Dependability and Security in Critical Transportation Industries

CERTS Workshop - Keynote - 2018-05-25

Michael Paulitsch

Legal Notices and Disclaimers

This presentation contains the general insights and opinions of Intel Corporation (“Intel”). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

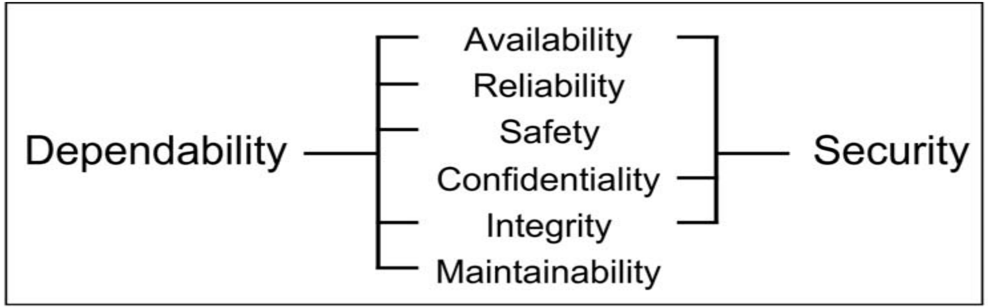
No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

What is Dependability & Security?

Dependability an integrating concept that encompasses the following **attributes**:



- Availability - readiness for correct service
- Reliability - continuity of correct service
- Safety - absence of catastrophic consequences on the user(s) and the environment
- Integrity - absence of improper system alteration
- Maintainability - ability for a process to undergo modifications and repairs

Security: composite of the attributes of confidentiality, integrity, and availability, requiring the concurrent existence of 1) availability for authorized actions only, 2) confidentiality, and 3) integrity with “improper” meaning “unauthorized”

Laprie et al 2004 :

Safety & Security

Safety: « The state of being free of risk or danger and the means/actions to obtain this state ».

Security: « The protection of information systems from theft or damage, as well as from disruption or misdirection of the services they provide ».

The « digital transformation » of embedded critical systems requires increased attention on cyber security to avoid operational disruption (availability), access to user confidential data, and ensure safety is not impaired (system integrity + availability).

Example: Safety Assurance Levels in Aerospace and Railway (e.g. DO-178C/ED-12C, EN 50129, …)

Criticality

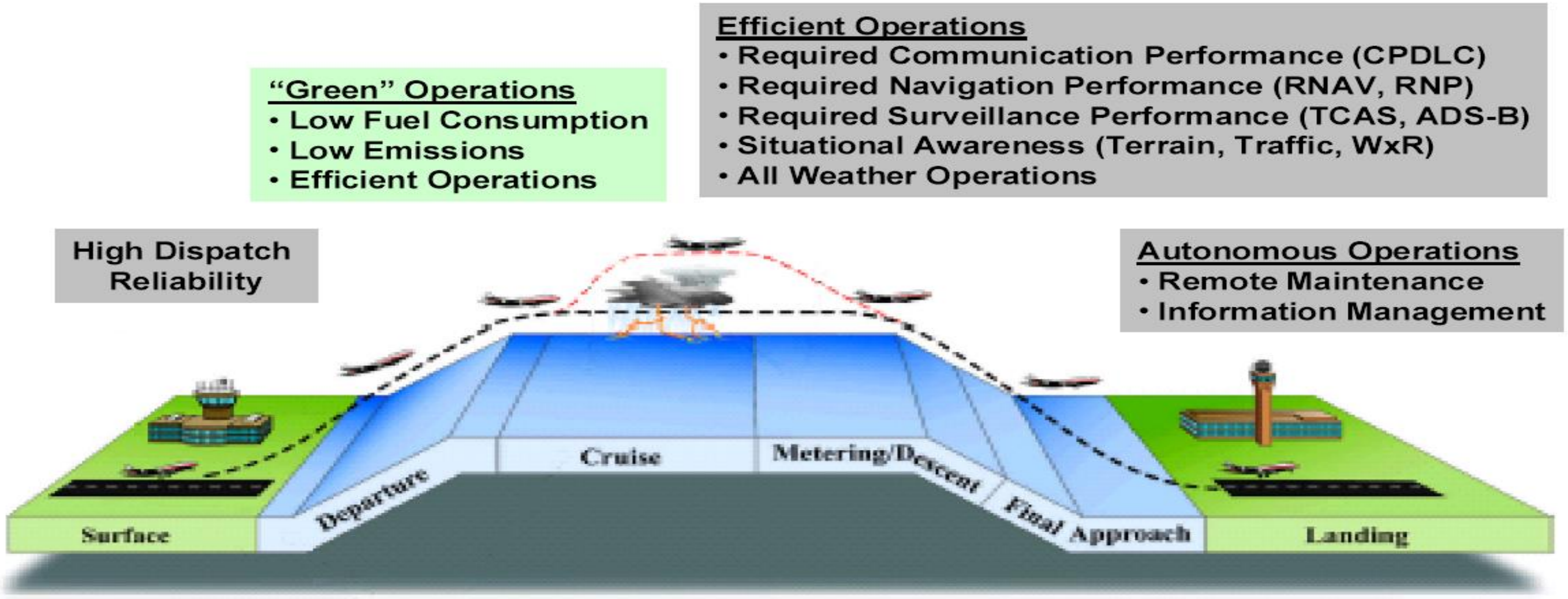
Software/hardware whose anomalous behaviour would cause or contribute to a failure of system function resulting in a failure condition for the aircraft / railway system that is:

