INVERSE PATH

Real-life experiences in avionics security assessment

Andrea Barisani
<andrea@inversepath.com>

INVERSE PATH

Security researcher & developer

Founder of international consultancy Inverse Path

Founder of oCERT
(Open Source Computer Security Incident Response Team)

Contributor to the international OSS and security community, several books and open standards

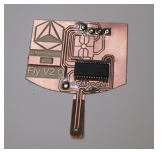
Speaker and trainer at BlackHat, CanSecWest, DEFCON, Hack In The Box, PacSec conferences among many others

INVERSE PATH

2007: Unusual Car Navigation Tricks
Injecting RDS-TMC Traffic Information Signals

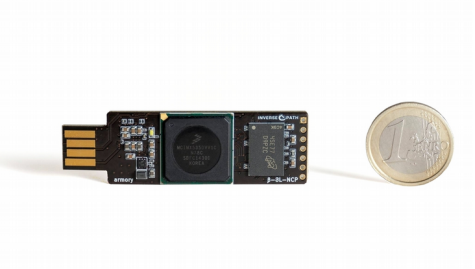
2009: Sniff Keystrokes With Lasers/Voltmeters
Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

2011: Chip & PIN is definitely broken
Credit card skimming and PIN harvesting in an EMV world



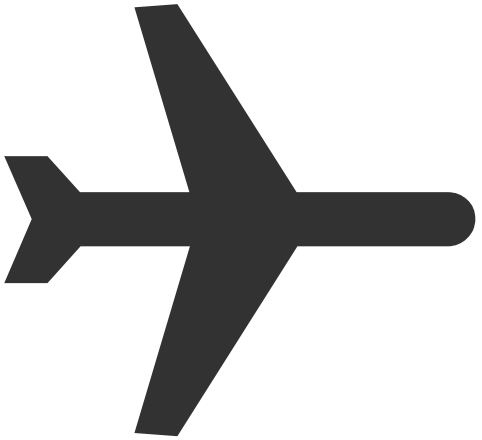
2013: Fully arbitrary 802.3 packet injection
Maximizing the Ethernet attack surface

2015: USB armory



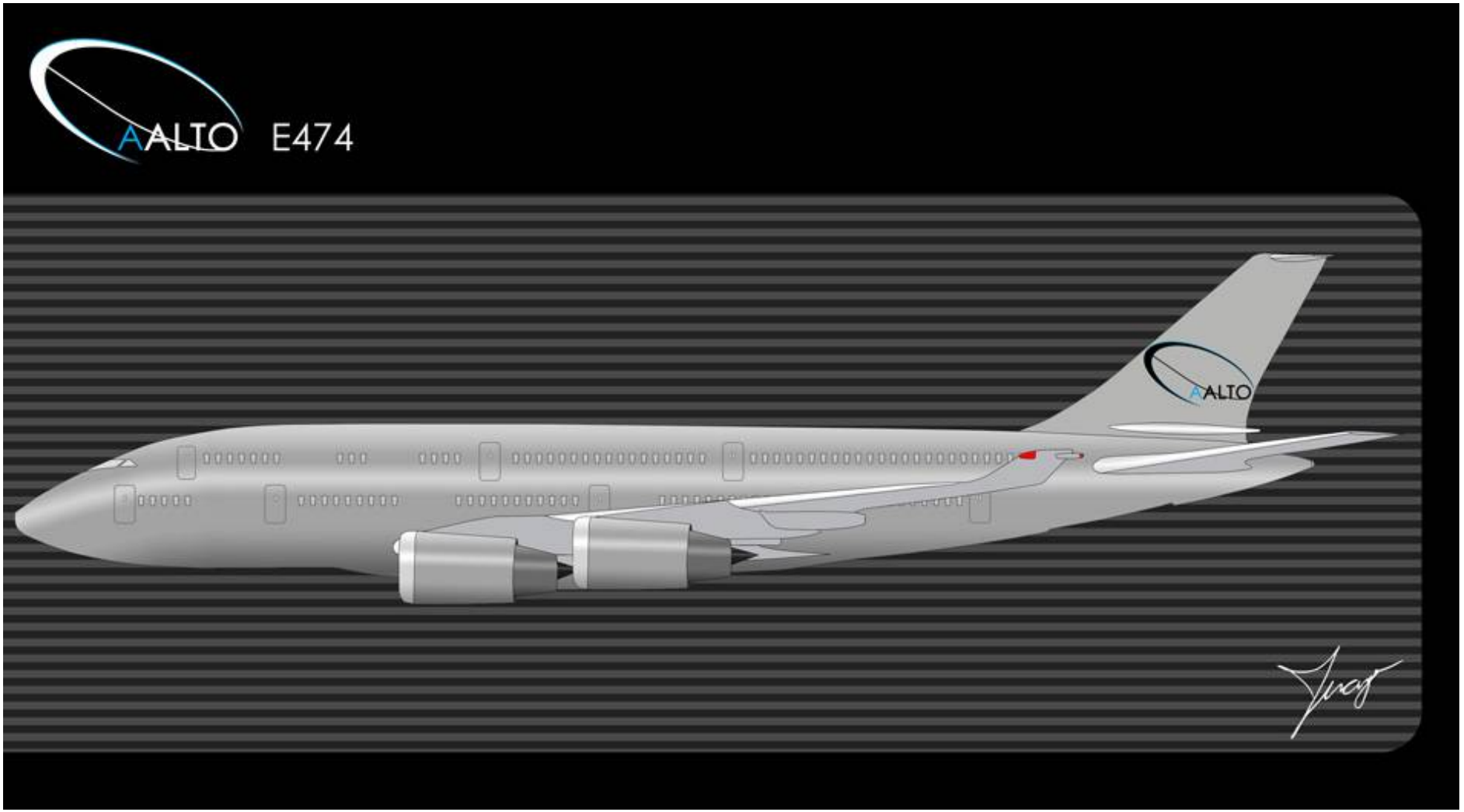
safety critical components are also security critical components

INVERSE PATH



Internet of Things

can’t think of a bigger “thing” than an aircraft…



Skyfleet S570

Safety critical industries, such as aviation and automotive, trigger a high degree of public attention on their potential security concerns.

At the same time aviation security is hard to approach for non experts despite a vast number of information and certification processes available.

It is hard to find comprehensive technical information due to the complexity of interconnected systems, number of parts and inherent non public nature of more detailed information.

This leads to a lot of **security circus**, **FUD** and **bad press**...

"Cyber-attack concerns raised over Boeing 787 chip's 'back door'"

A truly **outstanding** research is however reported with a lot of hyperbole.

"two...experts have discovered a 'back door' in a computer chip used in military systems and aircraft such as the Boeing 787 that could allow the chip to be taken over via the Internet"

"Cyber-attack concerns raised over Boeing 787 chip's 'back door'"

A truly **outstanding** research is however reported with a lot of hyperbole.

"two...experts have discovered a 'back door' in a computer chip used in military systems and aircraft such as the Boeing 787 that could allow the chip to be taken over via the Internet"

Translation: JTAG connection (unlikely to ever be "taken over via the Internet") allows compromise/reset of FPGA cryptographic functions/storage regardless of security level (bad!).

https://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf

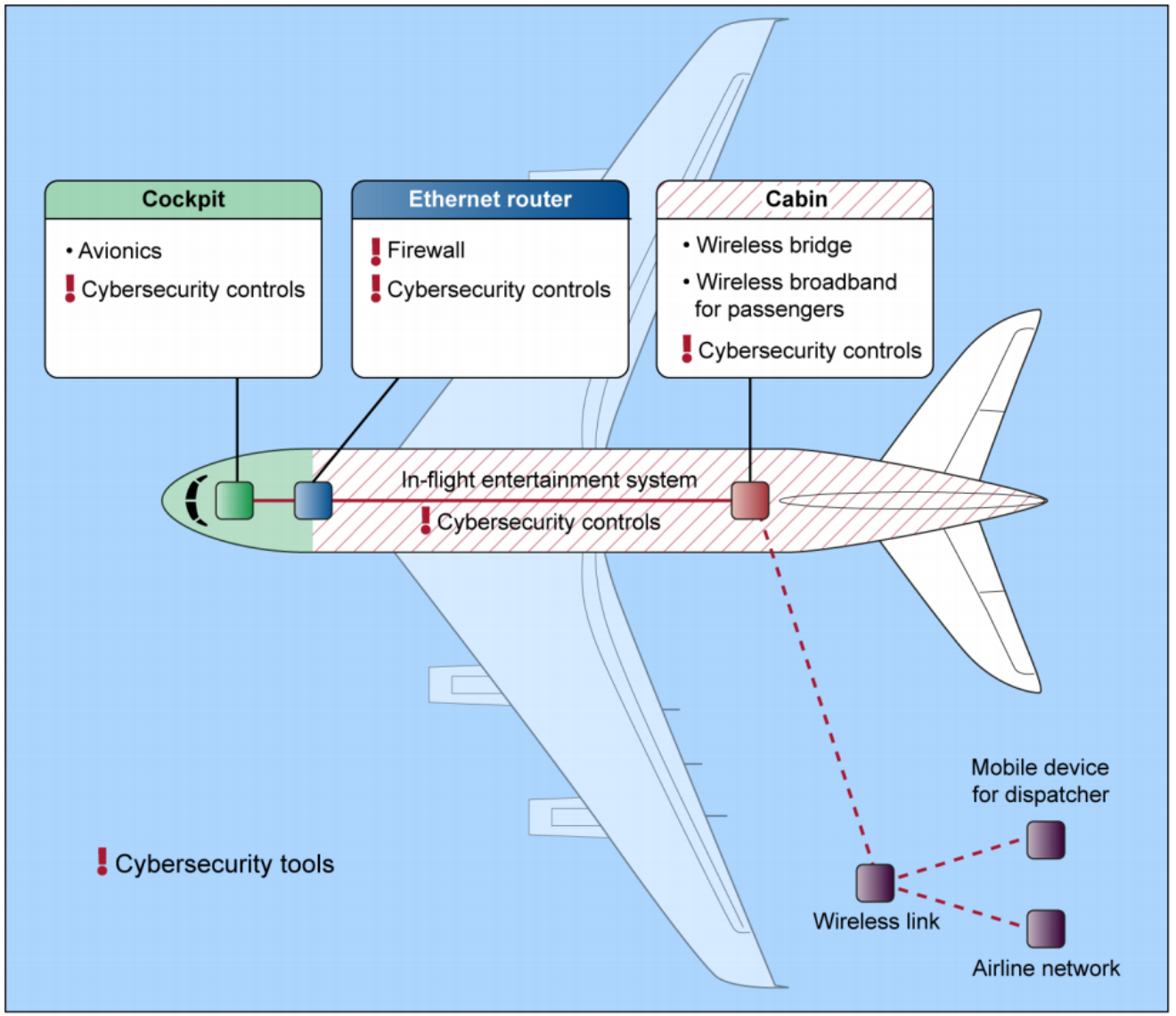
https://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip

