COMM/NAV & MISSION SYS
REDBALL?
WHO YOU GONNA CALL?

Avionics Primer for ~~Hackers~~ Security Researchers

COMM/NAV & MISSION SYS
REDBALL?
WHO YOU GONNA CALL?

Nicholas Childs TSgt, USAF

B-1 Weapon Systems Controller

Bomber/Special Integrated
Communication/Navigation/Mission Systems Craftsman
OAS?

Twitter/Instagram @Boxswapper
Email boxswappers@gmail.com

Avionics Primer for ~~Hackers~~ Security Researchers

Why?

Things are broken, Avionics bus systems were designed for use not for security, Like most legacy systems, the addition of new technologies has introduced vulnerabilities.

I need your help..or

WE'RE ALL GONNA DIE!!!

Avionics Primer for ~~Hackers~~ Security Researchers

COMM/NAV & MISSION SYS

REDBALL?

WHO YOU GONNA CALL?

```
C:\Users\1256369778>whoami
- 18 years experience in communication navigation systems
- Aeronautical Engineering Degree
- Proficient with multiple airframes and avionics systems; C-17,C-5,C-
141,KC-135,B-1
- 5 years experience Active Directory Administrator on DoD network
- Multiple cybersecurity certifications (all expired) ☹
- FCC Radiotelephone Operator License with Radar Endorsement
```

Avionics Primer for ~~Hackers~~ Security Researchers

(Origin Story)What problems did the BUS solve?

Communication along BUS systems

A few networks you should know about

Attack vectors sorry no POC

Avionics Primer for ~~Hackers~~ Security Researchers

What problems does the C/N BUS solve?

The MIL-STD-1553

-1973 To help with weight reduction, simplicity, standardization, and flexibility.
-First used in the F-16 Fighter.

Avionics Primer for ~~Hackers~~ Security Researchers

What problems did the BUS solve?

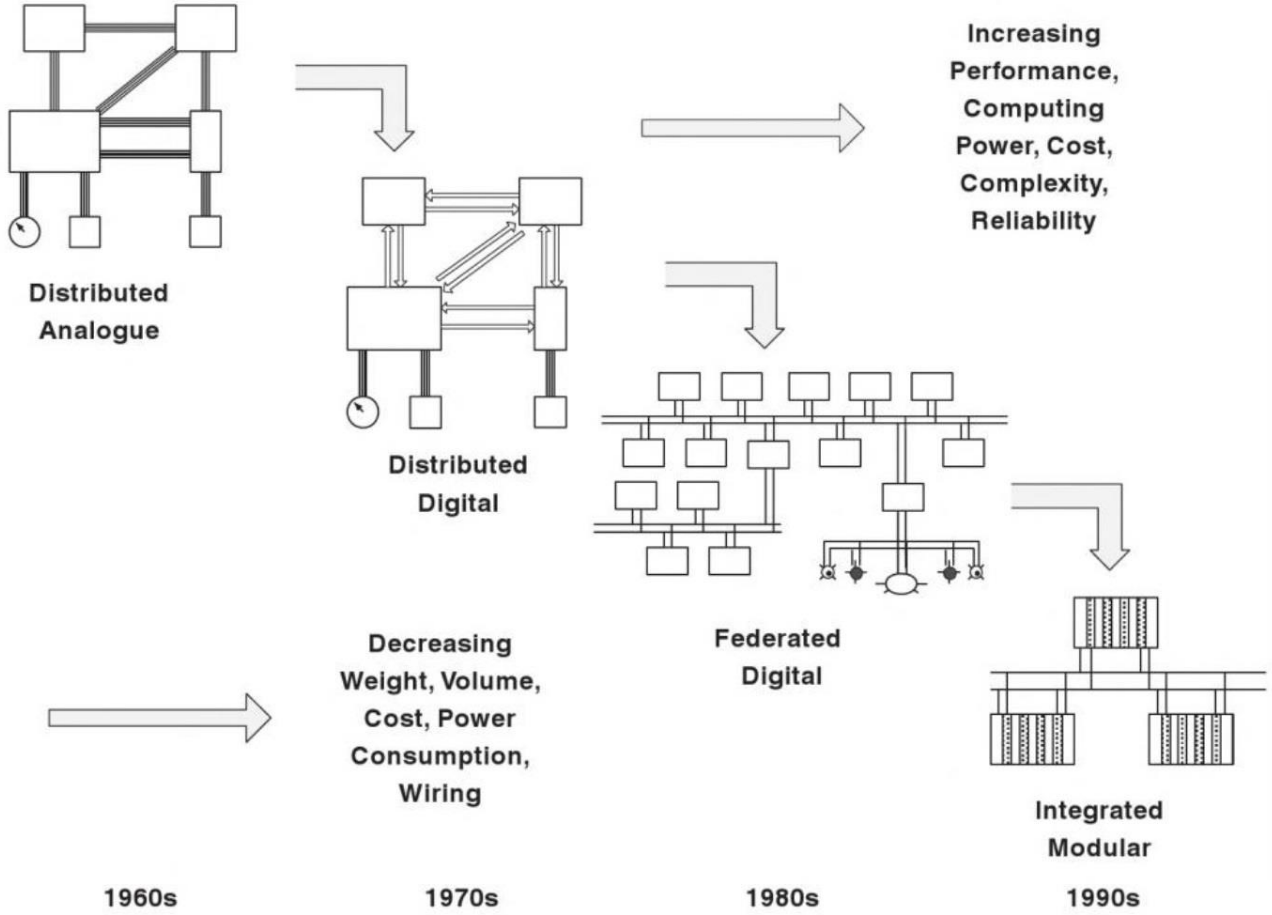
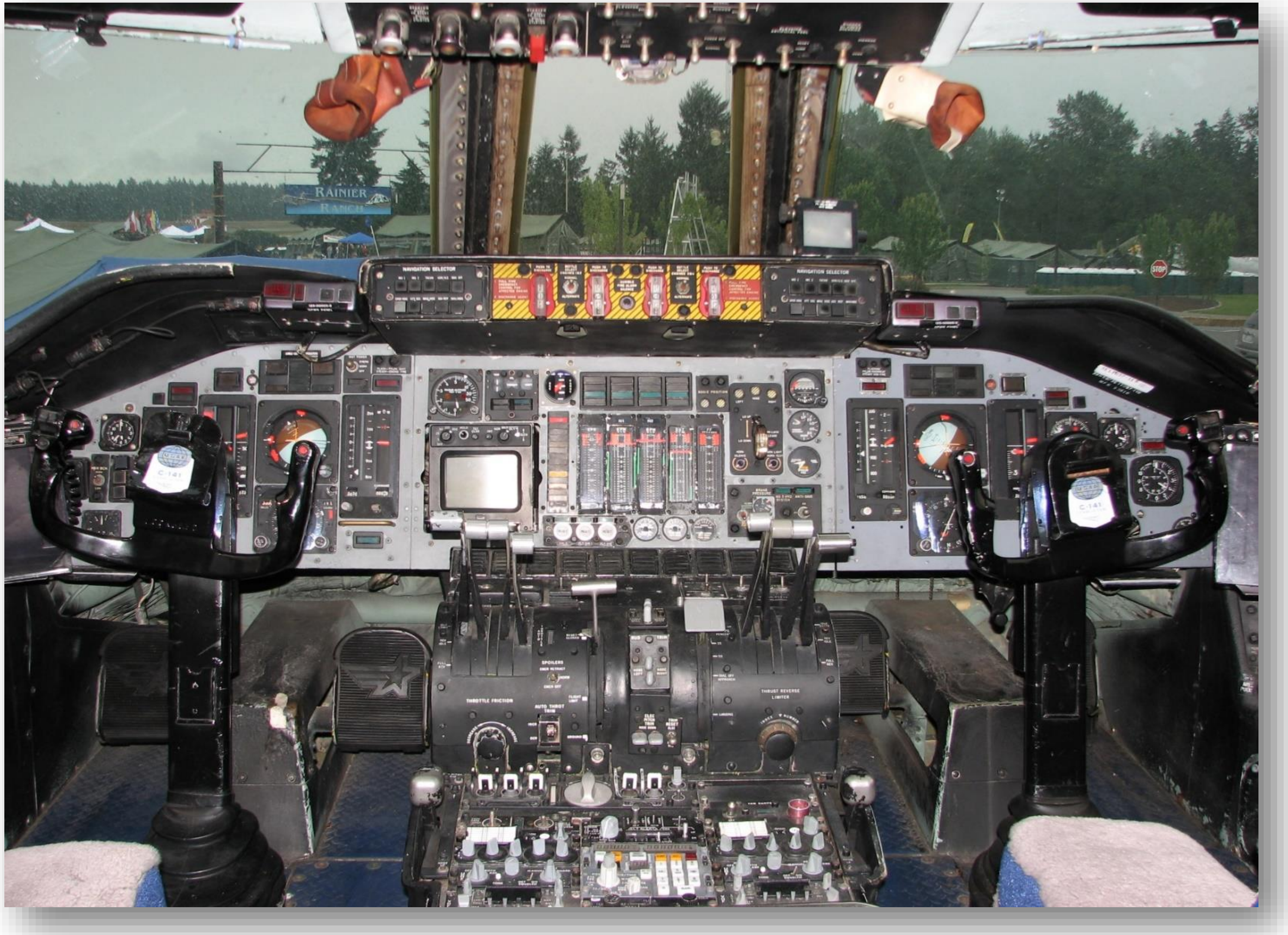