Level A - Catastrophic 10^{-9} failures/hour	**SIL 4** 10^{-8} failures/hour
Level B - Hazardous/Severe-Major	**SIL 3**
Level C - Major	**SIL 2**
Level D - Minor	**SIL 1**
	SIL 0
Design Assurance Level E - No Effect	**Safety Integrity Level - SIL 0 (non-SIL)**

Avionics

Electronics in Airplane

Avionics - Drivers



Source: Rockwell Collins

Trends in Aerospace

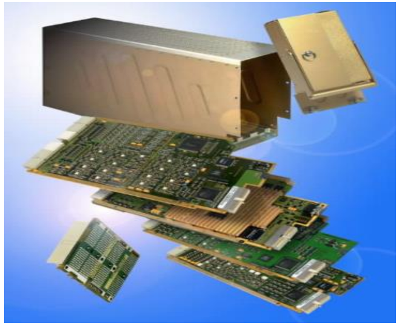
Trend towards new and additional IT-services and denser functional integration:

Demand for new and additional IT-services on aircraft itself and between aircraft and ground

- Integrate formerly physically separated functions onto one platform
- New failure modes and failures
- New threats and vulnerabilities

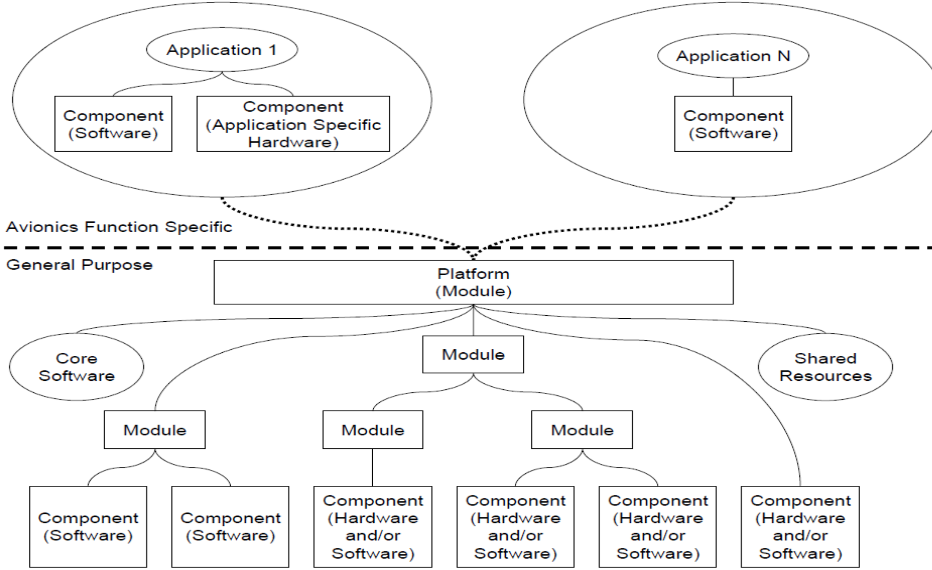
Trend Towards Integrated Modular Avionics (IMA)

