Don’t fear the BUS, It won’t run you over

Presenter: Nicholas Childs

Date: Friday, Aug 6th 1400-1425

Summary: **This talk is a basic introduction to aircraft avionics comm/nav bus systems and the expansion of the network to more vulnerable areas than have seen before. It is more of a primer and 101 for stepping into the larger world of aerospace networks**.

Don't fear the BUS

Nicholas Childs
Security Manager/OAS/B1Systems Controller/TODO/Forklift Operator/Bus Driver/Customs Inspector/CSL/Cut-Trained Crew Chief/Commercial Aircraft Servicing Technician
Retiree

github.com/boxswapper
Twitter @Boxswapper
Email nick@boxswappers.com

Don't fear the BUS

C:\Users\1256369778>whoami
- Intern with FullCircle Communications LLC
- 20 years experience in communication navigation systems
- Aeronautical Engineering Degree
- Mechanical repair and servicing experience with 737, L10-11, DC-10, 747
- Proficient with multiple airframe 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

Don't fear the BUS

Original 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!!!

Don't fear the BUS

New Why?

Avionics BUS systems and integrated flight management systems now seem to be the things of magic. Let's demystify and educate. I promise, we can easily learn things that high school educated Airmen know.

It's not as painful as you think

Additionally, input validation is not a thing!

Don't fear the BUS

Viewers Like you…

Don't fear the BUS

History Of Aircraft network systems

Communication along BUS systems

A few networks you should know about

Attack Vectors and Upgrades

Don't fear the BUS

History of Aircraft Network Systems

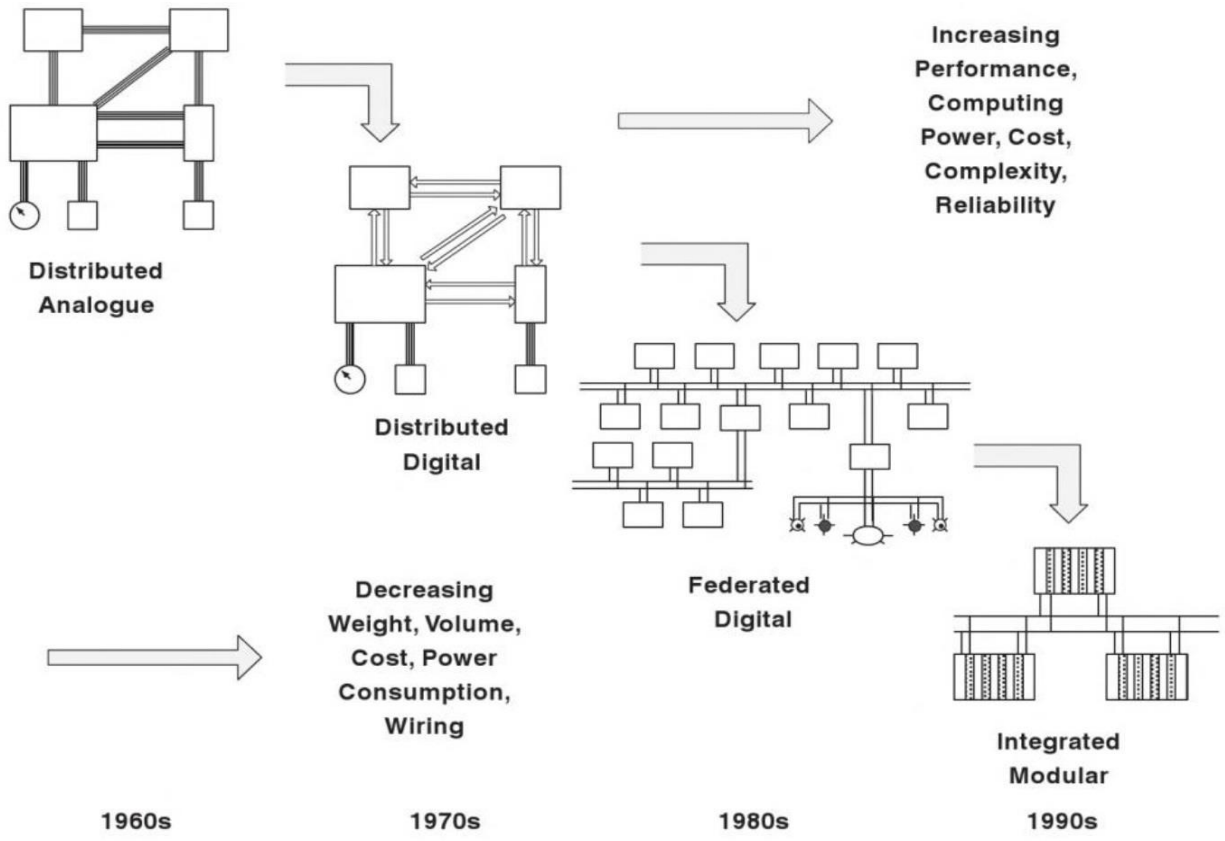
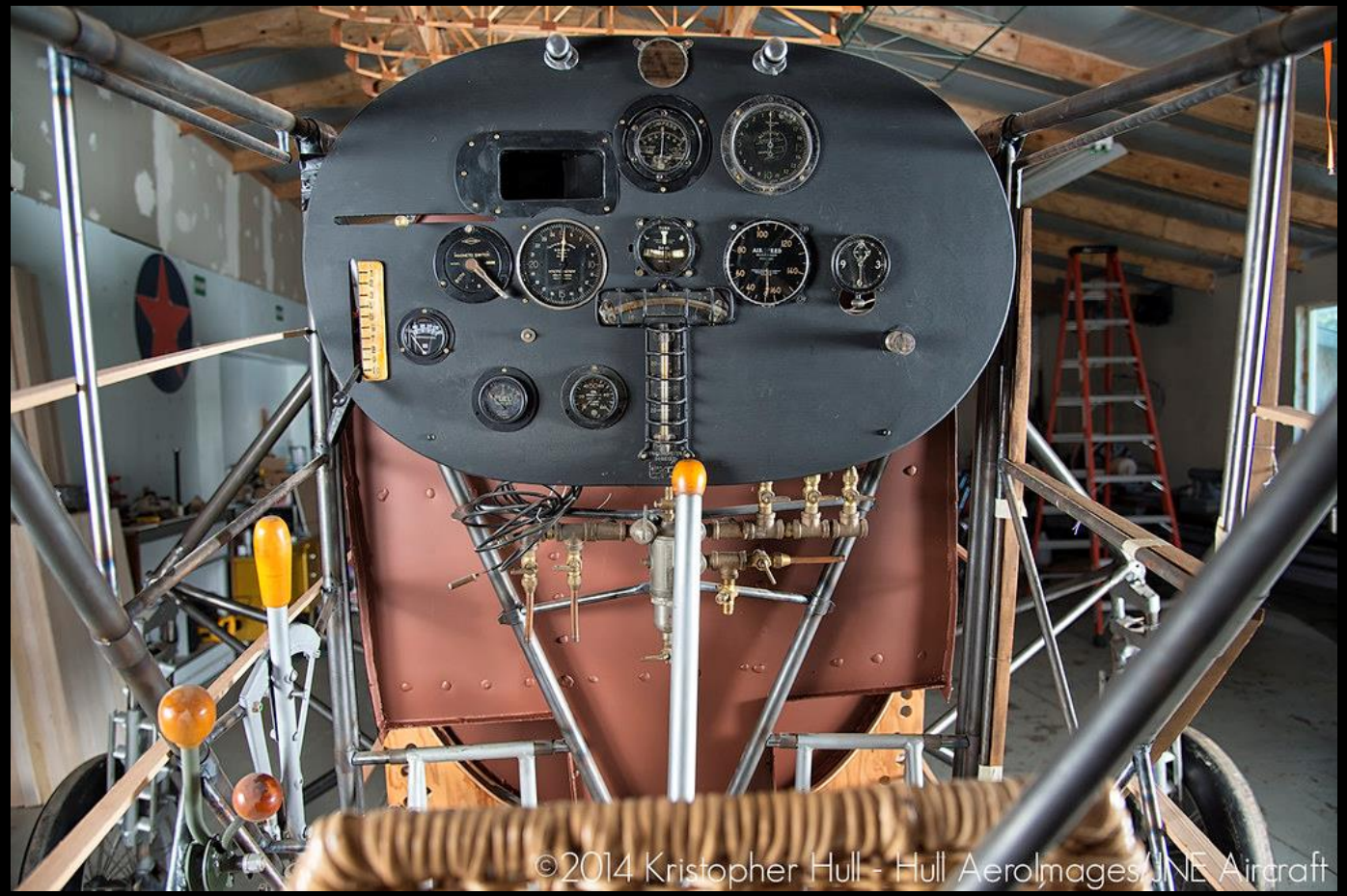