Figure 5.11 Evolution of avionics architectures.

Design and Development of Aircraft Systems Ref (a)

Avionics Primer for ~~Hackers~~ Security Researchers

Legacy Control and Navigation



C-141 Starlifter Cockpit
At Airshow McChord AFB

Avionics Primer for ~~Hackers~~ Security Researchers

Modern Control and Navigation

C-5M Super Galaxy Cockpit

Paris- LeBourget
©Jonathan Zaniger

Avionics Primer for ~~Hackers~~ Security Researchers

Commercial Aviation Bus system

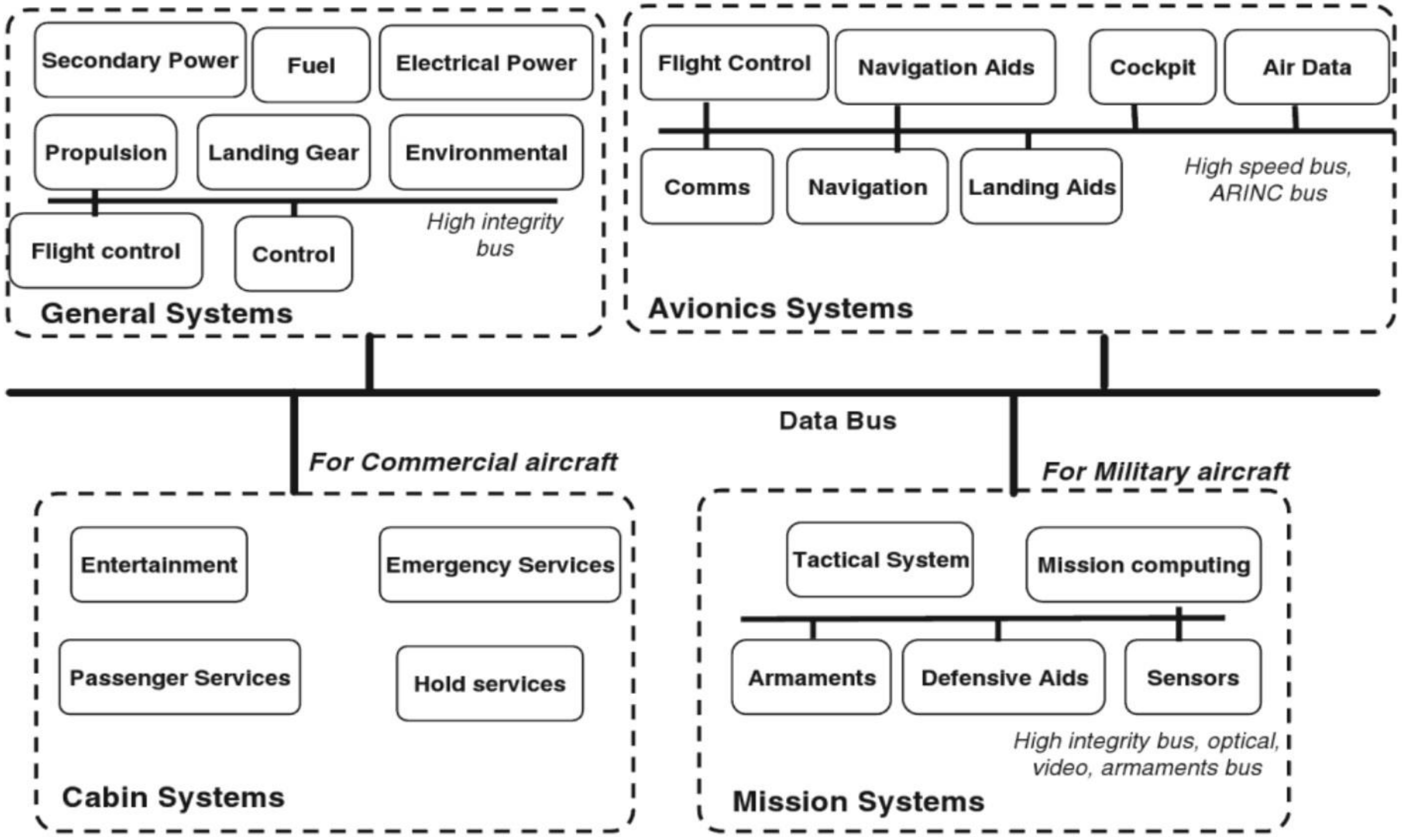


Figure 5.4 Aircraft systems.

Design and Development of Aircraft Systems Ref (a)