Due to weight constraints integration of multiple aircraft functions (of possibly different criticality) onto common platforms is an ongoing architectural trend in aerospace



A380 IMA components

Source: Airbus © Airbus



Relationship of IMA applications and HW/SW Modules

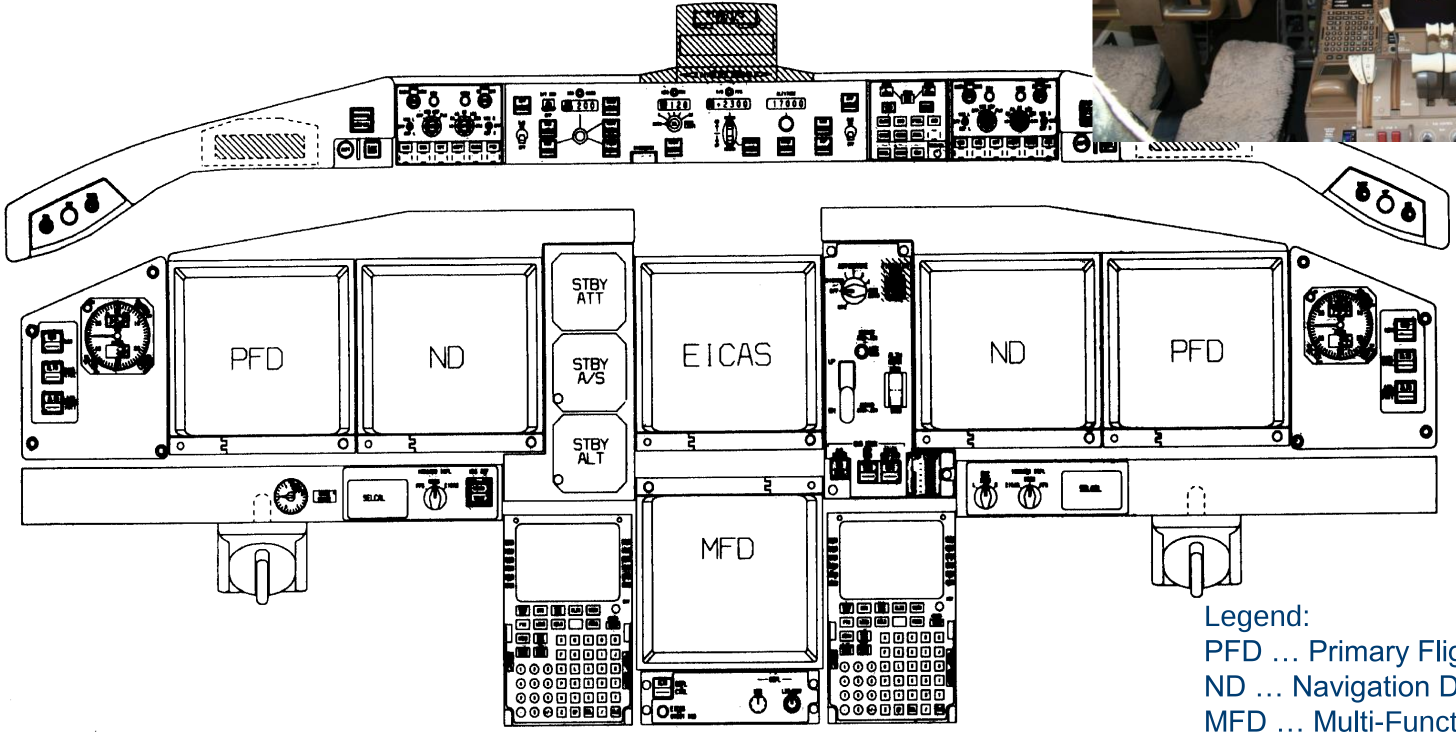
Source: ARINC297 © ARINC

Mixed-Criticality System in Industry – What’s it?