Figure 5.11 Evolution of avionics architectures.

Design and Development of Aircraft Systems Ref (a)

Don't fear the BUS

Distributed Analogue



Spirit of St. Louis Replica Cockpit
C/o Kristopher Hull

Don't fear the BUS

Distributed Digital

DC-7 Cockpit
Ramey Logan Photographer

Don't fear the BUS

Federated Digital

C-5M Super Galaxy Cockpit

Paris- LeBourget
©Jonathan Zaniger

Don't fear the BUS

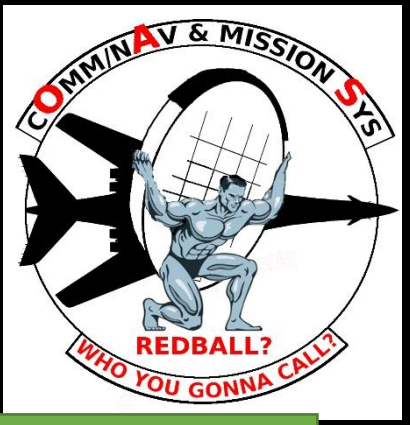
Integrated Modular

A380 Airbus cockpit

Wallpaper Safari

Don't fear the BUS

Federated Digital (Mil-STD-1553b & ARINC-429)



3. Interface Layer

Flight Management System

Data Loader

MX Computer

Emergency Comm Controller

2. LRU Layer

Radio set

BSIU

MFD controller

ADC

Trans-Ponder

TCAS

REMOTE TERM.

REMOTE TERM.

REMOTE TERM.

Controller

REMOTE TERM.

REMOTE TERM.

REMOTE TERM.

1. Network Layer

Don't fear the BUS

B-1b CITS

CITS "Maintenance Computer"

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

Don't fear the BUS

There are Many BUS'es

-MIL-STD-1553(B)	Federated Digital
-ARINC-429	Federated Digital
-AFDX® (ARINC-664)	Integrated Modular

Don't fear the BUS

BUS - MIL-STD-1553(B) Coded Language

- -Manchester II Encoding
- -Binary Phase Shift Keying (BPSK)
- -1.0 mbps
- -Accuracy of .01% short term (100Hz)
- -Accuracy of .1% Long term (1000Hz)
- -each word is 16 bits plus sync wave and parity