Avionics Primer for ~~Hackers~~ Security Researchers

Generic 1553 bus system

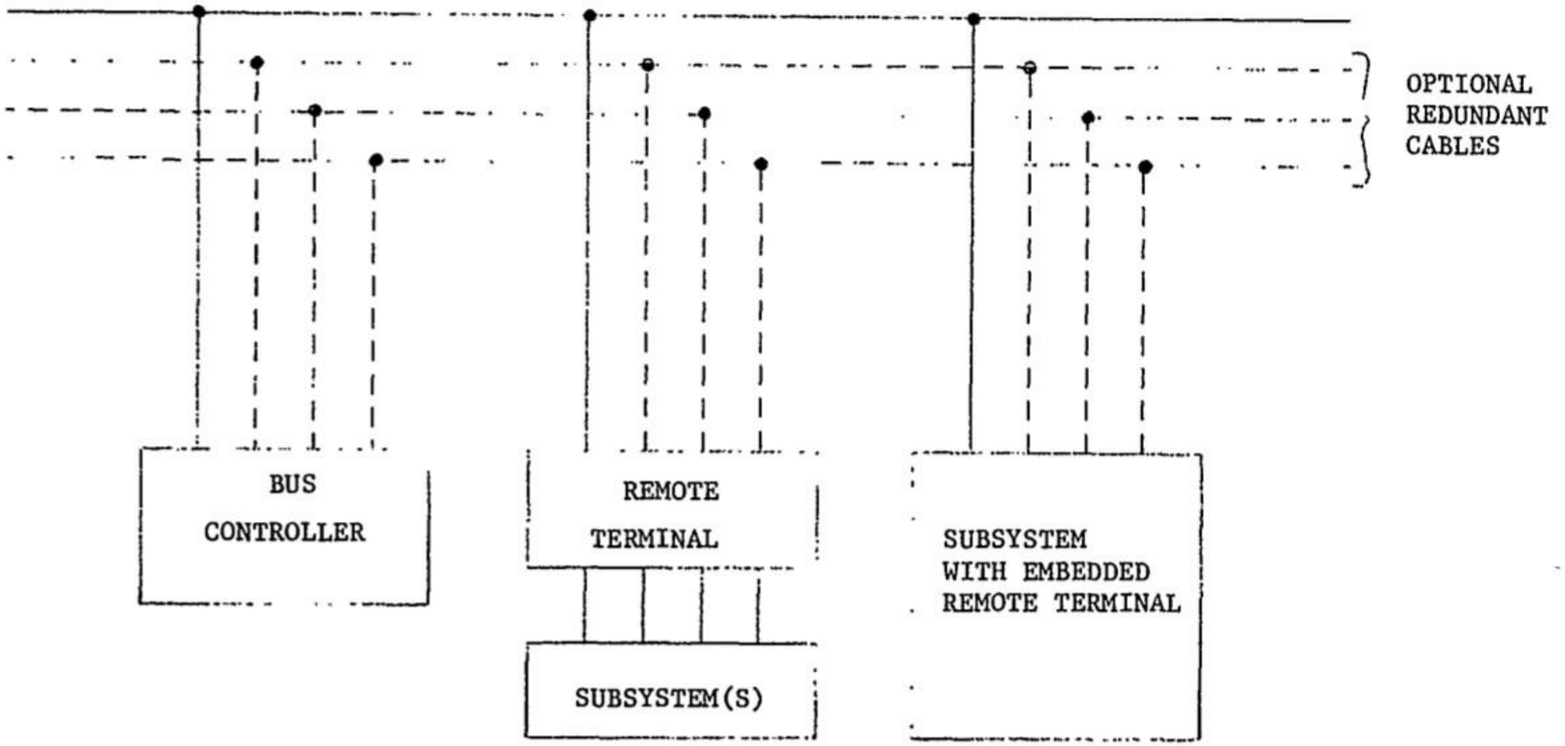
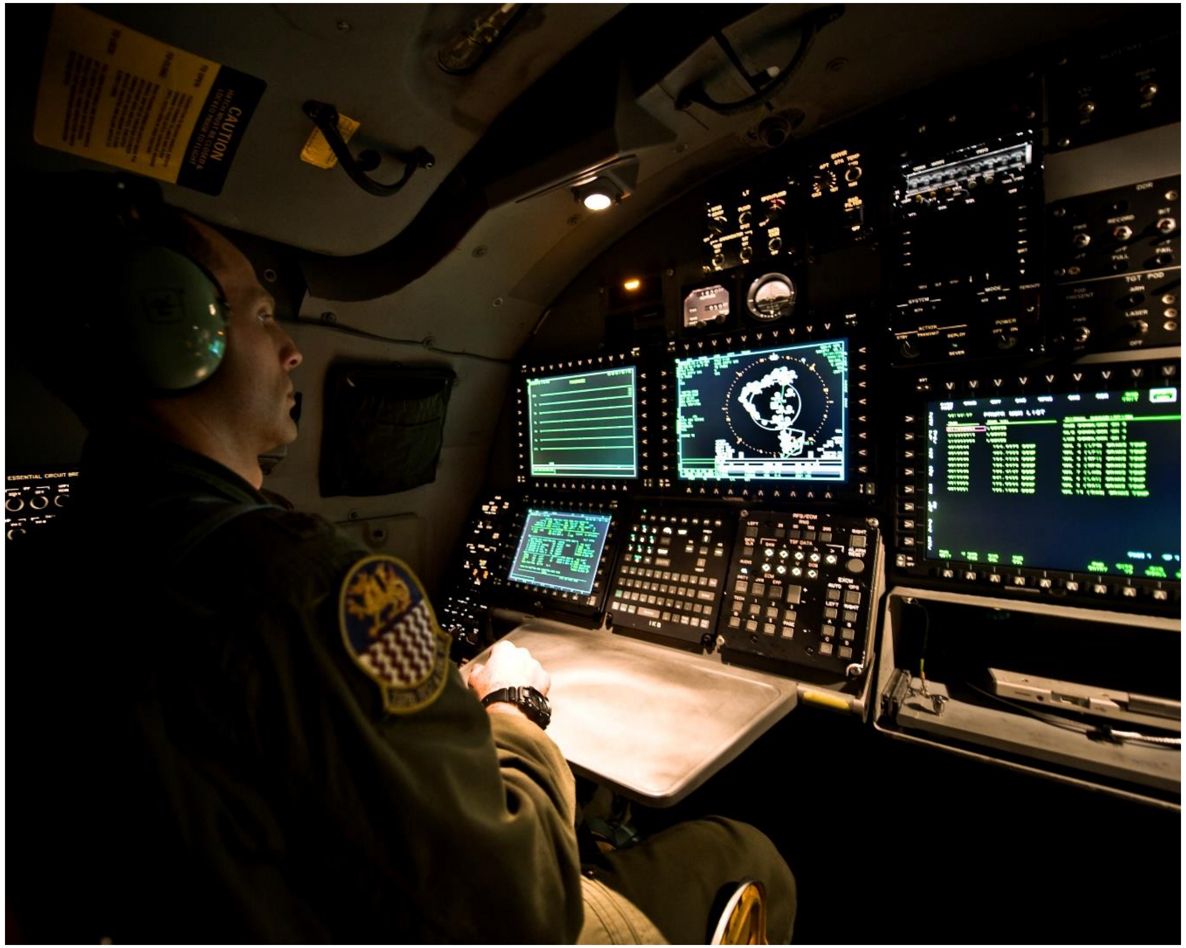

OPTIONAL REDUNDANT CABLES
BUS CONTROLLER
REMOTE TERMINAL
SUBSYSTEM(S)
SUBSYSTEM WITH EMBEDDED REMOTE TERMINAL

FIGURE 1. Sample multiplex data bus architecture.

MIL-STD-1553b Data bus Standard Ref(b)