Even expert/review boards don't always get it right.

U.S. Government Accountability Office (U.S. GAO)
GAO-15-370

"However according to FAA and experts we spoke to, IP networking may allow an attacker to gain remote access to avionics systems and compromise them-as shown in figure 4".

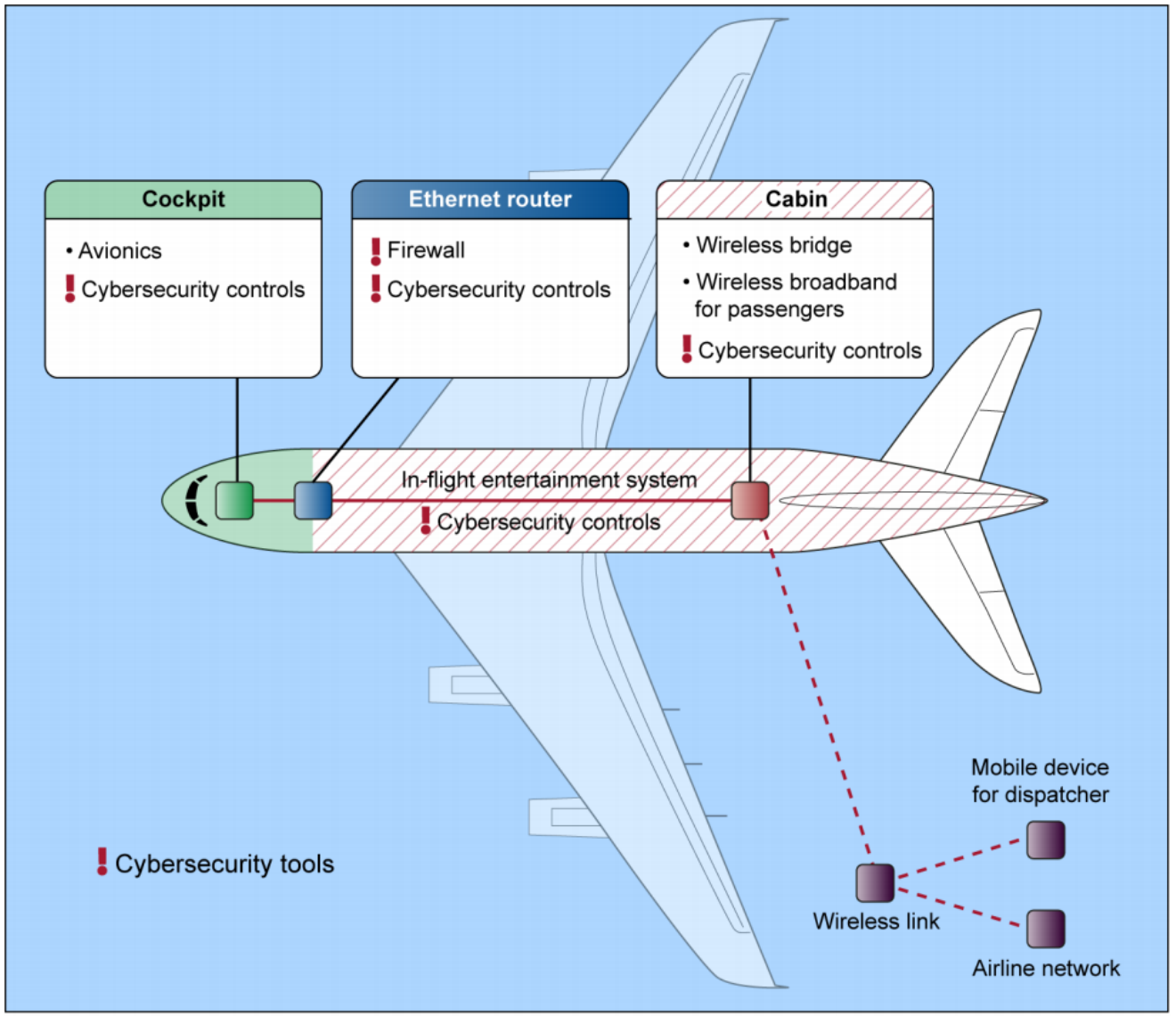
Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft



Source: GAO. | GAO-15-370

Accurate?

Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft



Source: GAO. | GAO-15-370

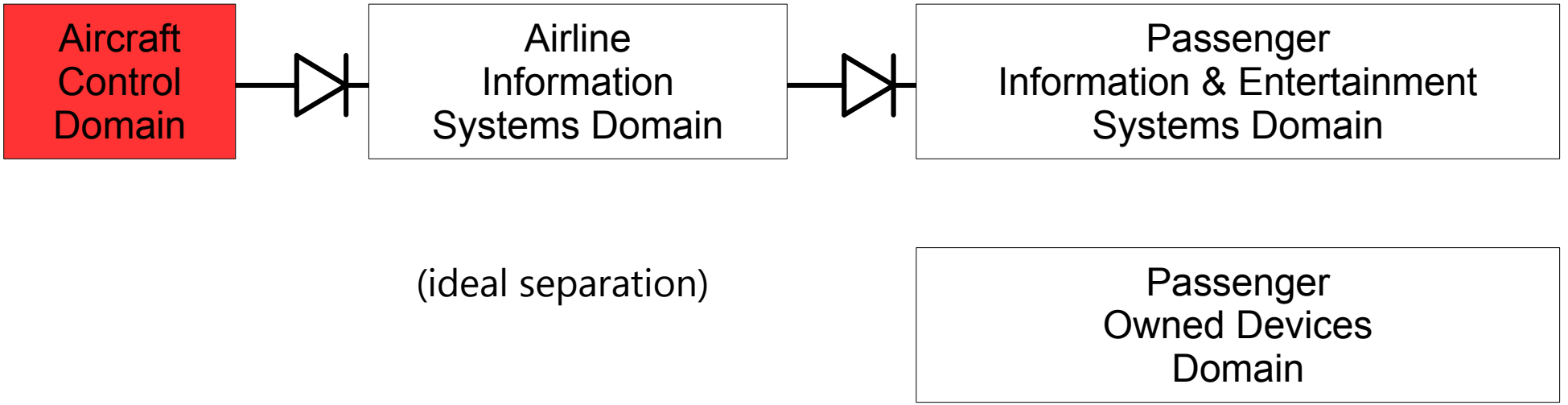
Not really...

the interaction between security and safety
accounts for all different trust domains
and interconnections

Aircraft Control Domain (ACD)

The ACD consists of systems and networks whose primary functions are to support the safe operation of the aircraft.