Multiple criticalities (residing) on same platform

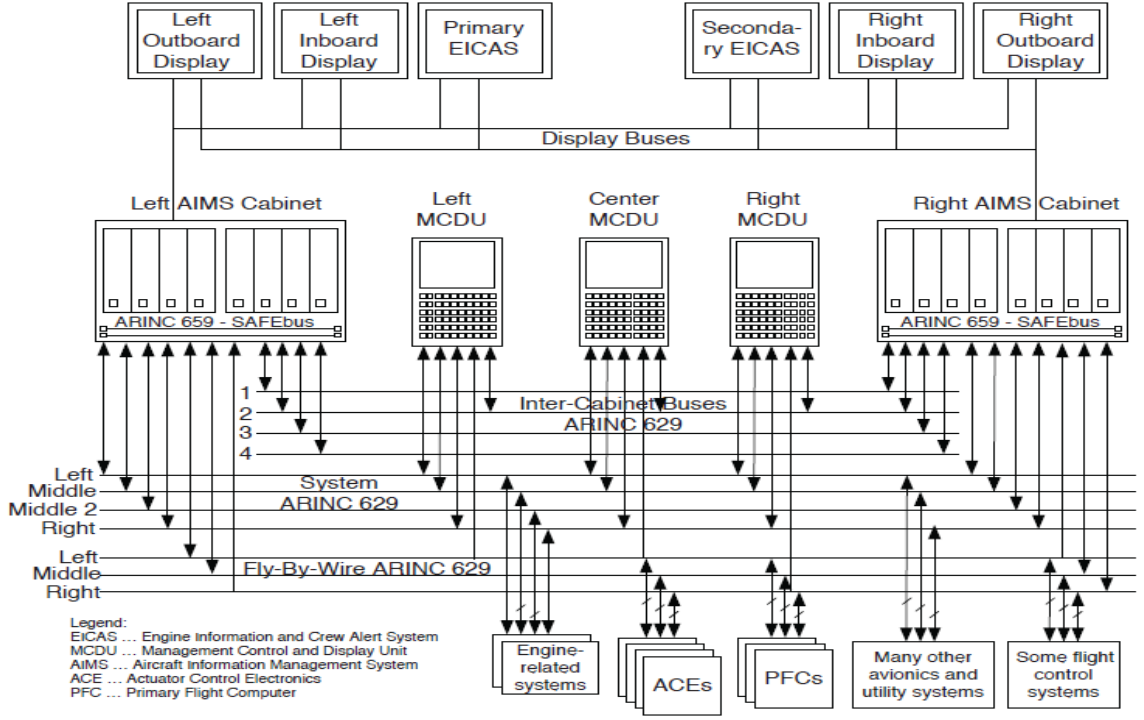
- Key requirement for platform: Platform needs to fulfill safety requirements at minimum of **highest safety** requirement of application. Security criticality requirements may be derived from safety requirements or from security data separation.
- Criticalities are **assigned by safety or security process** and typically don’t change during operation
- Safety: Chosen independence between applications to minimize interaction between otherwise independent “safety chapters” (system level safety analysis extremely complicated w/o this requirement).
- Security: co-habitance of different security levels needed for cost reasons or because of inherent security function (gateway, firewall)
- Deployed for many years in aerospace (B777, B787, A380, A350, E170/175, E190/195, …) under the name Integrated Modular Avionic (IMA) systems