Avionics Primer for ~~Hackers~~ Security Researchers

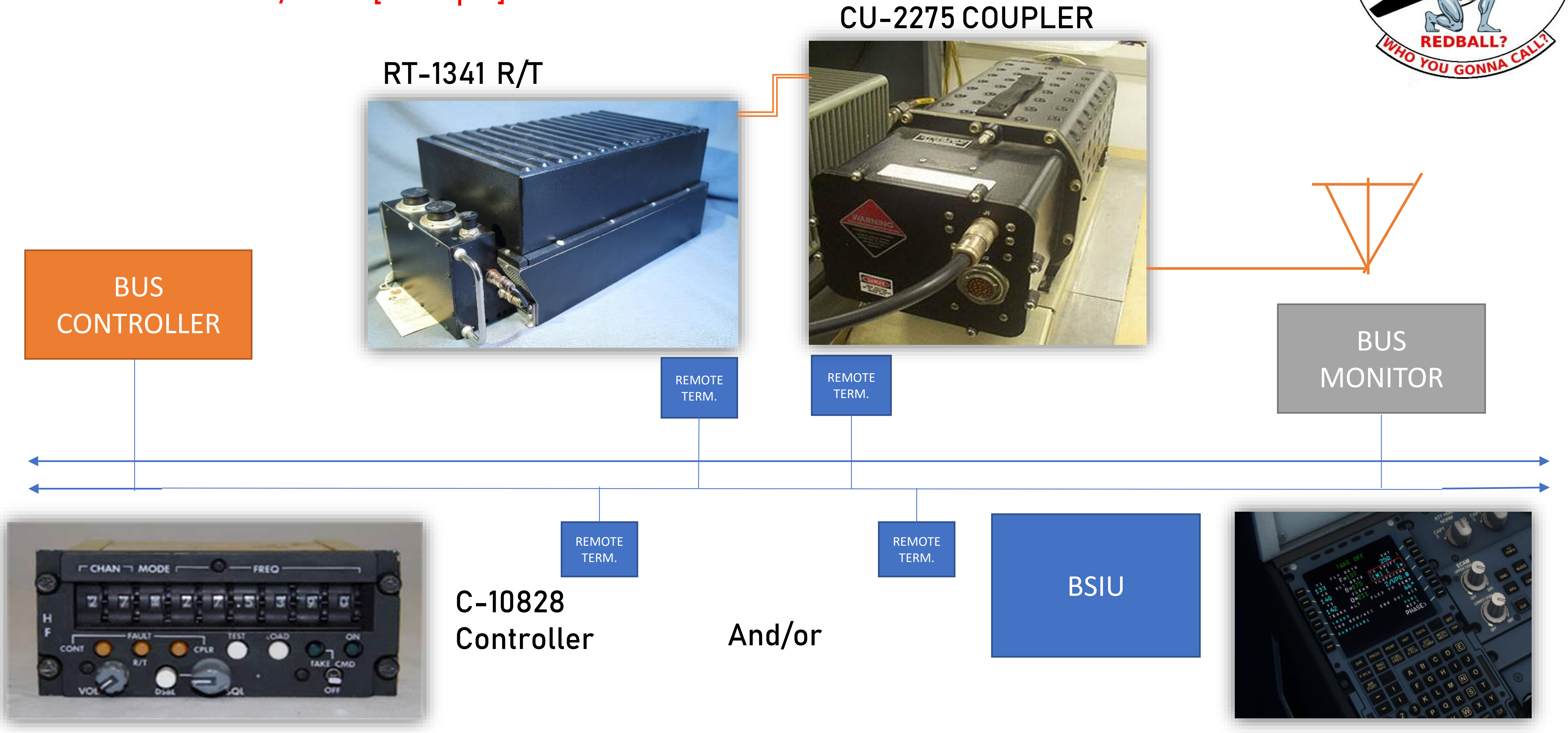
B-1b CITS



B-1b Offensive Officer Position
Dyess AFB
c/o Defense.gov

Avionics Primer for ~~Hackers~~ Security Researchers

HF radio on the C/N bus [example]



CU-2275 COUPLER

RT-1341 R/T

BUS CONTROLLER

REMOTE TERM.

REMOTE TERM.

BUS MONITOR

REMOTE TERM.

REMOTE TERM.

BSIU

C-10828 Controller

And/or

Avionics Primer for ~~Hackers~~ Security Researchers

MIL-STD-1553(B) Coded Language

-Manchester II Encoding

-Binary Phase Shift Keying (BPSK)

-1.0 mbps

-Accuracy of .1% Long term (1000hz)

-Accuracy of .01% short term (1second)

-each word is 16 bits plus sync wave and parity

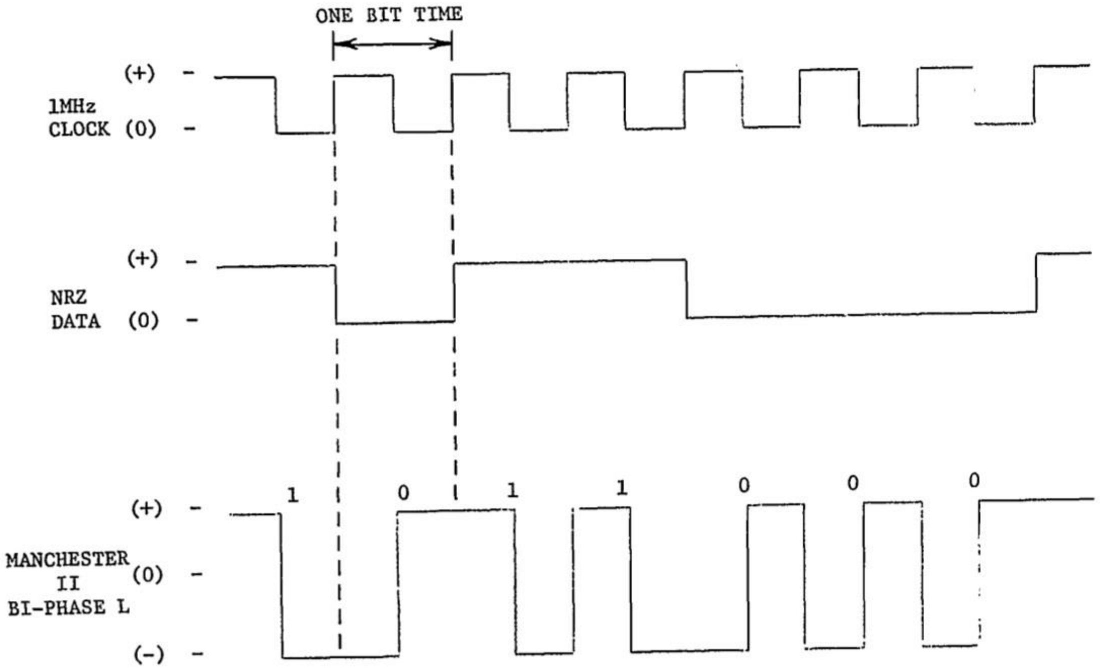
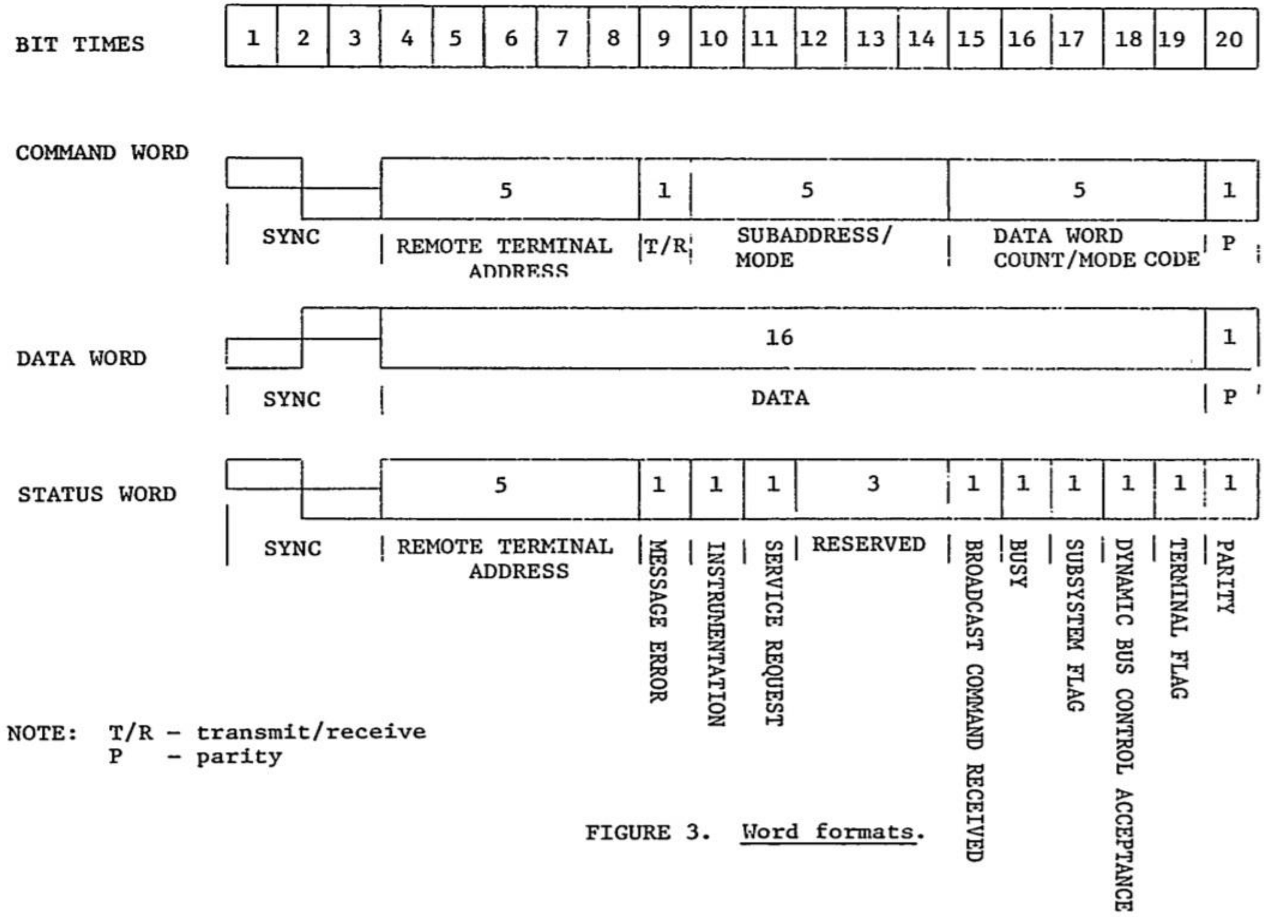


FIGURE 2. Data encoding.