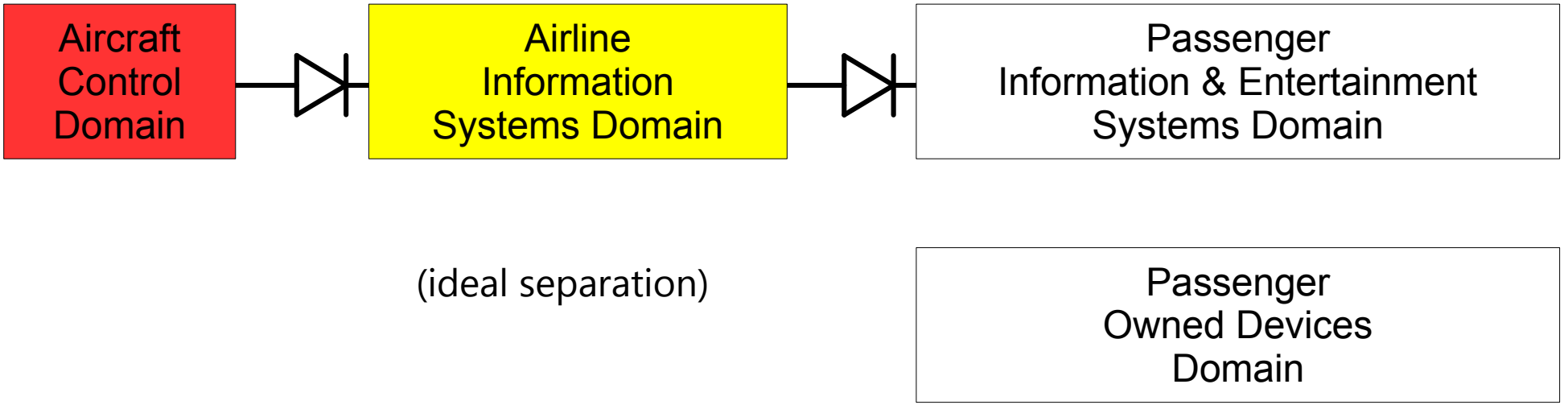
Example: Flight Management System (FMS)



Airline Information Services Domain (AISD)

The AISD provides general purpose routing, computing, storage and communications services for non essential applications. The AISD also provides routing between less critical domains.

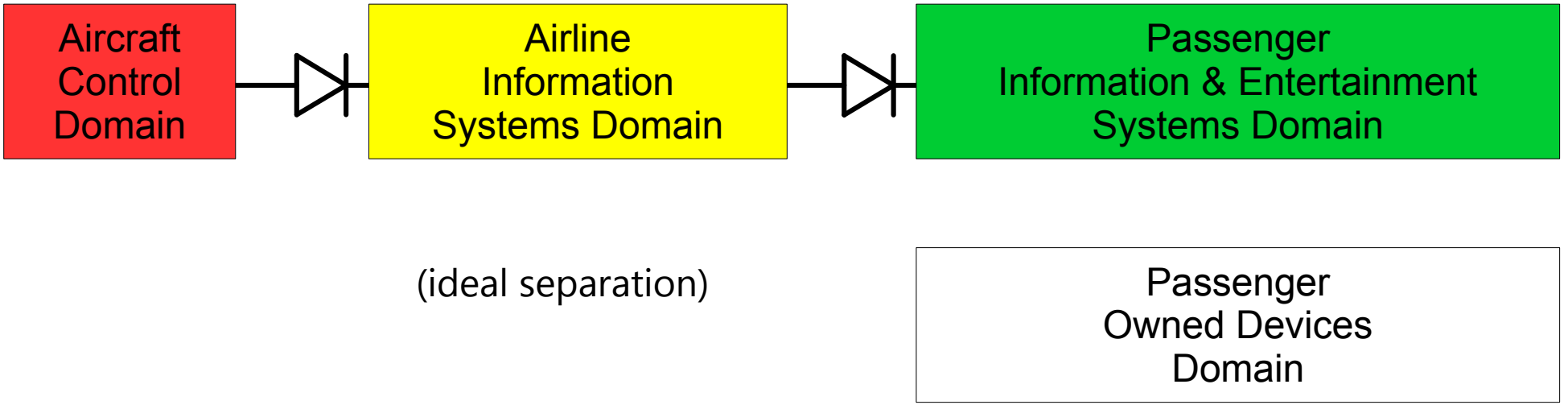
Example: Electronic Flight Bag (EFB), Airport surface communication link.



Passenger Information and Entertainment Services Domain (PIESD)

The PIESD is characterized by the need to provide passenger entertainment and network services.

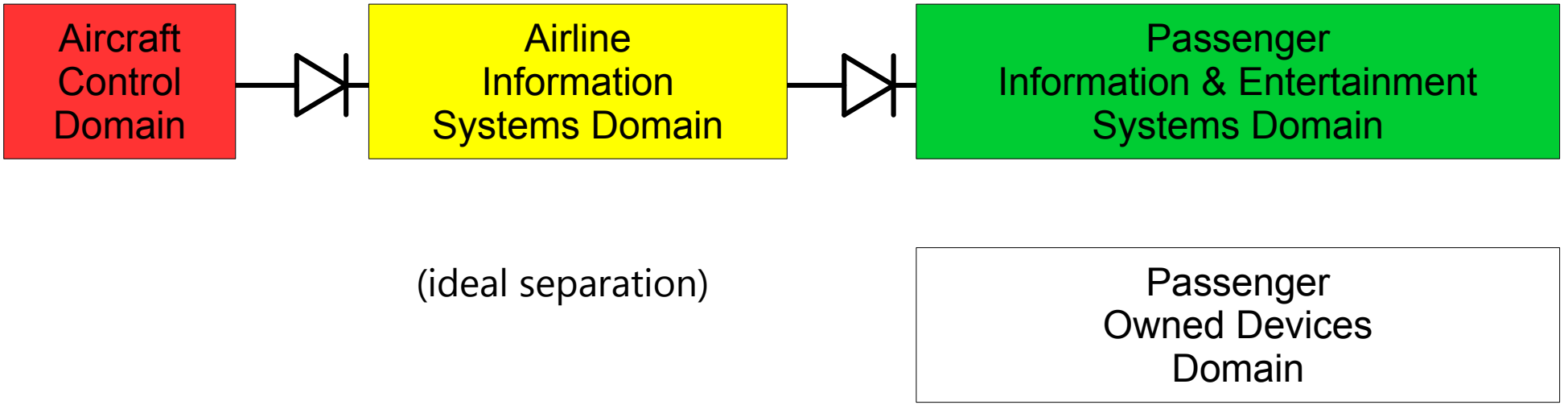
Example: In-Flight Entertainment (IFE), passenger GSM and WiFi.



Passenger Owned Devices Domain (PODD)

The PODD is defined to include only those devices that passengers may bring on board.

Example: mobile phones, laptops, tablets.



DO-178B/C: Software Considerations in Airborne Systems and Equipment Certification

Level A	→	failure is Catastrophic	(multiple loss of life)
Level B	→	failure is Hazardous	(injury or death)
Level C	→	failure is Major	(reduced safety margins)
Level D	→	failure is Minor	(no significant effect)
Level E	→	failure has No Effect	(no effect)

The associated software level or Design Assurance Level (DAL) is always determined from safety assessment.

Different DAL classifications can be assigned to entire systems, subcomponents of a system (e.g. daughterboard, discrete electronics, interconnections).

The DAL classification plays an important role, but it’s not the exclusive condition, in defining audit scope and prioritization.

AC 25.1309-1A: U.S. DoT/FAA Advisory Circular
System Design and Analysis (21/06/1988)

> "it is not feasible to assess the number or kinds of software errors, if any, that may remain after the completion of system design, development, and test."

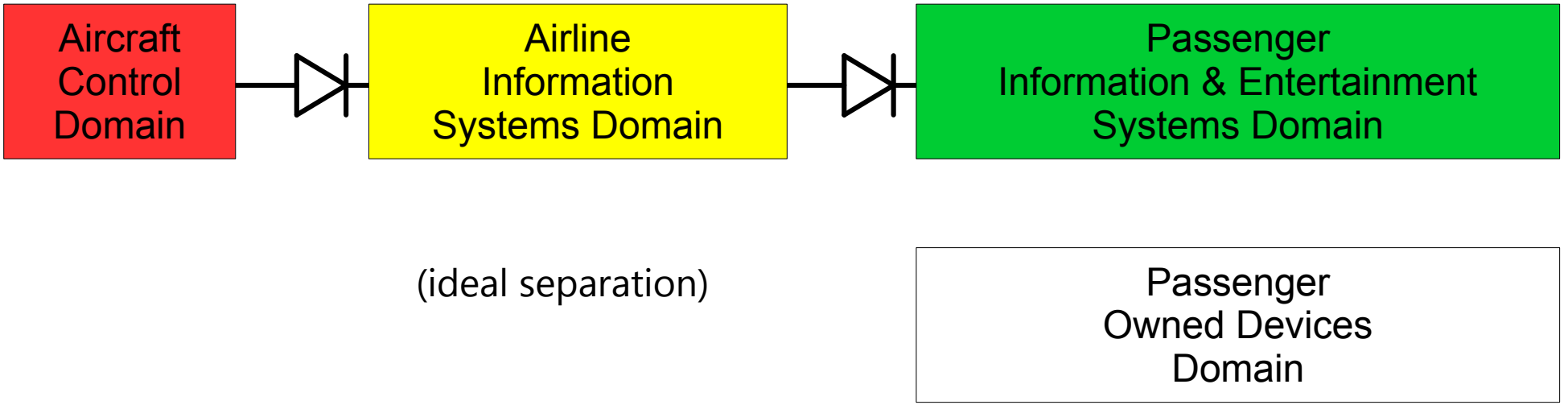
This means lots of assurance and **a lot of testing**.