Aircraft Cockpit



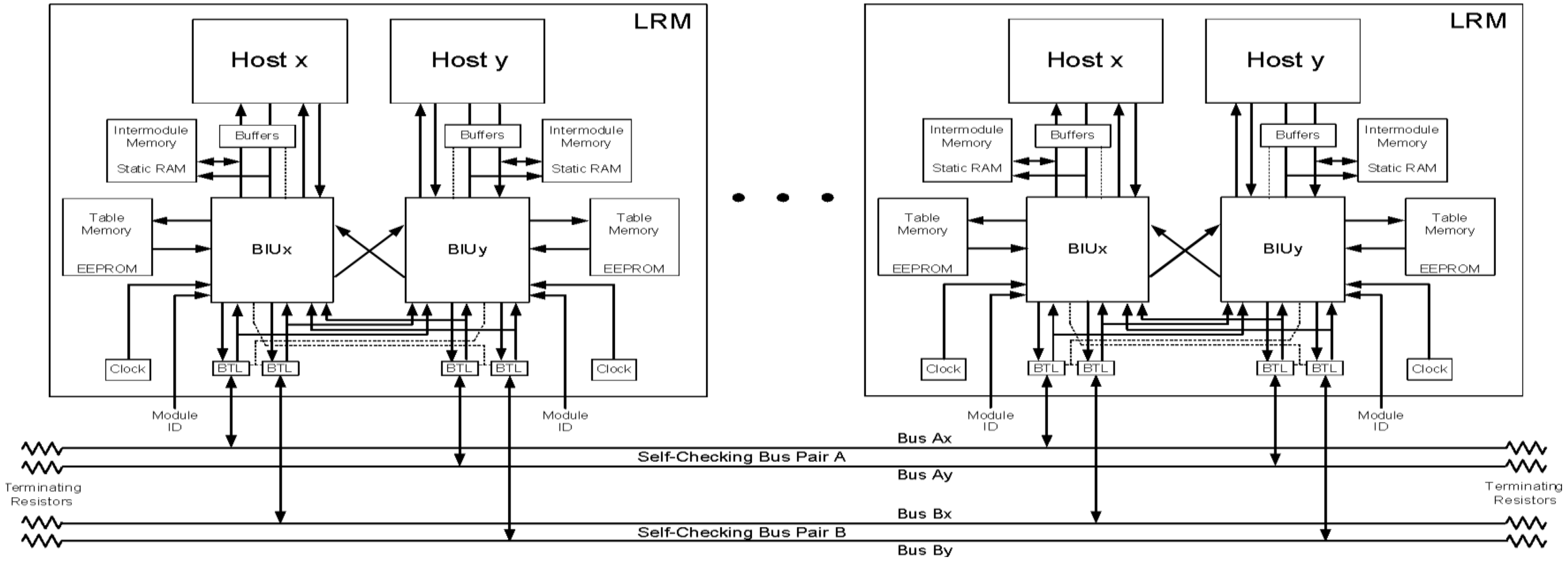
Legend:
PFD … Primary Flight Display
ND … Navigation Display
MFD … Multi-Function Display
EICAS … Engine Info & Crew Alert System

