Scalability
Context/Data layer independent

Deployment
FPGA IP , I/O card

Supported Networks:

- MIL-STD-1553
- ARINC429
- ARINC825
- CAN
- CAN-FD

Sital Technology Ltd.

Tel: +972-9-7633300

Fax: +972-9-7663394

Email: info@sitaltech.com

Web: www.sitaltech.com

Sital's FPS for Avionic Databus Protection

The Problem
Aircraft internal communication databuses are exposed for message spoofing and DDOS attacks

Legacy protocols for avionic control messages are highly optimized and lack basic capabilities for source message authentication. As a result, all mission critical avionic databuses are exposed to a verity of spoofing and DDOS attacks which **impact flight safety, navigation and weapon utilization and may result in aborted missions, aircraft flight route alterations and life threating events**

The Solution

Sital's FPS (**Finger Printing Sensor**) technology alerts and prevents against various spoofing and DDOS attacks on mission critical avionic data buses.

Implemented as FPGA IP, the Sital FPS passively monitors the communication buses in an aircraft and provides **real-time** detection of message spoofing and DDOS attacks. In addition, the FPS also **prevents** such attacks from propagating between avionic systems and **mitigates** the risk of mission failure due to cyber attacks

Key Benefits:

- **Seamless Integration – FPGA IP**
- **Support After Market Installations and Modifications**
- **Validated and tested**
- **DO-254 compatible**
- **Support the entire databus with a single installment**
- **Context and data layer independent**
- **Support all major control type databus communications**

Public Cyber Attacks

AIR, INTEL & CYBER
Wireless Hacking In Flight: Air Force Demos Cyber EC-130
By SYDNEY J. FREEDBERG JR
on September 15, 2015 at 3:12 PM

Chris Roberts
@Sidragon1

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)
11:08 PM - 15 Apr 2015
200   239

SITAL Technology