There is a lot of theory and processes on assurance, we focus strictly on secure design, code audit and testing.

Security analysis focuses an all interconnections between different domains to ensure their separation.

Separation does not mean full isolation but rather ensuring unidirectional connections or tightly controlled exceptions.

Direct and indirect paths are evaluated according to risk analysis.



Typical security threats include:

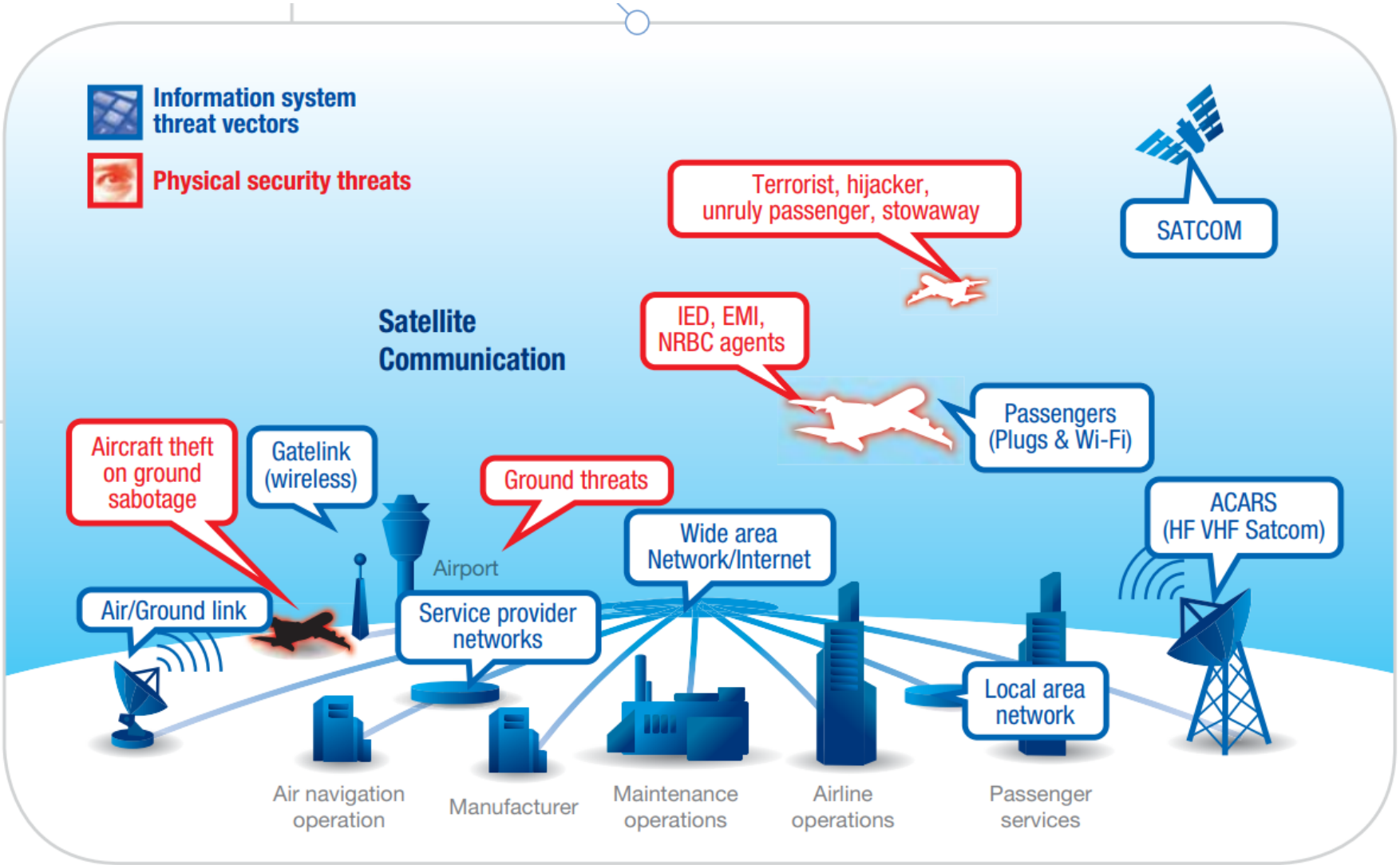
Field Loadable Software (FLS) shipment and data loading.

Maintenance procedures and connectivity (security of laptops, storage, peripherals, interfaces, etc.).

Aircraft to ground connectivity (Gate-link, SATCOM, WiFi, etc.).

Cabin links accessible to passengers (WiFi, Cellular, plugs).

Industrial/Access Control Systems employed in manufacturing.



ACARS: Aircraft Communication Addressing and Reporting System / **EMI:** Electromagnetic Interference / **HF:** High Frequency
IED: Improvised Explosive Device / **NRBC agents:** Nuclear Radiological Biological Chemical / **SATCOM:** Satellite Communication
VHF: Very High Frequency / **Wi-Fi:** Wireless Fidelity