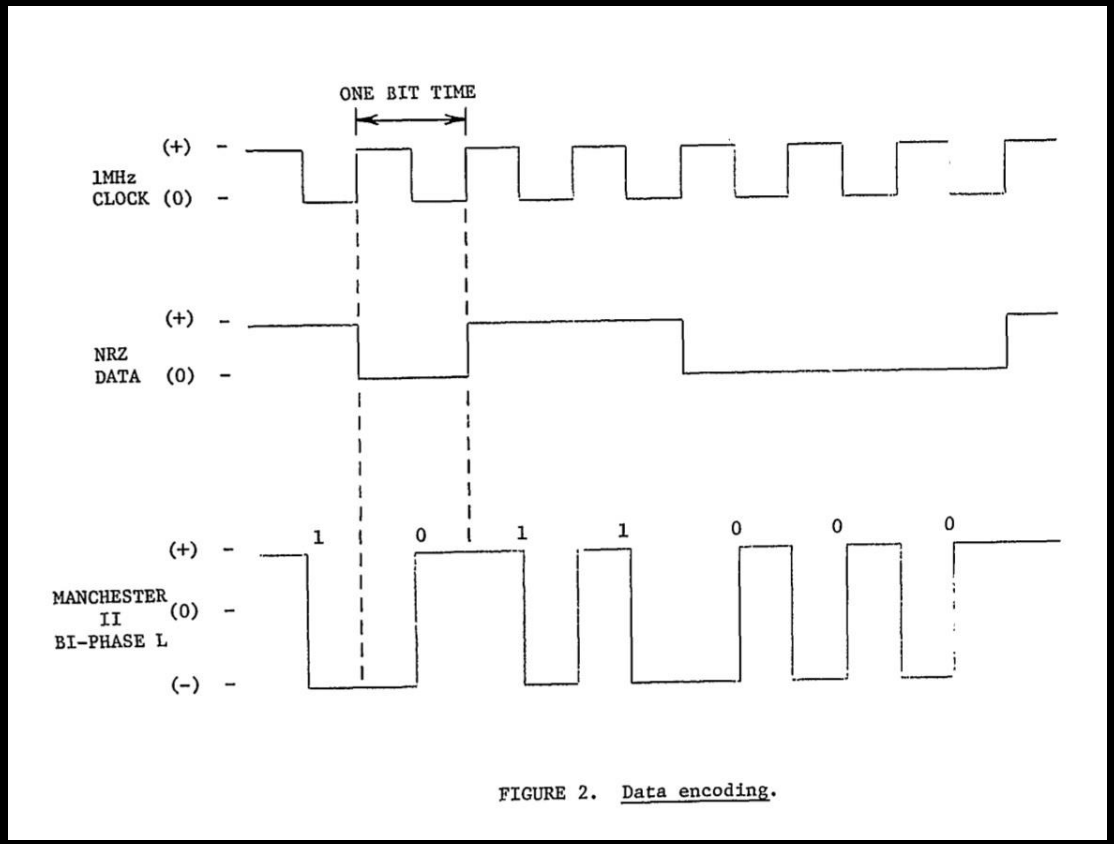


FIGURE 2. Data encoding.

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

Don't fear the BUS

BUS - MIL-STD-1553(B) Word

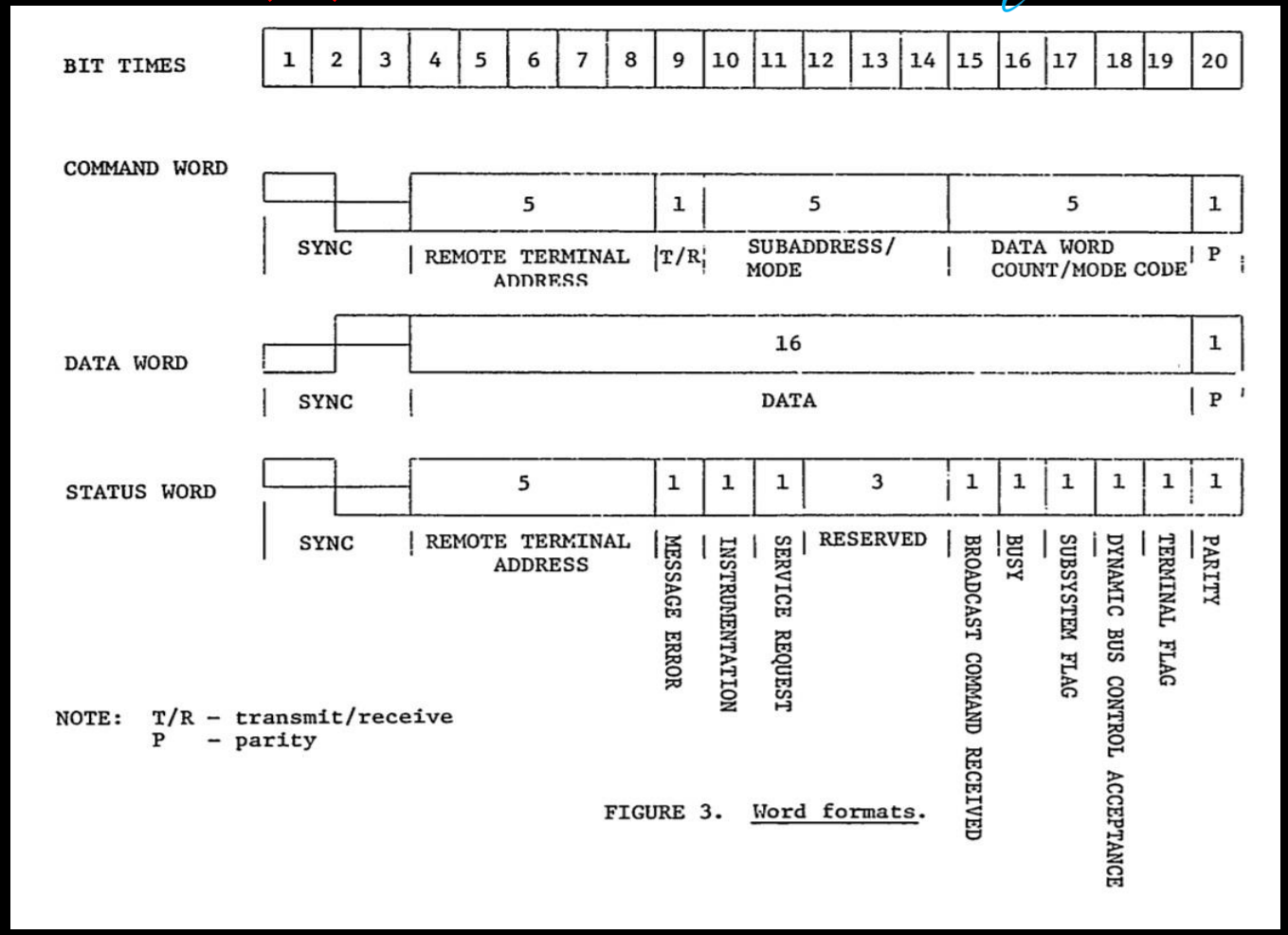


FIGURE 3. Word formats.

