

# The Center for Cyber Defenders

Expanding computer security knowledge



## Conan: Emulytics on the 1553 Protocol

Dalton Cole, Missouri University of Science and Technology;  
Michael Reeves, Purdue University

Project Mentor: Chris Jenkins, Org. 5827



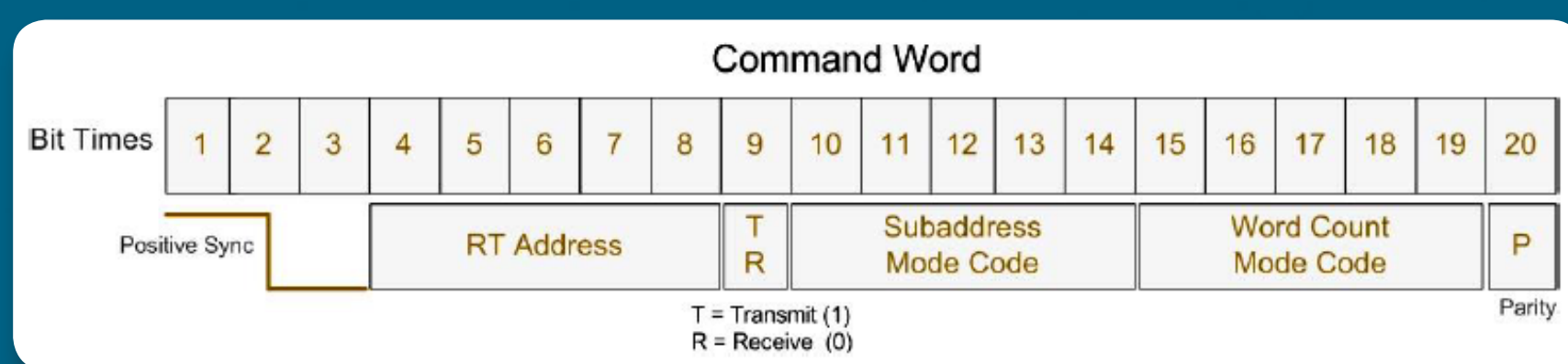
### Problem Statement

- Adversaries have shown the ability to attack and disrupt cyber-physical systems through cyber-attacks
- No mature technologies exist to detect cyber attacks within 1553 data bus systems on aviation aircraft

### Objectives

- Develop an emulytics environment to aid in the detection of vulnerabilities on a 1553 bus
- Take a multi-stage approach where we gradually add complexity to the emulated environment
- Capture and dissect network traffic to increase fidelity of emulation
- Be able to connect real 1553 hardware and have it interact with our emulated environment

Command Word Block Structure<sup>[1]</sup>



### Approach

- Review literature on the 1553 Military Standard
- Write a simple program using the Excalibur 1553UNET API to create phase 1 prototype scenario
- Analyze 1553 protocol structure using packet captures within Wireshark
- Write a dissector for Wireshark to better analyze packet captures
- Write a program to emulate 1553 traffic using ZMQ sockets
- Integrate emulated program in the SCEPTRE framework
- Gradually add complexity to emulated environment as time permits
- Apply analytics to emulated environment to find vulnerabilities

