ISOT Mil-STD-1553 Dataset

The dataset is a combination of datasets collected in a simulated environment consisting of normal activities and a series of attacks against the MIL-STD-1553 databus.

The simulation was conducted using Abaco R15-USB-2M USB interface box and Abaco BUSTOOLS/1553 GUI Software for MIL-STD-1553 bus analysis, simulation, and data logging.

Figure 1 depicts the simulated bus components. The bus architecture used in the simulation consists of a bus monitor (BM) and five different avionic systems, including a flight control computer (FCC) as RT3, a mission computer (MC) as BC, an inertial reference unit (IRU) as RT1, a mission control keyboard (MCK) as RT4, and a multi-function display unit (MFD) as RT2. The MC serves as bus controller (BC), while the remaining components are remote terminals.

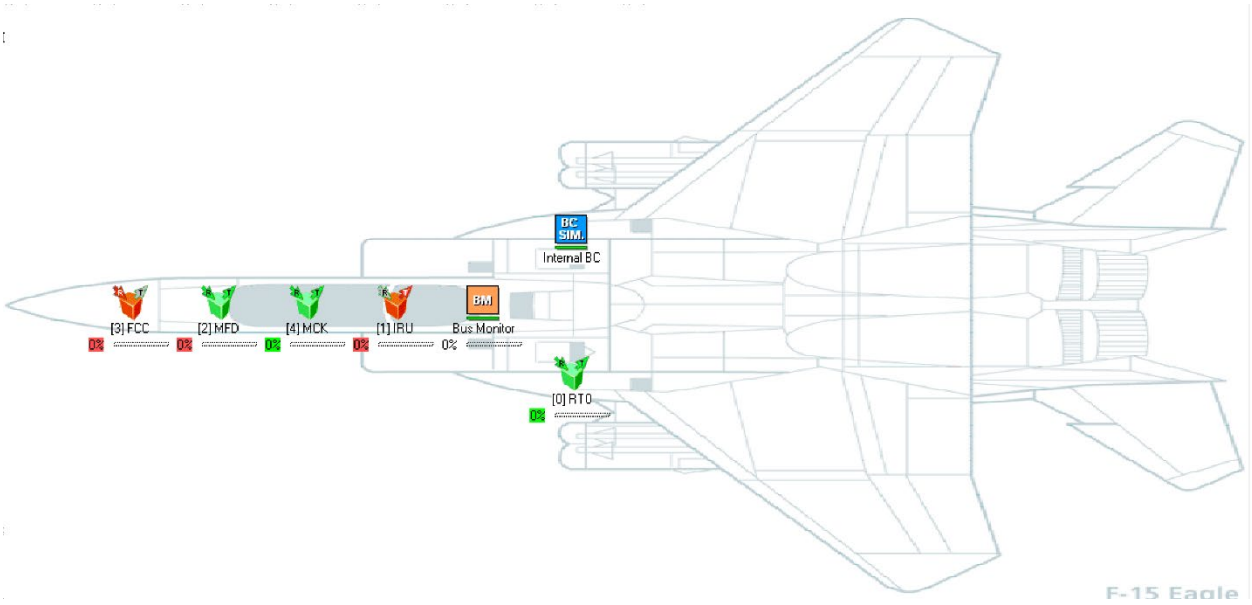

Figure 1. Simulated MIL-STD-1553 bus components

The components were the only ones used to execute the normal activities. To simulate the attack, we added a rogue terminal as RT0.

A baseline dataset consisting of normal activities was generated by running the simulation for 10 min. Subsequently, 6 different attack scenarios were run separately against the baseline architecture, by introducing RT0 as rogue terminal. Table 1 provides a summary of the different datasets and Table 2 shows the different fields involved in the raw data. The dataset is provided as separate CSV files.

Table 1. Outline of the collected MIL-STD-1553 datasets

Dataset #	Type of data	Attack type	Attack description	Number of messages	Simulation length
1	Normal	N/A	N/A	23,000	10 min
2	Mix normal/malicious	Targeted/Basic DOS (Attack 1)	rogue terminal (RT0) targets the FCC (RT3) by sending random words in a loop	148	30 sec
3	Mix Normal/malicious	Multi-target DOS (Attack 2)	Rogue terminal (RT0) sends broadcast messages in a loop	373	30 sec
4	Mix Normal/malicious	Subtle Fake data injection (Attack 3)	rogue terminal (RT0) replicates one of the messages sent by one of the legitimate RTs by slightly altering one of the data items	970	30 sec
5	Mix Normal/malicious	Noisy fake data injection (Attack 4)	similar to the above attack, except that in this case fake data is randomly generated.	970	30 sec
6	Mix Normal/malicious	Logic attack (Attack 5)	a rogue RT broadcast mode code value 4 (0x04), which corresponds to Transmitter Shutdown, and which is unusual	981	30 sec
7	Mix Normal/malicious	Hybrid Logic/fake data injection (Attack 6)	Combination of the attacks in datasets 5 and 6	1004	30 sec

Table 2. Raw dataset format

Fields	Description
msgID	Sequence number associated with the message by the simulator
timestamp	Message timestamp in seconds
error	Indicate whether the error bit of the status word related to the message is set; contains TRUE/FALSE accordingly.
modeCode	Indicate whether the message is a mode command message; contains TRUE/FALSE accordingly.
channel	Channel associated with the message
connType	Communication type
sa	Address of sending RT
ssa	Sub-address of the sending subsystem from the sending RT
da	Address of receiving RT
dsa	Sub-address of the receiving subsystem at the receiving RT
wc	Word count: number of data words included in the message
modeCode value	Mode code value when applicable
txRsp	Transmit command response time in μs
txSts	Transmit status word
rxRsp	Receive command response time in μs
rxSts	Receive status word
dw0 … dw31	Values of the data word included in the message ranging from dw0 to dw31; N/A is used when there is no data words for a field.

Malicious	Indication of whether the message is malicious: contains TRUE/FALSE accordingly.
injected	Indication of whether part of the data included in the message is injected: contains TRUE/FALSE accordingly.
gap	Inter-message gap time in μs
msgTime	Message time in μs

To cite this dataset use:

Hadeer Saad, Issa Traore, Paulo Quinan, Karim Ganame, Oussama Boudar, “A Collection of Datasets for Intrusion Detection in MIL-STD-1553 Platforms”, in Artificial Intelligencefor Cyber-Physical Systems Hardening, I. Traoré, I. Woungang, and S. Saad, Eds. Springer, 2022, Chapter 4.