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

Don't fear the BUS

BUS – 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

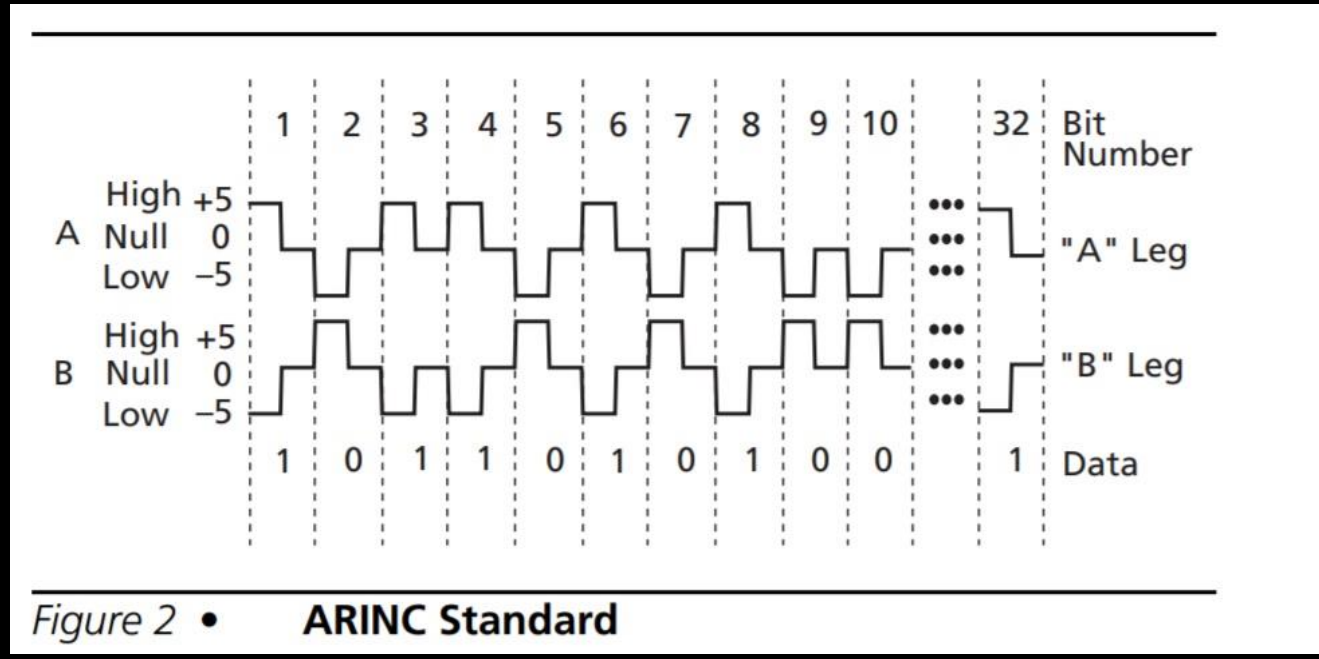


Figure 2 • **ARINC Standard**

ARINC-429 Bus Standard Ref(c)

Don't fear the BUS

BUS - ARINC-429 Coded Word

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

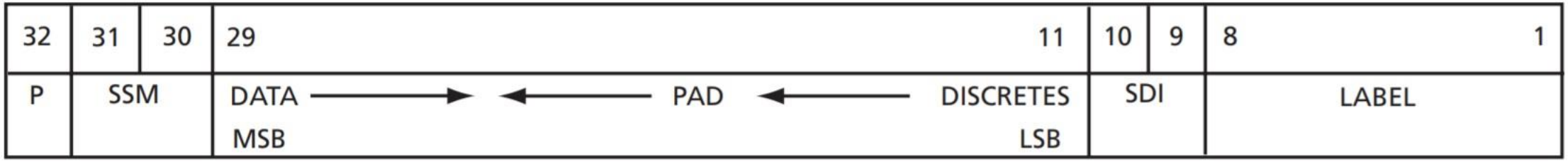


Figure 3 • **ARINC Data Bit Positions**

ARINC-429 Bus Standard Ref(c)