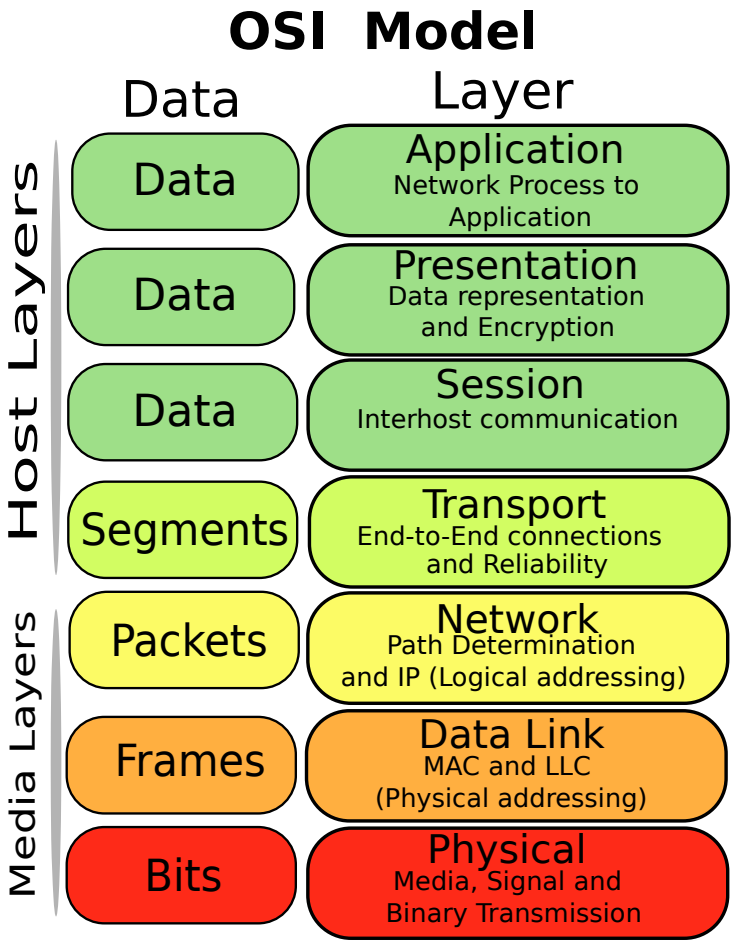
Airbus Technical Magazine FAST 51

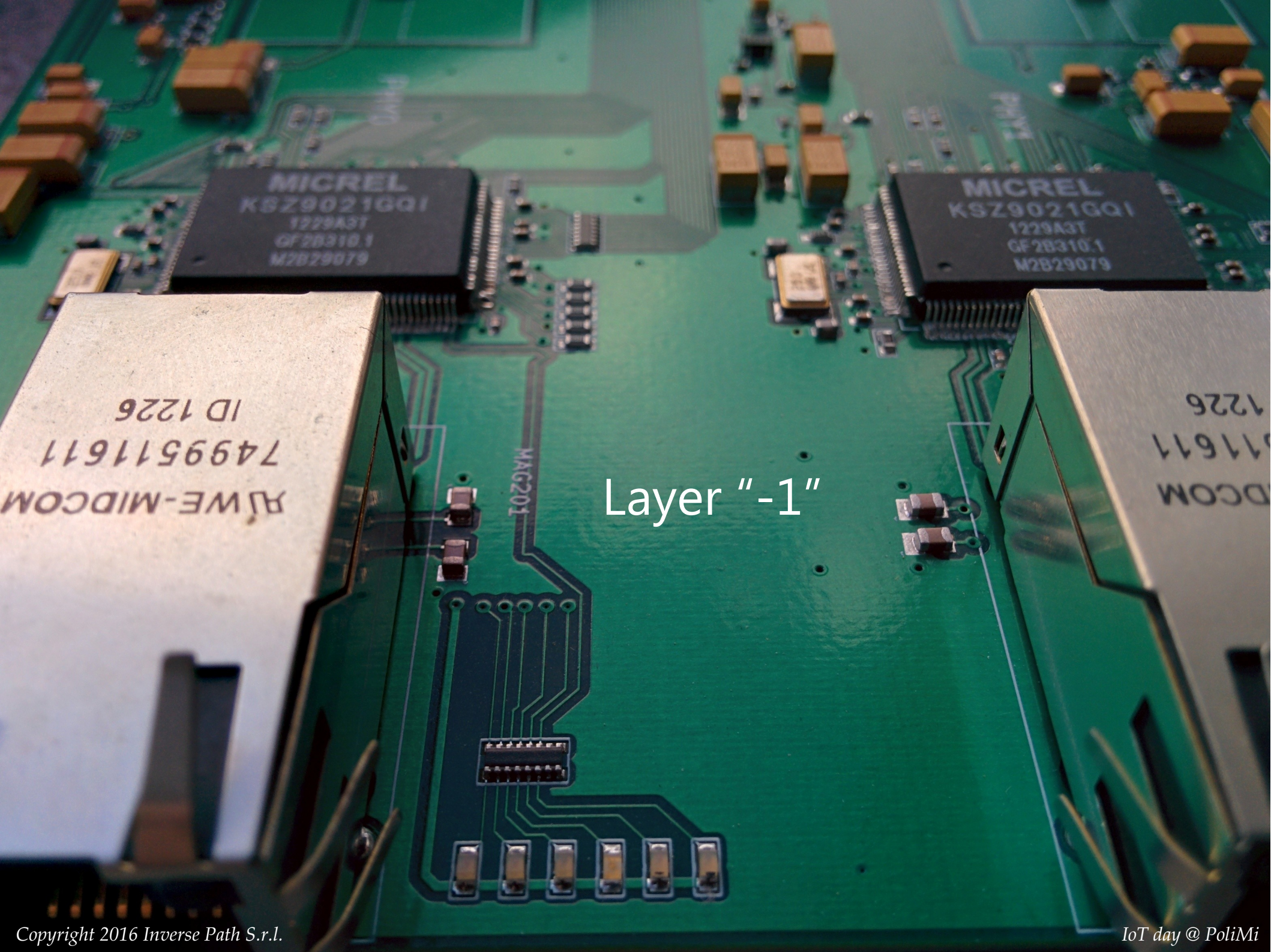
Typical components targeted during tests include:

- I/O ports (CAN, USB, Ethernet, Serial)
- Access points and routers (WiFi, Cellular, SATCOM, VPNs)
- Multiplexers
- Data diodes
- Custom interlocks

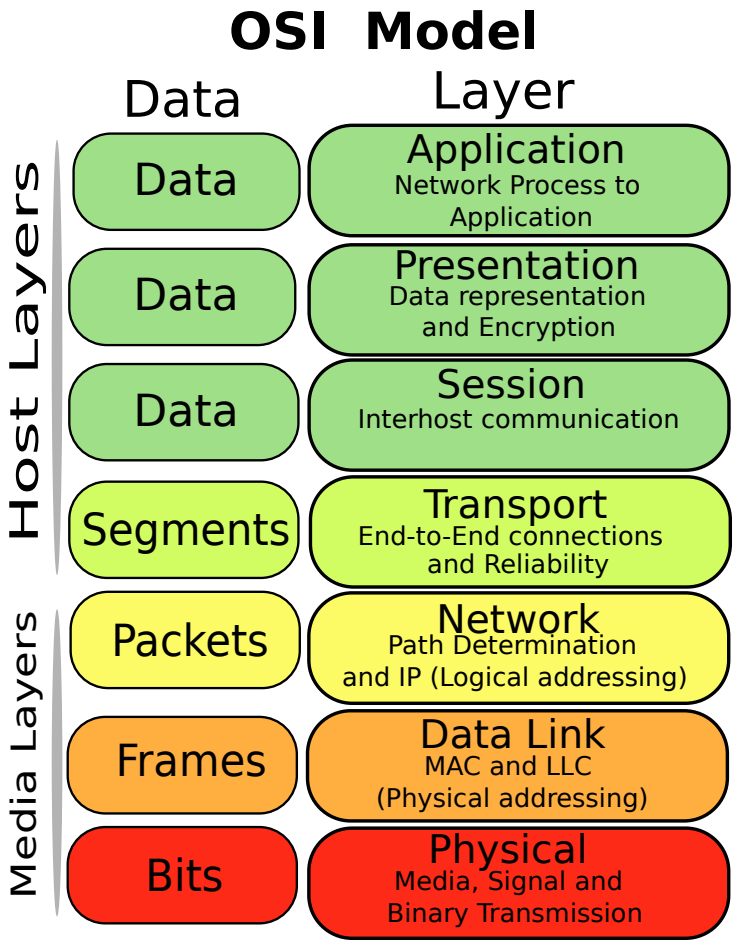
INVERSE PATH

Test all the layers!





Physical layer



Electrical schematics ->

Are there any (de)multiplexers ?

Are there any signal switches ?

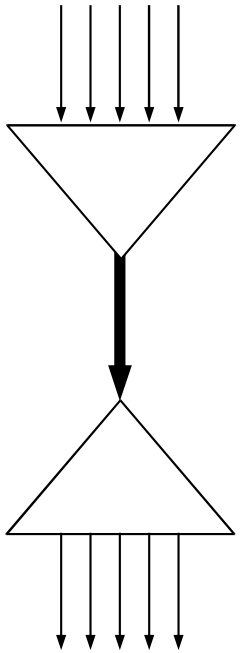
Are there any signal converters ?

Are there any signal extenders?

The attack surface is often expanded by such elements which are common in the industry.

INVERSE PATH

Multiplexing | Extenders | Converters



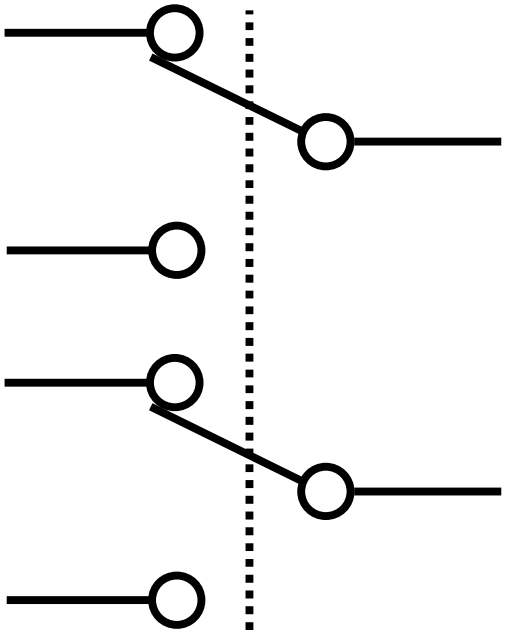
Various multiplexers and extender varieties exist (USB, Serial, Ethernet, …).

Typically time-division multiplexing allows cable reduction and weight loss, particularly appealing for aviation.

Extenders are sometimes required to extend cable maximum length requirements when physical layout demands longer connections than the standard.

Multiplexers and extenders can also be protocol converters.

Signal Switches



Switches can subvert the signal paths completely upon predetermined external or internal conditions, which all require careful evaluation.

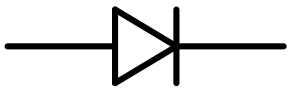
Their presence might affect the state and even protocols of internal interconnections or exposed ports.

Their identification and role within system schematics is a primary concern and target during security reviews.

Switches can be driven by simple relays or more complex conditions (e.g. see FSA9280A).

INVERSE PATH

Data Diodes



A data diode must ensure unidirectional data flow.

In fiber-optic networks it is common to simply remove send and receive transceivers for one direction.

On Ethernet receive only connections can be implemented through partial cable pairs or MAC <> PHY interconnection cutoffs.

The effectiveness for unidirectional assurance is always up to the specific design, implementation and capabilities of the PHYs and/or MACs on each side.