MIL-STD-1553b Data bus Standard Ref(b)

Avionics Primer for ~~Hackers~~ Security Researchers

MIL-STD-1553(B) Word



NOTE: T/R - transmit/receive
P - parity

FIGURE 3. Word formats.

MIL-STD-1553b Data bus Standard Ref(b)

Avionics Primer for ~~Hackers~~ Security Researchers

ARINC-429 Coded Language

-BOEING Standard in legacy systems

-Each word is 32bits

-No more than 20 receivers on single wire

-Unidirectional (tx and rx are on different Ports)

-12.5, 50, or 100kbps

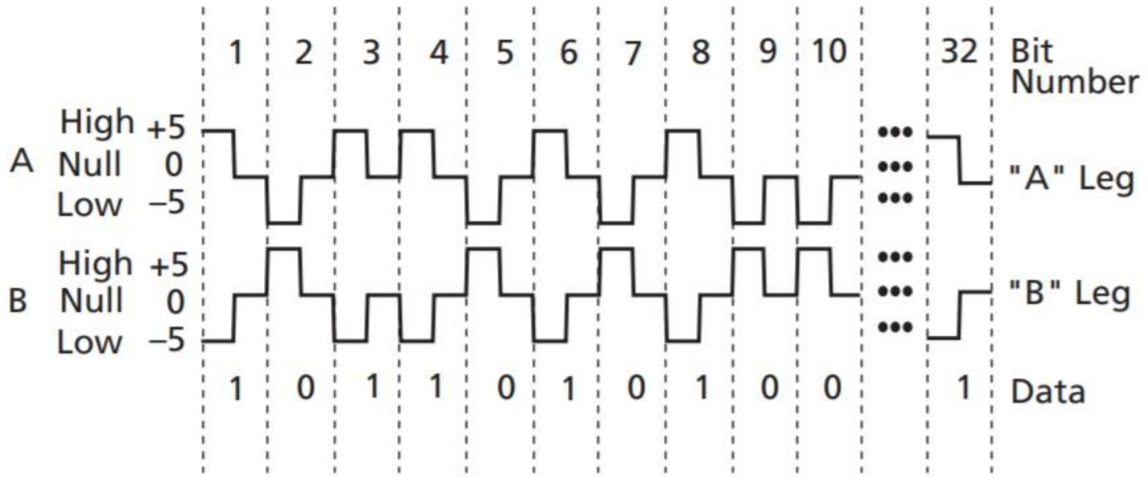


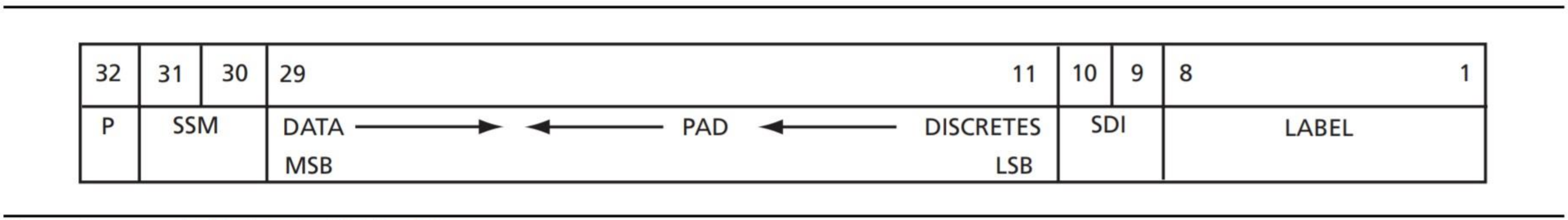
Figure 2 • **ARINC Standard**

ARINC-429 Bus Standard Ref(c)

Avionics Primer for ~~Hackers~~ Security Researchers

ARINC-429 Coded Word

-Contains five fields to every word: Parity Sign/Status Matrix Data Source/destination Label



32	31	30	29 11	10	9	8 1
P	SSM		DATA → ← PAD ← DISCRETES MSB LSB	SDI		LABEL

Figure 3 • **ARINC Data Bit Positions**

ARINC-429 Bus Standard Ref(c)

Avionics Primer for ~~Hackers~~ Security Researchers

AFDX® (ARINC-664)