Don't fear the BUS

BUS – Integrated Modular

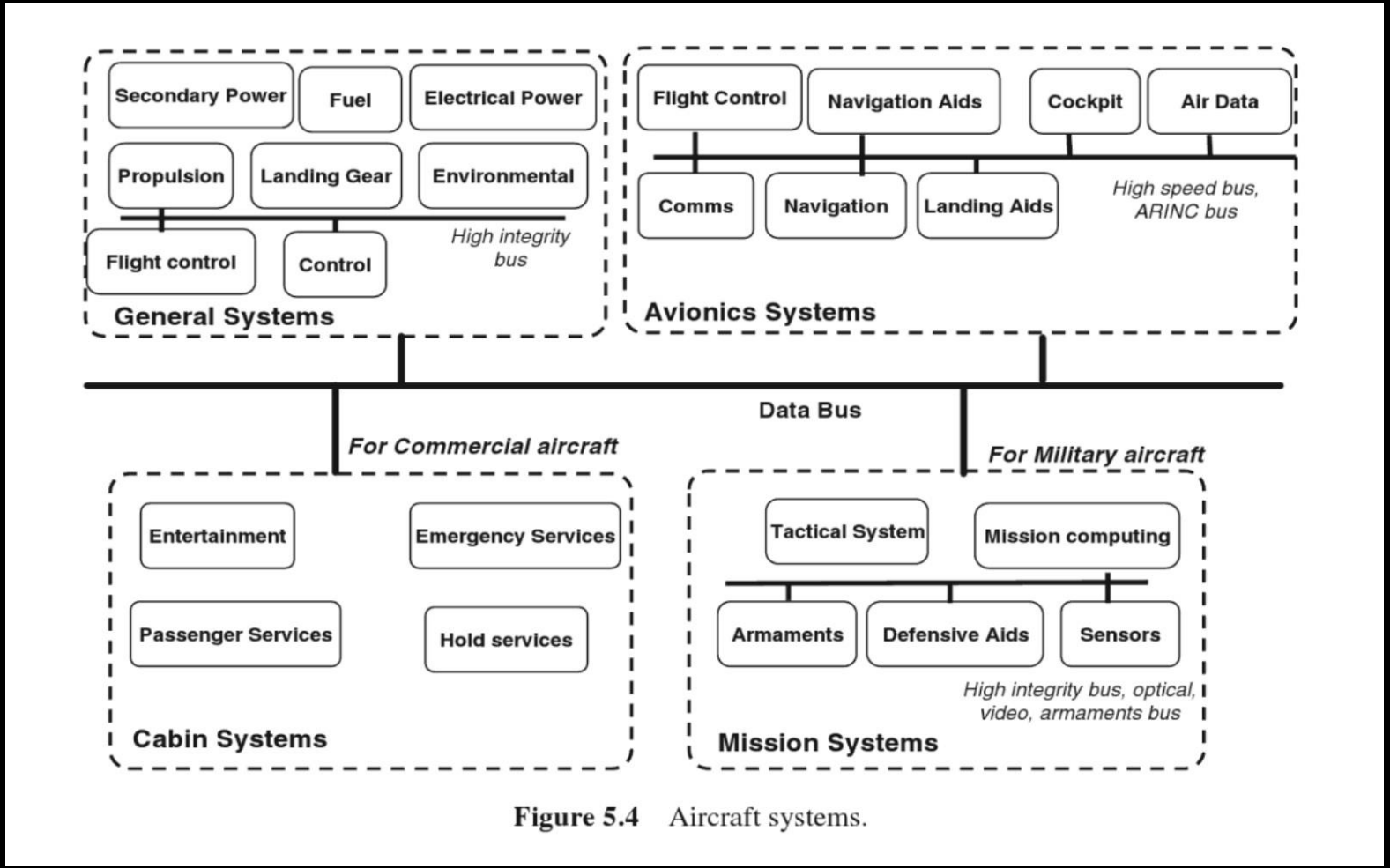


Figure 5.4 Aircraft systems.

Design and Development of Aircraft Systems Ref (a)

Don't fear the BUS

BUS - AFDX® (ARINC-664))

Avionics Full-Duplex Ethernet Switching

-Airbus Standard

-Maximum 120 data terminals per controller

-2 Mbps

-Each word 32 bits

-COTS Integration

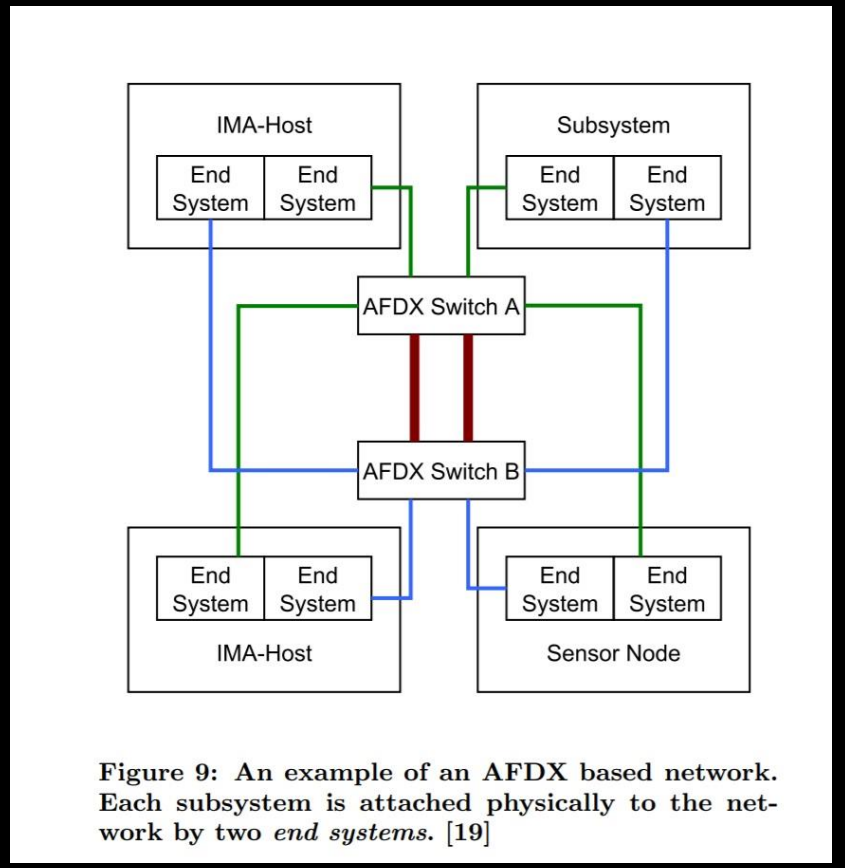
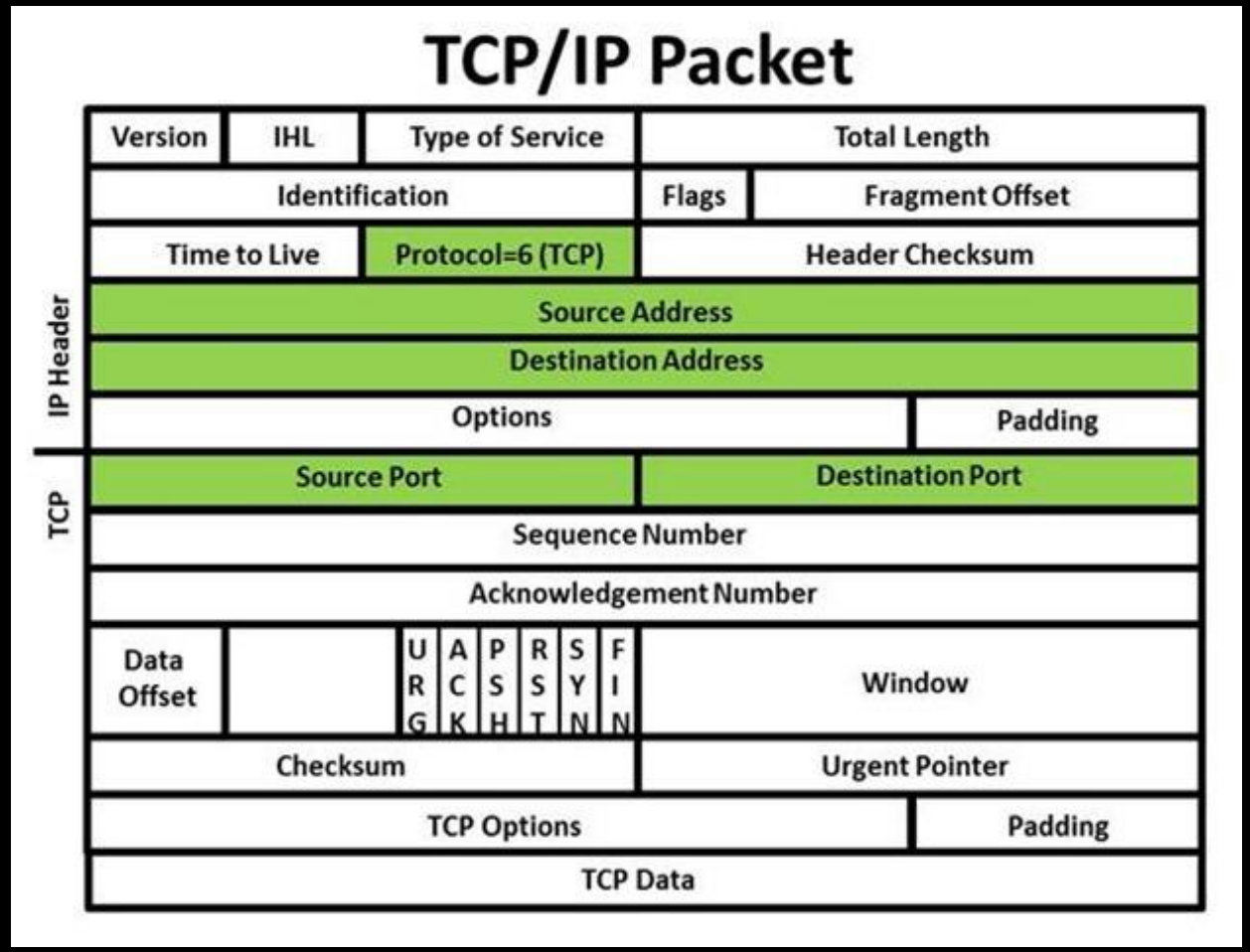