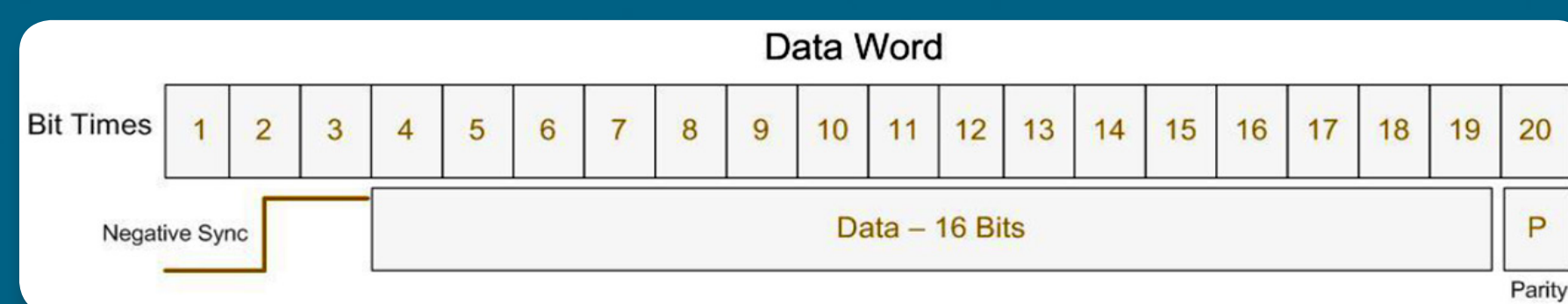
### References

- [1] Alta Data Technologies LLC. MIL-STD-1553 Tutorial and Reference. N.p.: n.p., n.d. [www.altadt.com](http://www.altadt.com). Alta Data Technologies LLC, 21 Sept. 2014.
- [2] [http://www.boeing.com/resources/boeingdotcom/defense/f-15\\_strike\\_eagle/images/f15\\_strike\\_eagle\\_hotspot\\_bg\\_960x410\\_mobile.png](http://www.boeing.com/resources/boeingdotcom/defense/f-15_strike_eagle/images/f15_strike_eagle_hotspot_bg_960x410_mobile.png)
- [3] "MIL-STD-1553." Wikipedia. Wikimedia Foundation, 24 June 2017. Web. 05 July 2017.

### Challenges

- Difficulty of acquiring data captures to improve model fidelity
- Integrating hardware into SCEPTRE and still meet latency on the order of microseconds

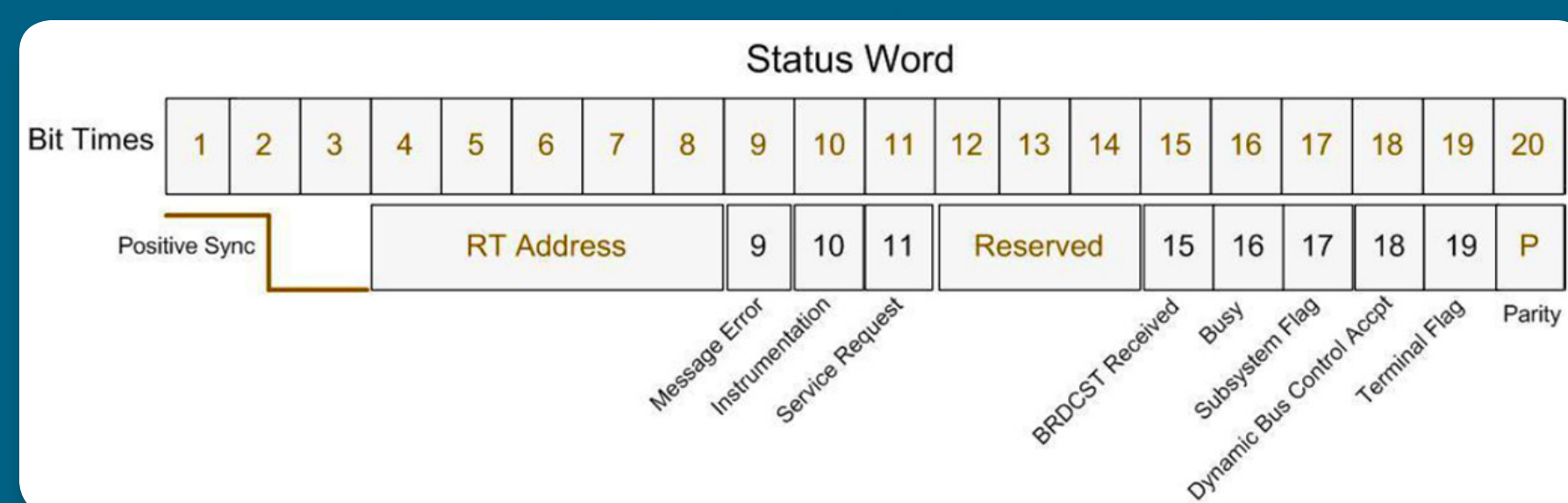
Data Word Block Structure<sup>[1]</sup>



### Components

- Bus Controller
  - Initiates all message communications
- Bus Monitor
  - Monitors and records bus transactions
- Remote Terminal
  - End application, such as motor controls and sensors

Status Word Block Structure<sup>[1]</sup>



### Impact and Benefits

- Improve cyber security posture of military aviation systems
- Emulate possible vulnerabilities
- Maintain avionic bus integrity and provide mission assurance for the DoD

Typical 1553 Architecture<sup>[3]</sup>