Boeing 777 – Avionics Level
Real-Life Mixed Criticality System



Boeing 777 – Avionics – Computer Level

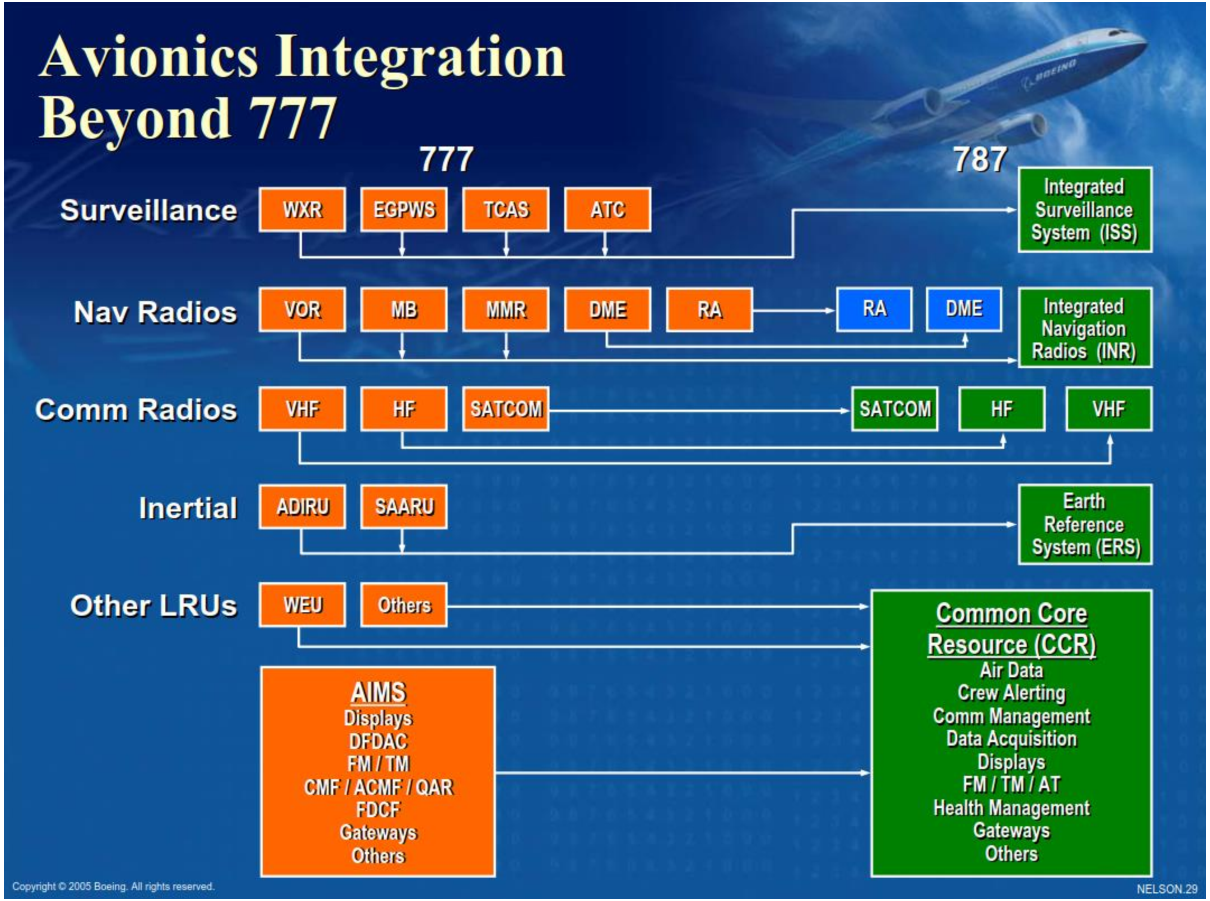
Avionics based on ARINC629 system bus and ARINC659 (SafeBus).



Boeing 787

Increased functional integration

© Boeing



Tim Nelson, 787 Systems and Performance, Boeing, 2005

Boeing 787

Core Computing System (core IMA platform):