Figure 9: An example of an AFDX based network. Each subsystem is attached physically to the network by two *end systems*. [19]

ARINC-429 to AFDX ref(d)

Don't fear the BUS

BUS - AFDX® (ARINC-664 upgraded)



Don't fear the BUS

BUS - AFDX® (ARINC-664) FRAME

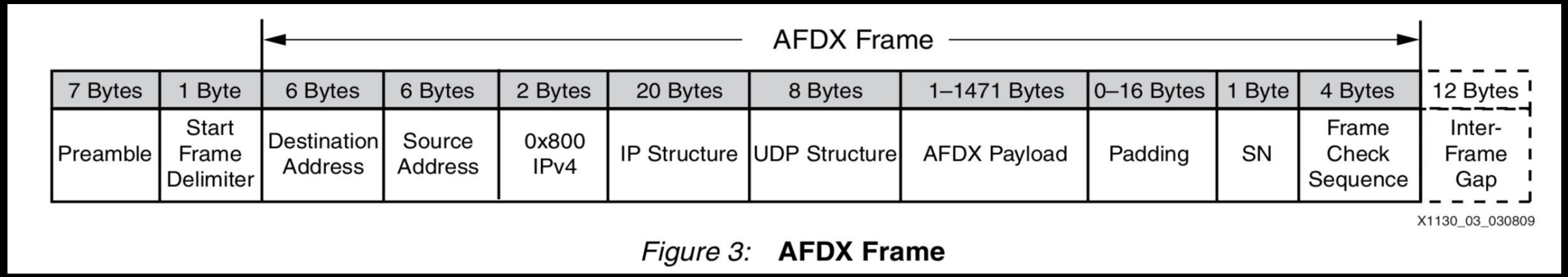


Figure 3: **AFDX Frame**

XILINX Architecting ARINC 664 Part 7 (ref da)

Don't fear the BUS

Attack Vectors (If they existed)

-COTS (Commercial Off the shelf Devices)

-Local Data Connections

-External Data Connections

-People (always with the People)

Don't fear the BUS

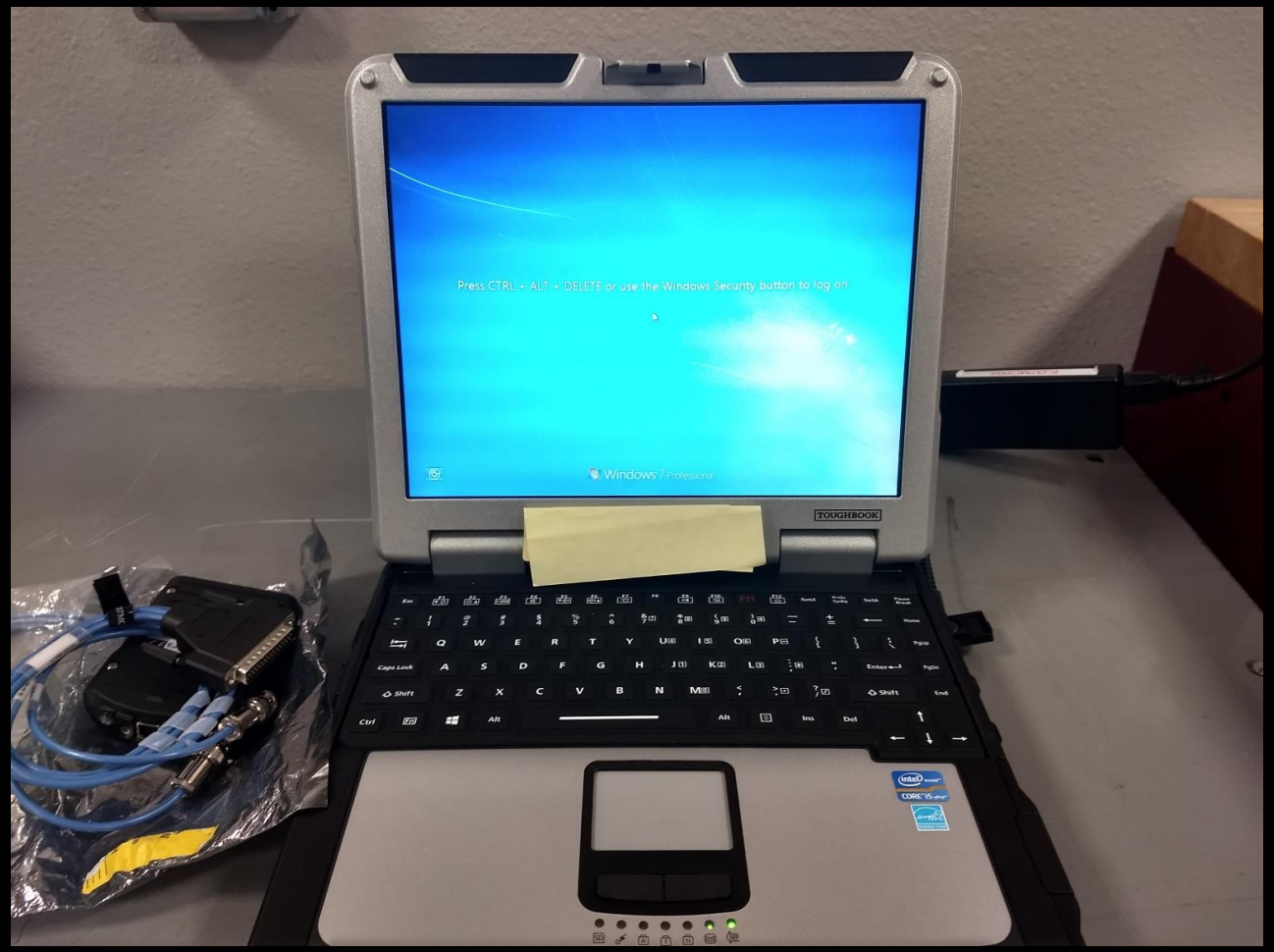
Vectors -COTS

-network hubs

-USB hubs

Literally, commercial Devices designed for IT infrastructure.