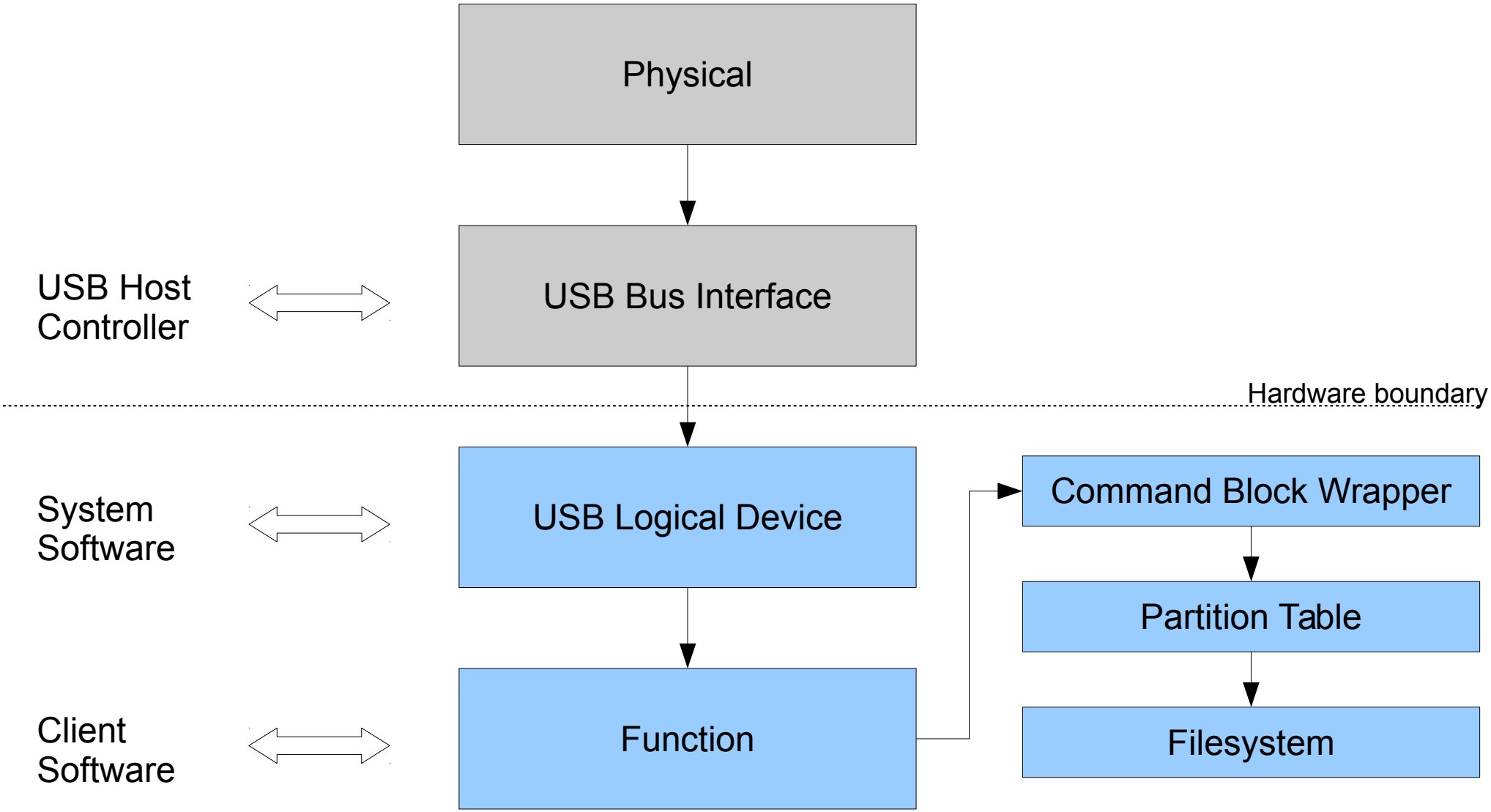
Great care must be taken to avoid malicious subversion in case of compromise.

Tools of the trade involve standard as well as non-standard equipment.

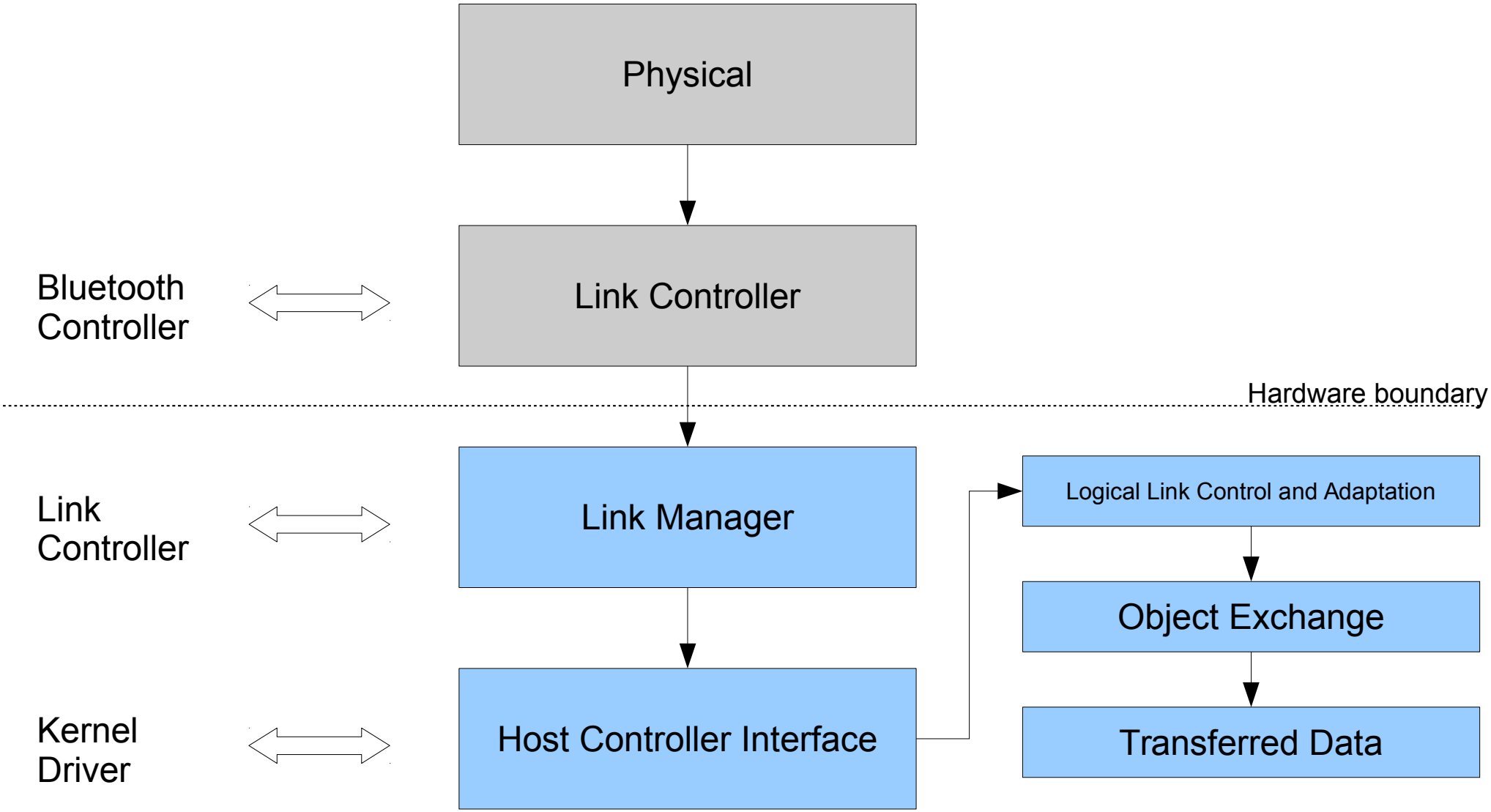
The ability to maximize any I/O port attack surface is a natural challenge in this field, often impeded by the inadequacy of tools.

This represents a classic hacking dilemma that any serious tester must overcome with identification, or development, of the right tool for the job.