- WindRiver VxWorks (ARINC 653)
- ARINC664 – Ethernet
- High-integrity compute

Cockpit looks nearly the same to B777 … but only at first glance …

- Additional functions in cockpit (e.g.): EFB … Electronic Flight Bag

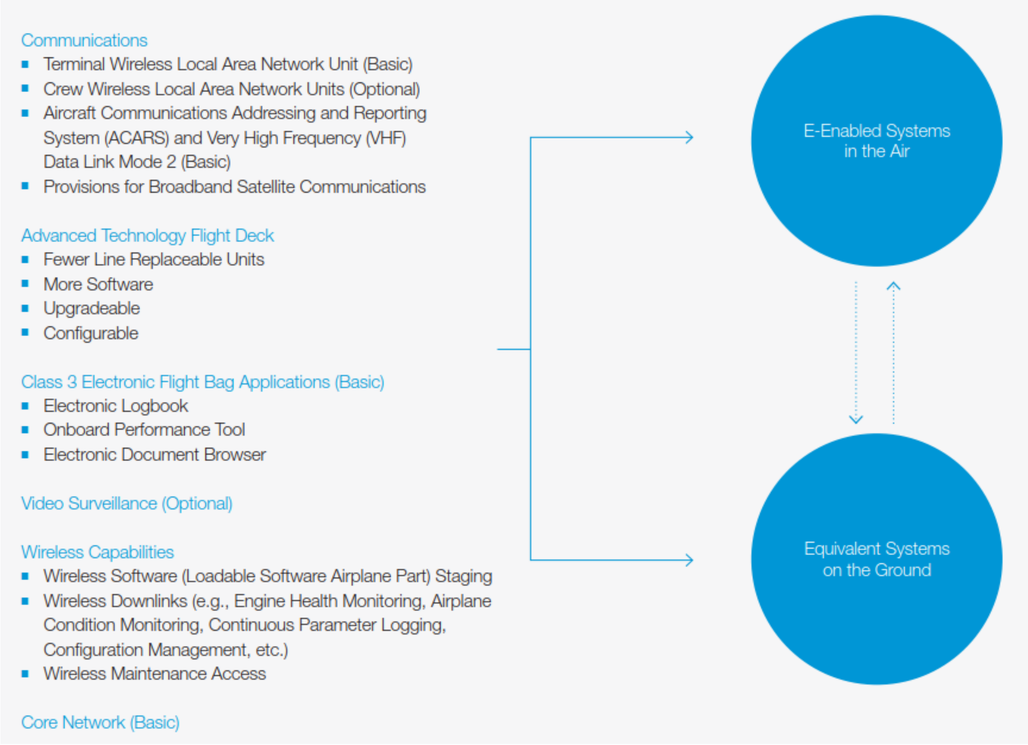
© Engadget

EFB … Electronic Flight Bag © Boeing

B787: E-Enabled Capabilities

“the e-enabled tools on the 787 will be a dramatic change from any other commercial airplane previously operated []. These tools promise to change the flow of information and create a new level of situational awareness that airlines can use to improve operations. At the same time, the extensive e-enabling on the 787 increases the need for network connectivity, hardware and software improvements, and systems management practice []. […] Airlines have the option to include a wireless network for maintenance access, enabling airline back-office teams to remotely deploy software, parts, data, charts, and manuals to airplanes with minimal hands-on mechanic involvement. ”

K. Gosling, E-Enabled Capabilities of the 787 Dreamliner, Aero Quarterly, 01/2009.



New Connectivity: New Threats

How to Hack Into a Boeing 787

Wednesday, February 20, 2008

FOX NEWS

Last month, technology news sites and blogs breathlessly reported on a Federal Aviation Administration document suggesting that Boeing's new 787 Dreamliner passenger jet may be vulnerable to computer hackers.