- Surprisingly enough, COTS protocols and Services as well.



Don't fear the BUS

Vectors – Local Data Connections

-OFP Loading (1553 Coax shown)
- Using on A/C Data bus to load common Processors,
- EX:
- Primary Flight Computer OFP
- Air Data Computer OFP
- Inertial Navigation Units OFP
- More updates as tech advances

BYOD type MEDIA
- Electronic Flight Bag

-MX data Media
- Hot swappable HDD
- PCM/CIA Cards
- USB drive
- SD Cards

Don't fear the BUS

Vectors –External Data Connections

-CPLDC (Controller Pilot Data Link)

-ACARS (Aircraft Communication, Addressing and reporting System)

-FANS (Future Air Navigation Systems)(VDL2)

Don't fear the BUS

Vectors –External Data Connections

-CPLDC (Controller Pilot Data Link)

Don't fear the BUS

Vectors –External Data Connections

-CPLDC (Controller Pilot Data Link)

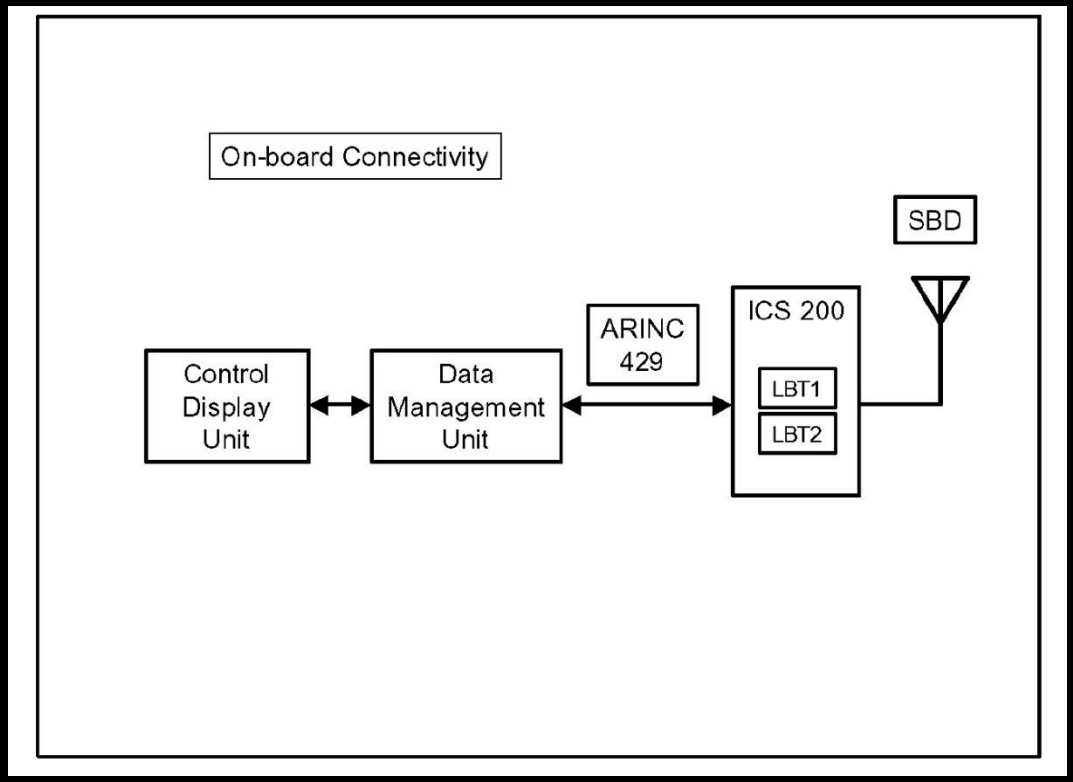
-CPLDC is Application layer relying on VDL2
-Used for sending Clear text messages between the ATC and Pilot operators
-Is based off a network to include Iridium Commercial Satellites and ground stations
-VHF band in use for data

Don't fear the BUS

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



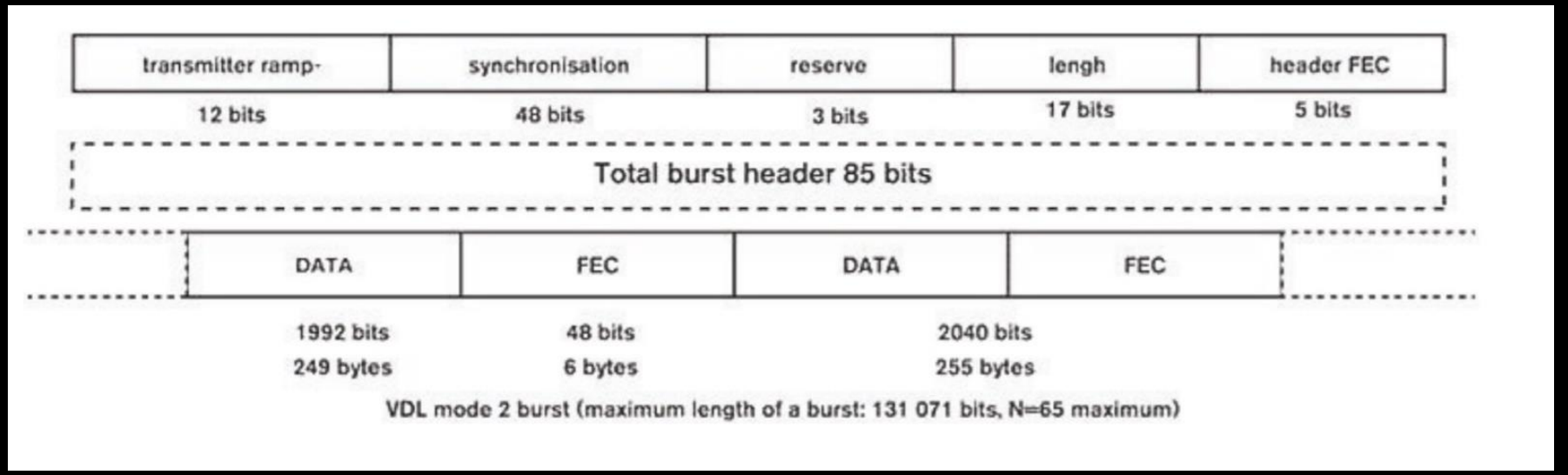
ACARS ICS-200-1 ref(e)