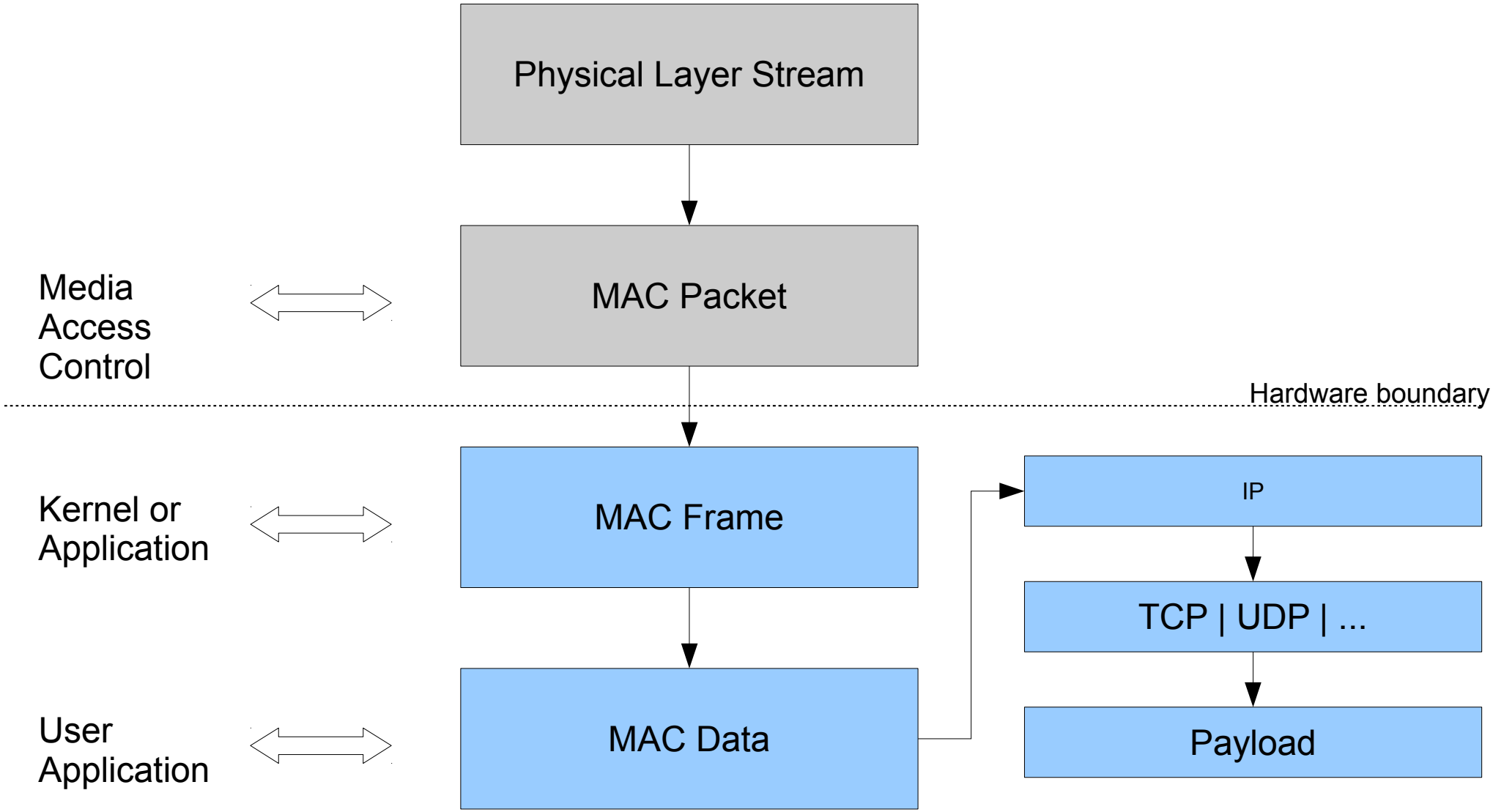
Example: USB



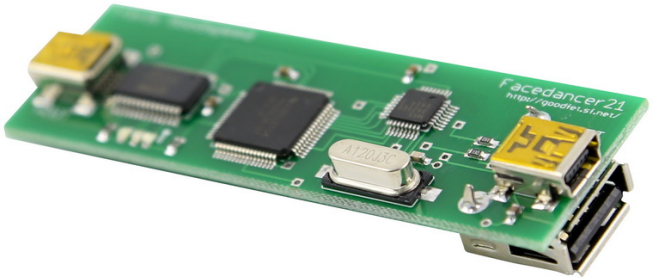
Example: Bluetooth



Example: Ethernet

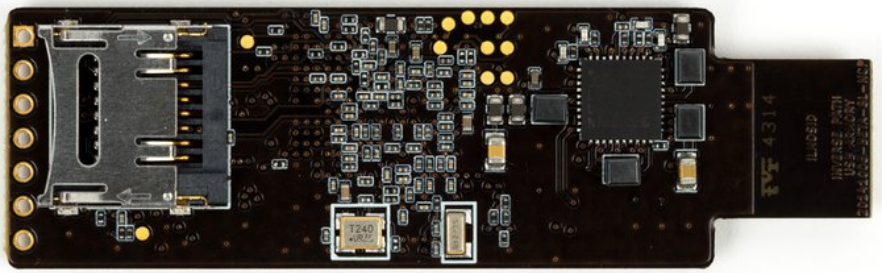


Low-level USB

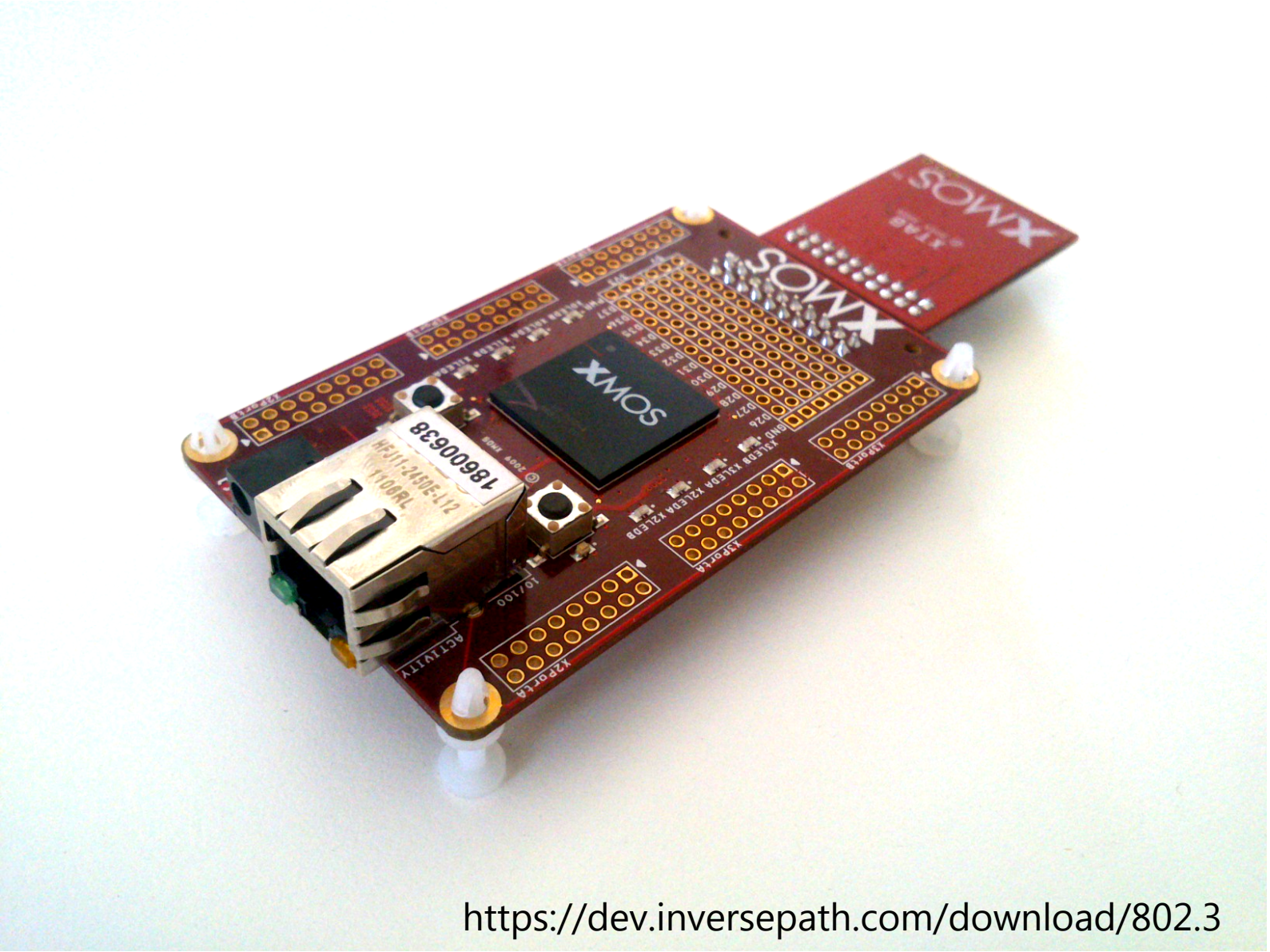


Facedancer
Travis Goodspeed

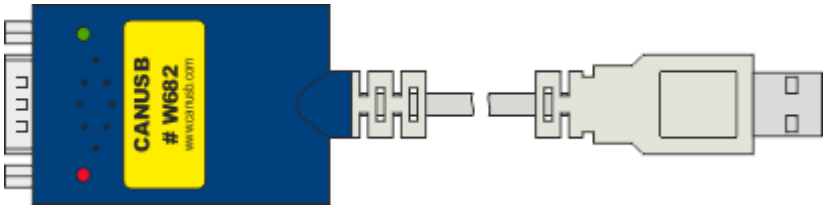
USB armory
Inverse Path



Low-level Ethernet



What about CAN Bus ?



https://dev.inversepath.com/download/serial_can_bus/
https://github.com/inversepath/serialcanbus

Example: Airbus CIDS (Cabin Intercommunication Data System)

"The system controls and displays cabin functions for passenger and crew. This includes cabin lightning, cockpit/cabin announcements, door status indication, emergency signals,..."

2x Director Interface Board (DIB) — IFE interface for
2x Director — signs panel, seat data

CIDS application software → DAL C, D
Smoke Detector Board → DAL B

http://www.techsat.com/fileadmin/media/pdf/DataSheets.engl/TechSAT-DS-CIDS-380-EN.pdf
http://www.redlogix.de/en/references/airbus-cabin-management-system-cids/

Social media and the information security community is always ready to jump on IFE security :).

The In-Flight Entertainment system is (understandably) everyone's favorite being the most visible/accessible aircraft IT system to passengers.

Code changes are tightly controlled and features are often "frozen" due to the consequences of re-certification process.

This is the reason why IFEs might run very old software and should always be irrelevant security wise (do not forget the domain separation we already covered).

Example: maintenance ports (e.g. USB).

Can a port (or even a cable in specific scenarios) be easily accessed by untrusted parties **or** untrusted/infected devices (regardless of trust level of the user)? If so it's **very likely** to be thoroughly tested.

In some cases physical security risk analysis also plays a role in scope definition.

Examples include storage ranging from floppy drives (yes I said floppy) to USB as well as data ports connected to specific peripherals.

Example: advanced attacks on multiplexers, extenders, converters.

Our Packet-In-Packet research was inspired by investigation of advanced attacks when such devices are used to multiplex, extend or convert payloads, or faction of payloads, from different domains.