Avionics Full-Duplex Ethernet Switching

-Airbus Standard

-Maximum 120 data terminals per controller

-2 Mbps

-Each word 32 bits

-COTS Integration

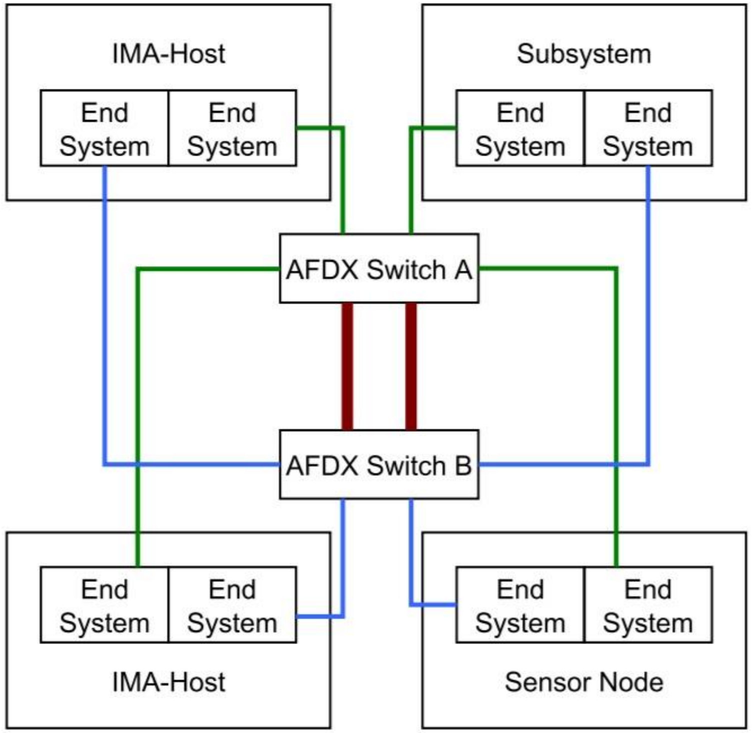
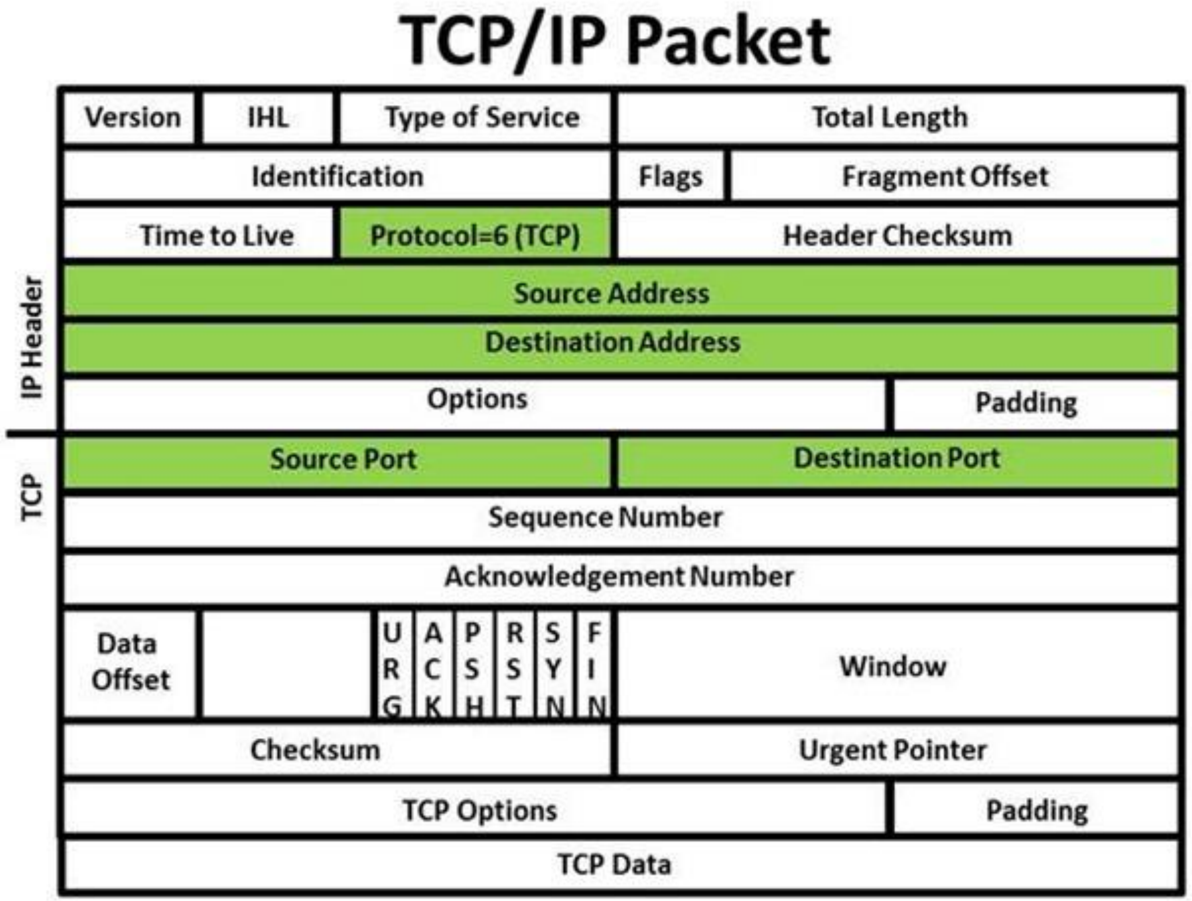


Figure 9: An example of an AFDX based network. Each subsystem is attached physically to the network by two *end systems*. [19]

ARINC-429 to AFDX ref(d)

Avionics Primer for ~~Hackers~~ Security Researchers

AFDX® (ARINC-664 upgraded)



TCP/IP Packet

IP Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol=6 (TCP) | Header Checksum

Source Address

Destination Address

Options | Padding

TCP

Source Port | Destination Port

Sequence Number

Acknowledgement Number

Data Offset | | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

TCP Options | Padding

TCP Data

Packetpushers.net

Avionics Primer for ~~Hackers~~ Security Researchers

Attack Vectors (If they existed)

-COTS (Commercial Off the shelf Devices)

-Local Data Connections

-External Data Connections

-People (always with the People)

Avionics Primer for ~~Hackers~~ Security Researchers

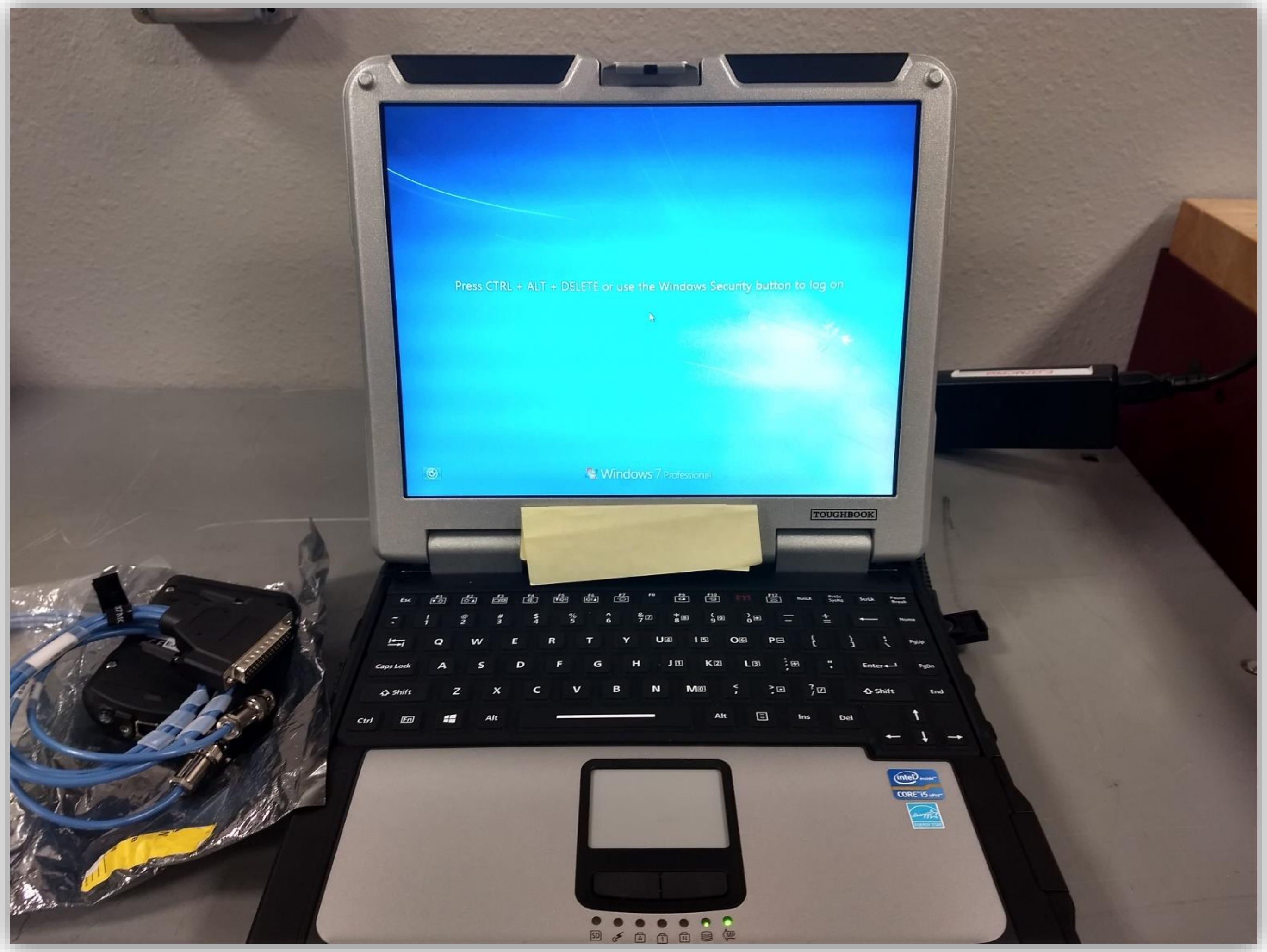
Vectors -COTS

-network hubs

-USB hubs

-computers

-personal devices


Press CTRL + ALT + DELETE or use the Windows Security button to log on
Windows 7 Professional
TOUGHBOOK

Avionics Primer for ~~Hackers~~ Security Researchers

COMM/NAV & MISSION SYS
REDBALL?
WHO YOU GONNA CALL?