Don't fear the BUS

Vectors –External Data Connections

-FANS (Future Air Navigation System)

-VDL is a point-to-point communication technology
-VHF, limited to 200NM of the Aircraft 3k-4k feet
-SDR project Dumpvdl2 on Github



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

Don't fear the BUS

Vectors –External Data Connections

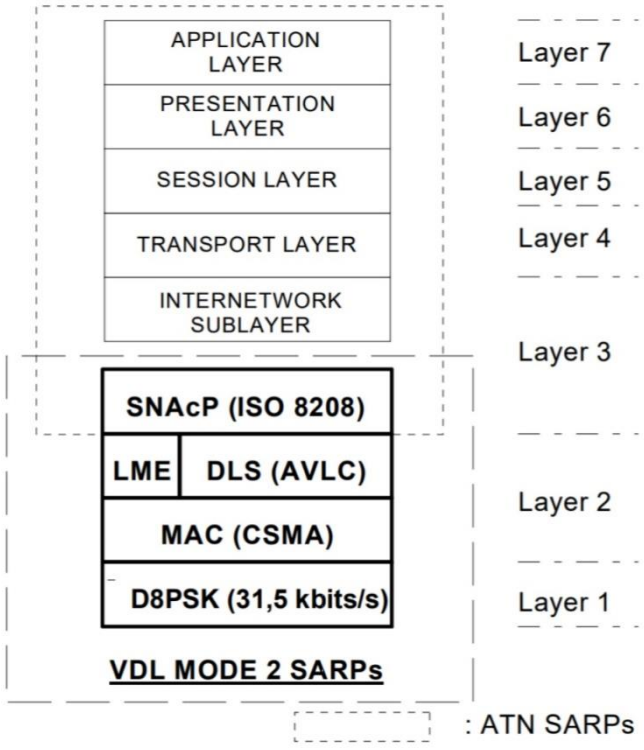
Very High Frequency Digital Link Mode 2 (VDL2)

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



LINKÖPING UNIVERSITY

Andrei Gurtov Air Traffic Seminar 2019 ref(f)

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

Don't fear the BUS

Hacker Hurdles

-Understanding Aircraft Infrastructure

-Understanding Specific components Functions

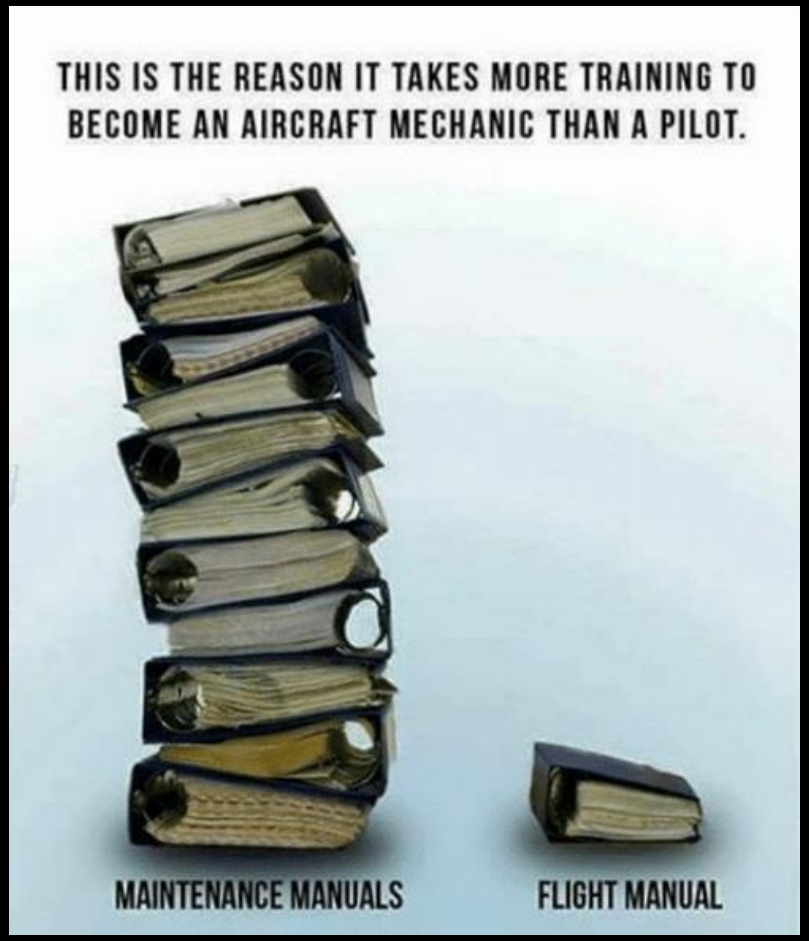
-Physical Access to hardware

-Testing / Tabletop Access to Software & Hardware

Don't fear the BUS

Addendum: Things are happening

- Bombardier Data Leak of CG information, RADAR and linkage
- Software Example, Boeing 737 MAX (OFP)
- US Government Probes A/C Vulns 'Only a Matter of time'



Don't fear the BUS

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/39QFmLu

(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

(da)XILINX Architecting ARINC 664 https://bit.ly/36VM2s1

(e)ICAO International Introduction to ACARS ICS-200-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/2pl63Qj

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

*Evolution of Avionics Netoworks from ARINC-429 to AFDX https://bit.ly/3eSKOC7

Exploring the Vulns. Of TCAS through SDR PDF http://bit.ly/2Wcjzd6