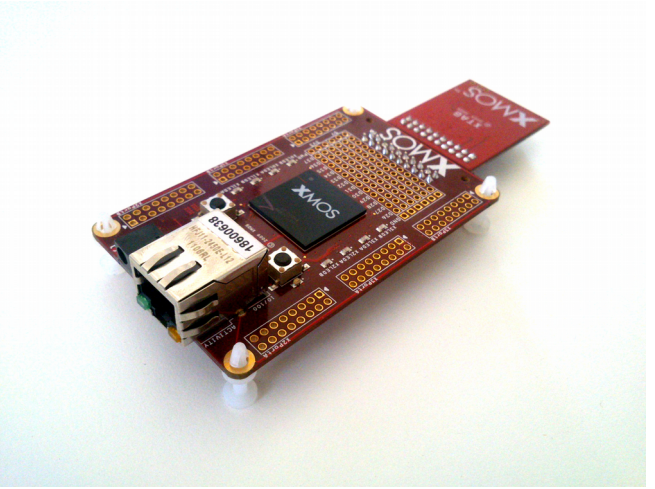
The possibility of affecting the timing of such devices or injecting out-of-band data has the potential of completely subverting their role in security domain separation.

Packet-In-Packet: packet **data** becomes packet **header + data**

INVERSE PATH

Packet-In-Packet on wired Ethernet through custom injector firmware

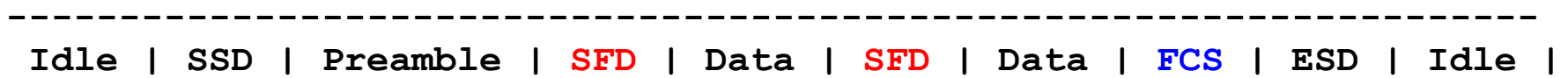
```
$ xrun --id 0 --io ethernet.xe
injector start
Enter payload
5555555555555d5001f1637f2ff0000000000108004500003900004000400616bb0
a0108020a010801029a029a0000000000000000500200004f55000000000000000
000000666f6f626172027123 2ab
Enter repeat count (0 = unlimited)
0
Sending payload unlimited times (83 bytes)
```



https://dev.inversepath.com/download/802.3/

INVERSE PATH

Packet-In-Packet on wired Ethernet




```
17:47:15.972801 00:1f:16:37:b1:3d > 00:22:6b:dc:c6:55, ethertype IPv4
(0x0800), length 1104: (tos 0x0, ttl 64, id 20574, offset 0, flags [none],
proto UDP (17), length 1090)
    192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
        0x0000:  0022 6bdc c655 001f 1637 b13d 0800 4500  ."k..U...7.=..E.
        0x0010:  0442 505e 0000 4011 62f1 c0a8 0001 c0a8  .BP^..@.b.......
        0x0020:  420a 927d 0035 0024 0000 c007 0100 0001  B..}.5.$........
        0x0030:  0000 0000 0000 0667 6f6f 676c 6503 636f  .......google.co
        0x0040:  6d00 0001 0001 0000 749c 9b85 0000 0000  m.......t.......
        0x0050:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        .....
        0x01f0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0200:  2165 c8fe 0000 0000 0000 0000 0000 0000  !e..............
        0x0210:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        .....
        0x0400:  0055 5555 5555 5555 d500 1f16 37f2 ff00  ..UUUUUU....7...
        0x0410:  1f16 37b1 3d08 0045 0000 3900 0040 0040  ..7.=..E..9..@.@
        0x0420:  0616 bb0a 0108 020a 0108 0102 9a02 9a00  ................
        0x0430:  0000 0000 0000 0050 0200 004f 5500 0000  .......P...OU...
        0x0440:  0000 0000 0000 0000 0066 6f6f 6261 7200  .........foobar.
```

Packet-In-Packet on wired Ethernet

```
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 10.1.8.2.666 > 10.1.8.1.666: Flags [S], seq 0:17, win 0, length 17
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)
12:04:34 IP 192.168.0.1.37501 > 192.168.66.10.53: 49159+ A? google.com. (1062)

12:04:34.442052 00:1f:16:37:b1:3d > 00:1f:16:37:f2:ff, ethertype IPv4
(0x0800), length 71: (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP
(6), length 57)
    10.1.8.2.666 > 10.1.8.1.666: Flags [S], cksum 0x4f55 (correct), seq 0:17,
win 0, length 17
        0x0000:  001f 1637 f2ff 001f 1637 b13d 0800 4500  ...7.....7.=..E.
        0x0010:  0039 0000 4000 4006 16bb 0a01 0802 0a01  .9..@.@.........
        0x0020:  0801 029a 029a 0000 0000 0000 0000 5002  ..............P.
        0x0030:  0000 4f55 0000 0000 0000 0000 0000 0000  ..OU............
        0x0040:  666f 6f62 6172 00                        foobar.
```

Regardless of the field of application being involved in security **design** rather than pure testing is (unfortunately) too rare of an opportunity but always a great one.

The potential for effective impact is vast, however the intrinsic nature of this industry renders effects to be seen only several years later.

The possibility of commenting on the choice of interfaces, storage mediums, diode design, interlocking layouts sometimes allows great reduction of attack surface at minimum cost and without compromising functionality.

Do we ever find issues? If so what is their severity and how are they mitigated?

Do we ever find issues? If so what is their severity and how are they mitigated?

In our experience we se that [redacted] and [redacted], more interestingly [redacted] is [redacted].

;-)

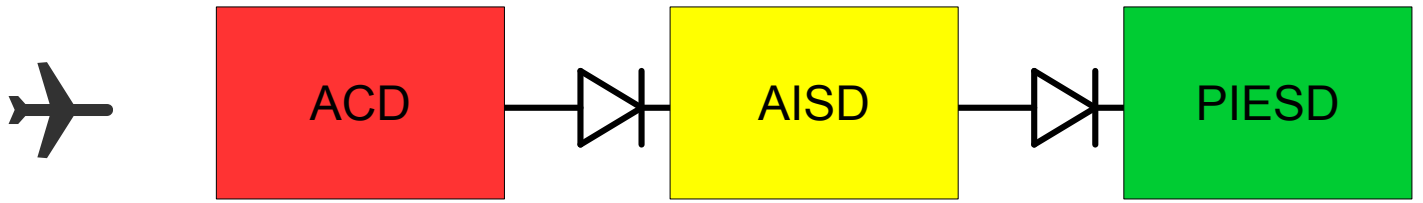
How does the avionics security culture compare to automotive?

Regulations and assurance procedures are much more pervasive and have a longer history in aviation safety and security, also in relation to information technology systems.

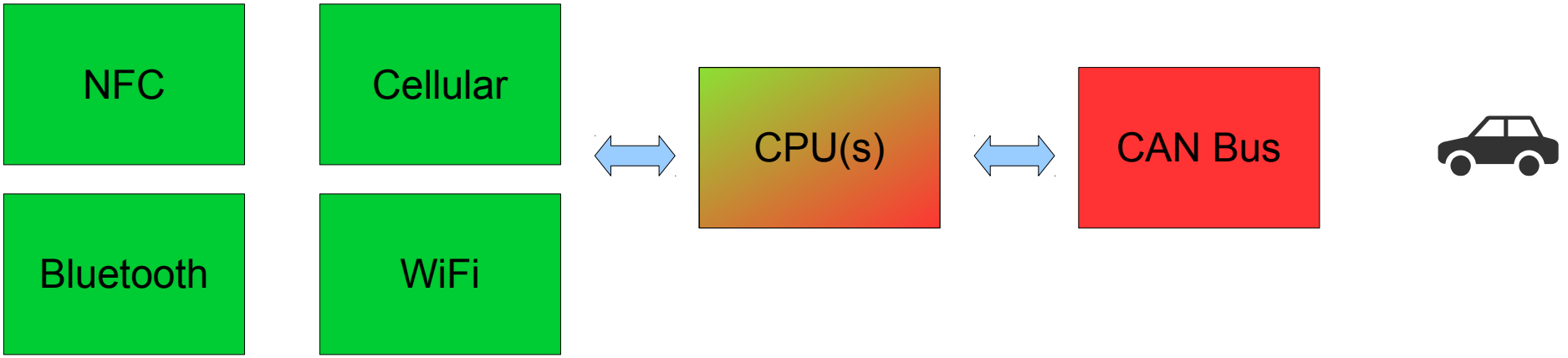
Automotive security has been classically oriented against theft and is now taking the spotlight at 360° degrees.

In automotive assessments physical possession and manipulation of a target device (e.g. ECU, head unit) is more likely, has more impact and takes a big role in security assessments.

Domain separation in automotive and avionics is still dramatically different as of today (with few notable exceptions a.k.a Tesla).



vs.



In conclusions avionics security is a field where design and testing take much greater roles than the common perception, even the one of the information security community.

Having said that there is a lot to improve in all areas, particularly in active participation and confrontation in the public security community.

A lot of work/research is still done under the curtains and one of the goals of this presentation is to improve this.

Thank You!

Q & A

andrea@inversepath.com