Vectors – Local Data Connections

-OFP Loading (1553 Coax shown)

Using on A/C Data bus to load common Processors,

EX:

Primary Flight Computer OFP
SATCOM network Radio
Inertial Navigation Units
More updates as tech advances

-MX data Media

Hot swappable HDD
PCM/CIA Cards
USB drive
SD Cards

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

-CPLDC (Controller Pilot Data Link)

-ACARS (Aircraft Communication, Addressing and reporting System)

-Link-16 (TADIL J – Tactical Digital Information Link J)

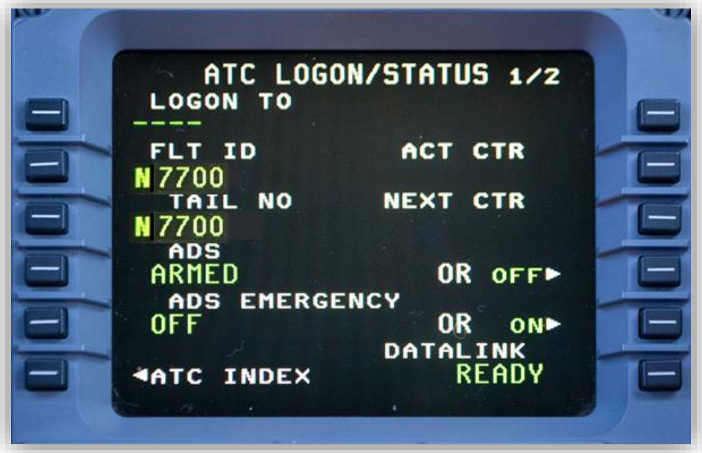
Imagine injection

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

-CPLDC (Controller Pilot Data Link)

-CPLDC is Application layer relying on VDL2
-Used for sending Clear text messages between the ATC and Pilot operators
-Is based off a network to include Iridium Commercial Satellites and ground stations
-VHF band in use for data



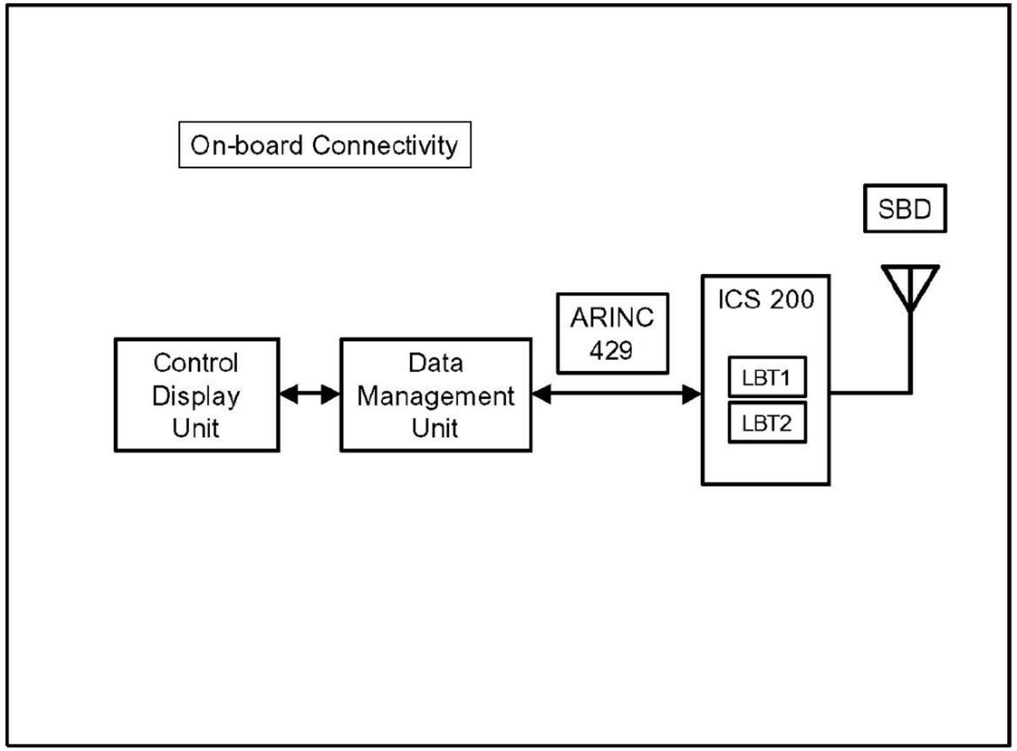
```
   ATC LOGON/STATUS 1/2
 LOGON TO
----
 FLT ID              ACT CTR
N7700
  TAIL NO           NEXT CTR
N7700
  ADS
 ARMED                OR  OFF►
  ADS EMERGENCY
 OFF                  OR  ON►
                    DATALINK
◄ATC INDEX            READY
```

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

-ACARS (Aircraft Communication, Addressing and reporting System)

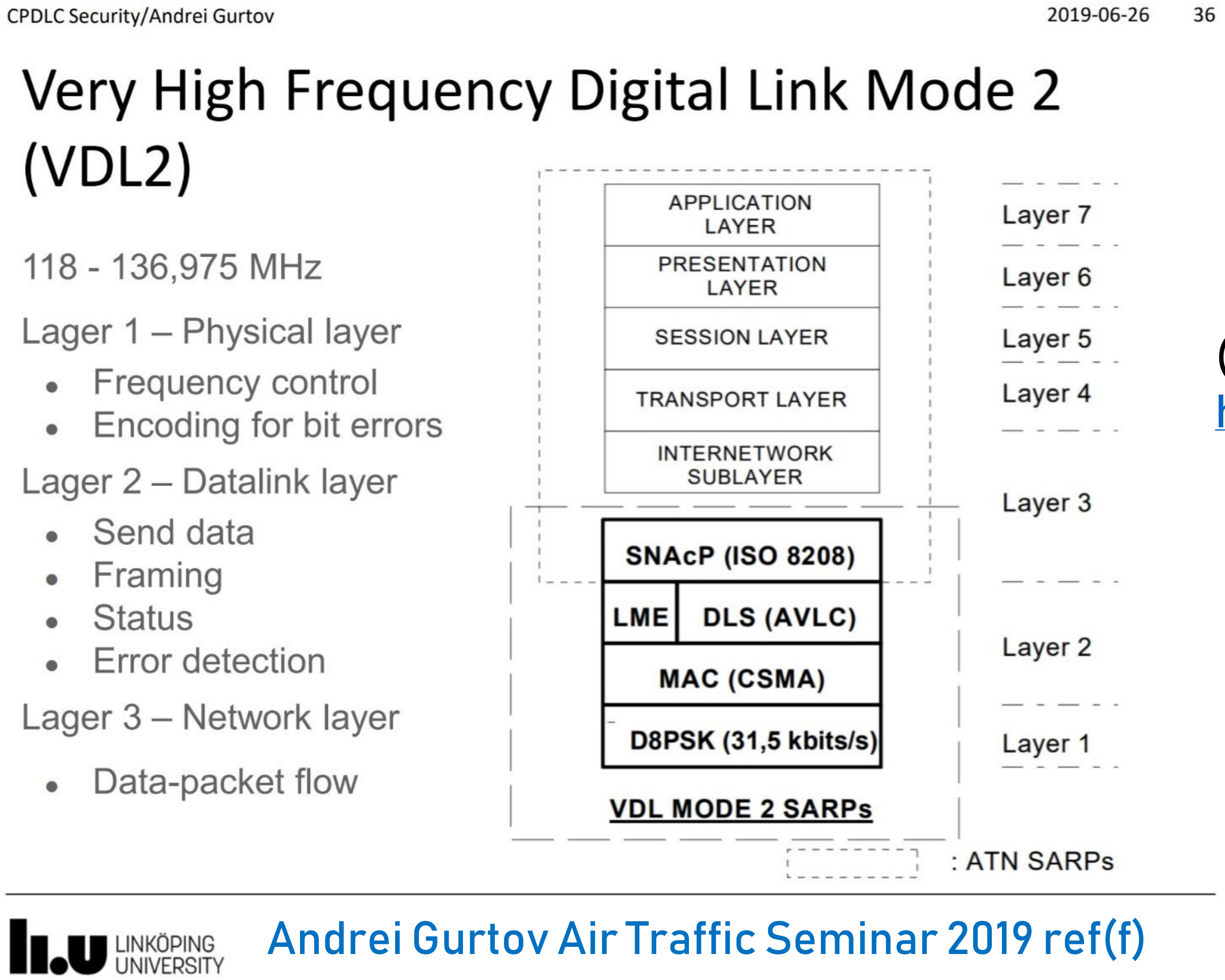
- VHF and HF
- Receive Data to print onto Thermal Paper
-Relies on Readily Available commercial networks
-Also a VDL2 product



ACARS ICS-200-1 ref(e)

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections



CPDLC Security/Andrei Gurtov 2019-06-26 36

Very High Frequency Digital Link Mode 2 (VDL2)

118 - 136,975 MHz

Lager 1 – Physical layer

- Frequency control
- Encoding for bit errors

Lager 2 – Datalink layer

- Send data
- Framing
- Status
- Error detection

Lager 3 – Network layer

- Data-packet flow

APPLICATION LAYER | Layer 7

PRESENTATION LAYER | Layer 6

SESSION LAYER | Layer 5

TRANSPORT LAYER | Layer 4

INTERNETWORK SUBLAYER | Layer 3

SNAcP (ISO 8208)

LME | DLS (AVLC) | Layer 2

MAC (CSMA)

D8PSK (31,5 kbits/s) | Layer 1

VDL MODE 2 SARPs

: ATN SARPs

LINKÖPING UNIVERSITY

Andrei Gurtov Air Traffic Seminar 2019 ref(f)

(h)Github DumpVDL2 from Tomasz Lemiech(szpajder)
https://github.com/szpajder/dumpvdl2

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

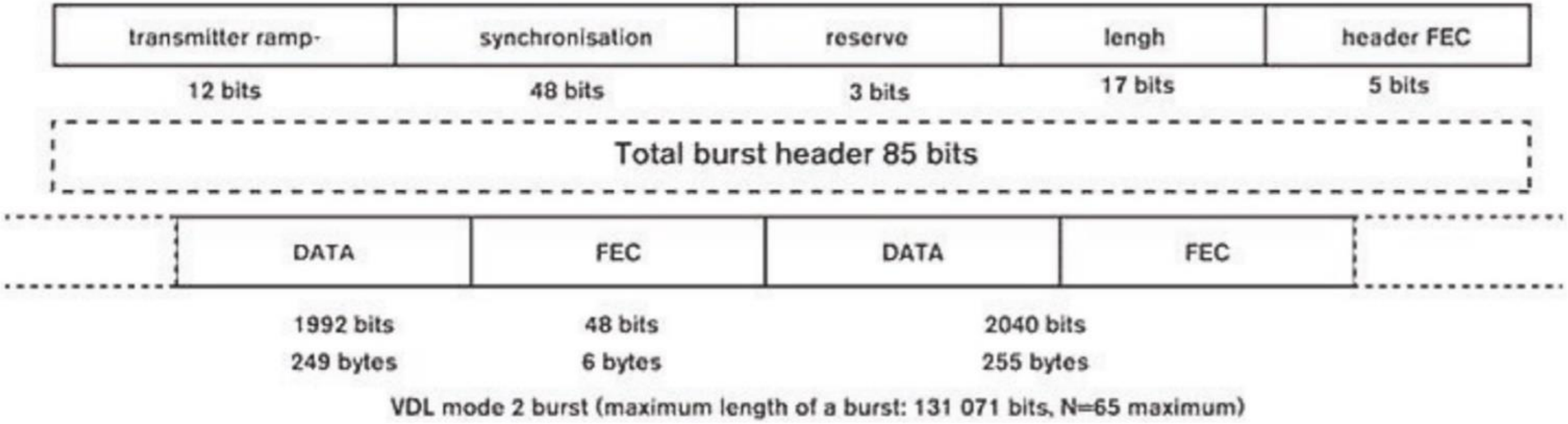
-A little bit about VDL

-ACARS and CPDLC are applications

-VDL is a point-to-point communication technology

-VHF, limited to 200KM of the Aircraft 3k-4k feet

-SDR project Dumpvdl2 on Github



VDL mode 2 burst (maximum length of a burst: 131 071 bits, N=65 maximum)

European Telecommunications Standards Institute Master Documentation for VDL
(Ref g)VDL Technical characteristics ETSI EN 301 841-1

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

-Link-16 TADILJ (Tactical Digital Information Link)

-PSK on SECRET hardware devices (Air Gapped)
-Uses freq hop to prevent jamming, (WOD,TOD, Net number) HAVEQUICK
-960-1200MHZ VHF/UHF
-Limited to LOS but this includes Satellites
-Provides
- -target data
- -Friendly location data
- -command and control
- -Mesh Network
- -Different hardware performs different roles/functions

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –External Data Connections

-Link-16 TADILJ (Tactical Digital Information Link)

Message Catalogue

Network Management
Precise Participant Location and Identification
Surveillance
Antisubmarine Warfare
Intelligence
Information Management
Weapons Coordination and Management
Control
Platform and System Status
Electronic
Threat warning
National Use

TADIL J Introduction and Reference Guide Ref(i)

Avionics Primer for ~~Hackers~~ Security Researchers

Vectors –~~Users~~, Pilots & Maintainers

-Aircraft Software updates are time sensitive, especially combat DoD

-Chain of custody is not always verified in Commercial products

-Engineers use publicly available sources (such as VDL2)

-Pilots are starting to bring Personal devices to aircraft flight decks

-Civilian customers on the Aircraft Network.

Avionics Primer for ~~Hackers~~ Security Researchers

RESOURCES

(a)Design and Development of Aircraft systems Google-book http://bit.ly/2k6kICx

(b)MIL-STD-1553b Data bus Standard 1979/01/22 PDF http://bit.ly/2m2UBwZ

(c)ARINC-429 Bus Standard PDF (Archive.org) http://bit.ly/2qtYb5f

Data Link Advisory Circular PDF http://bit.ly/2pGR5Ke

(d)Evolution of Avionics Networks from ARINC-429 to AFDX PDF http://bit.ly/2N4DGnm

IRIG-106 Aeronautical telemetry Open source 1553 Mil standard format 0 http://bit.ly/31AMUgu

Data Comm Systems with FANS 1/A+, CPDLC DCL and ATN B1 PDF http://bit.ly/2N1jR0h

(e)ICAO International Introduction to ACARS ICS-200-1 PDF http://bit.ly/2Bvuhjp

SDRPlay Decoding ACARS Messages PDF http://bit.ly/2J9KMGf

(f)Andrei Gurtov Air Traffic Seminar 2019 http://bit.ly/2Na0pia

(g)VDL Technical characteristics ETSI EN 301 841-1 PDF http://bit.ly/2pI63Qj

(h)Github DumpVDL2 from Tomasz Lemiech(szpajder) https://github.com/szpajder/dumpvdl2

(i)TADIL J Introduction and Reference Guide PDF http://bit.ly/2obvLf0

Avionics Primer for ~~Hackers~~ Security Researchers

Nicholas Childs TSgt, USAF

B-1 Weapon Systems Controller

Bomber/Special Integrated
Communication/Navigation/Mission Systems Craftsman
OAS?

Twitter/Instagram @Boxswapper
Email boxswappers@gmail.com