Read more: http://www.foxnews.com/story/0,2933,331088,00.html#ixzz2WgwFJQq6

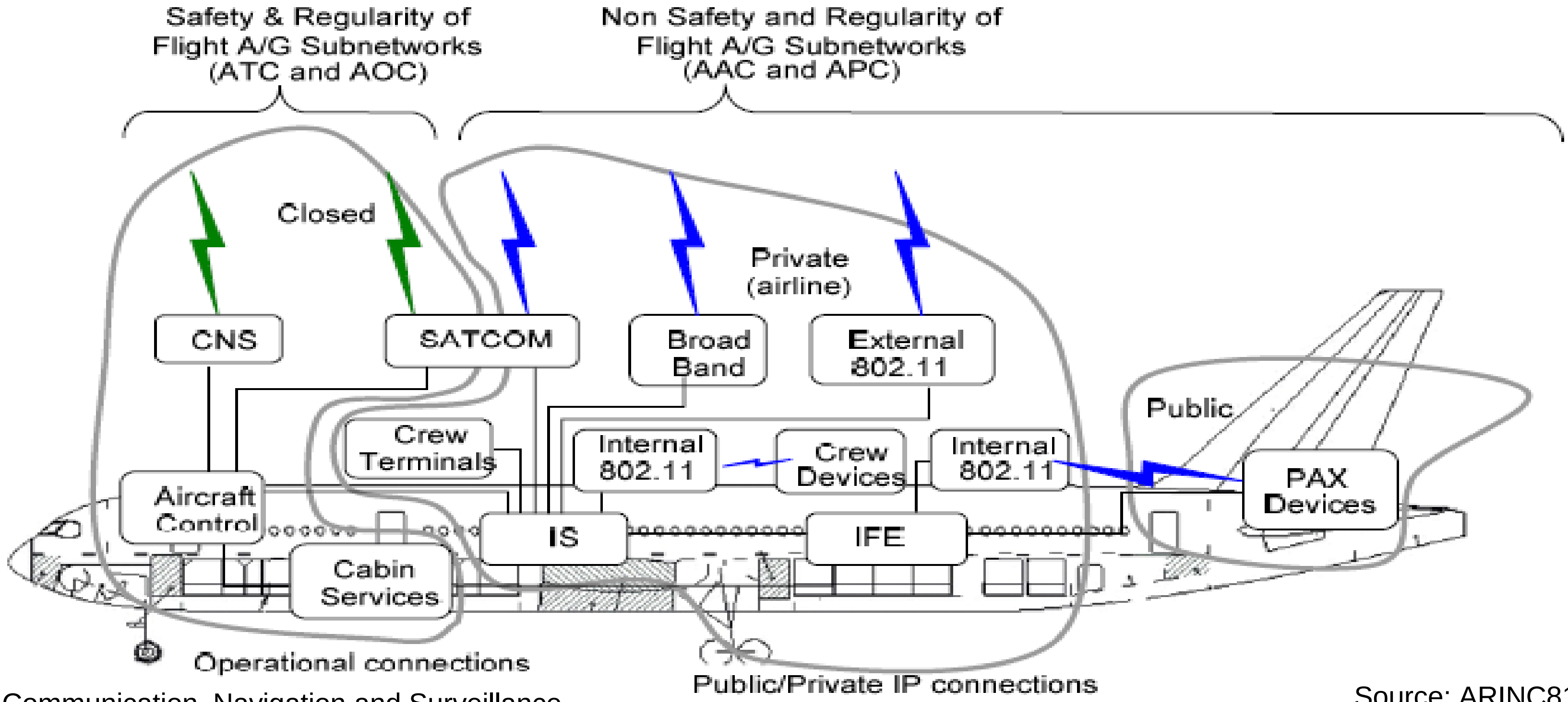
….

The FAA was specifically concerned that a passenger could use the on-board entertainment network, which personal laptops can plug into, to access the plane's navigation system and disable or take over the plane

Read more: http://www.foxnews.com/story/0,2933,331088,00.html#ixzz2Wgw9n3LC

Just because the architecture is different,
it does not mean automatically that it is vulnerable …

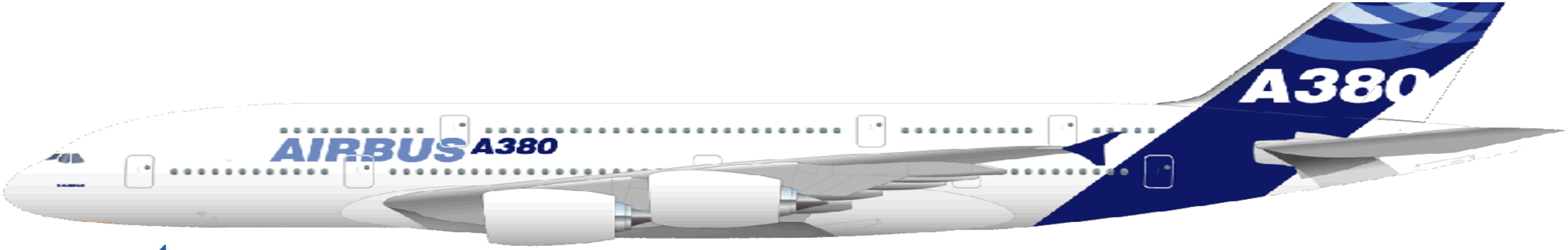
Example: Communication Requirements in Aircraft



CNS Communication, Navigation and Surveillance
IS Information Systems
IFE In-light Entertainment

Source: ARINC811

Communication Domains & Means in Civil Aircrafts



Criticality

Avionics | A/C Ops ↔ Cab Ops ↔ IFE

Ethernet 802.3 Phy + ARINC 664 MAC (AFDX)
10 / 100 Mbit/s

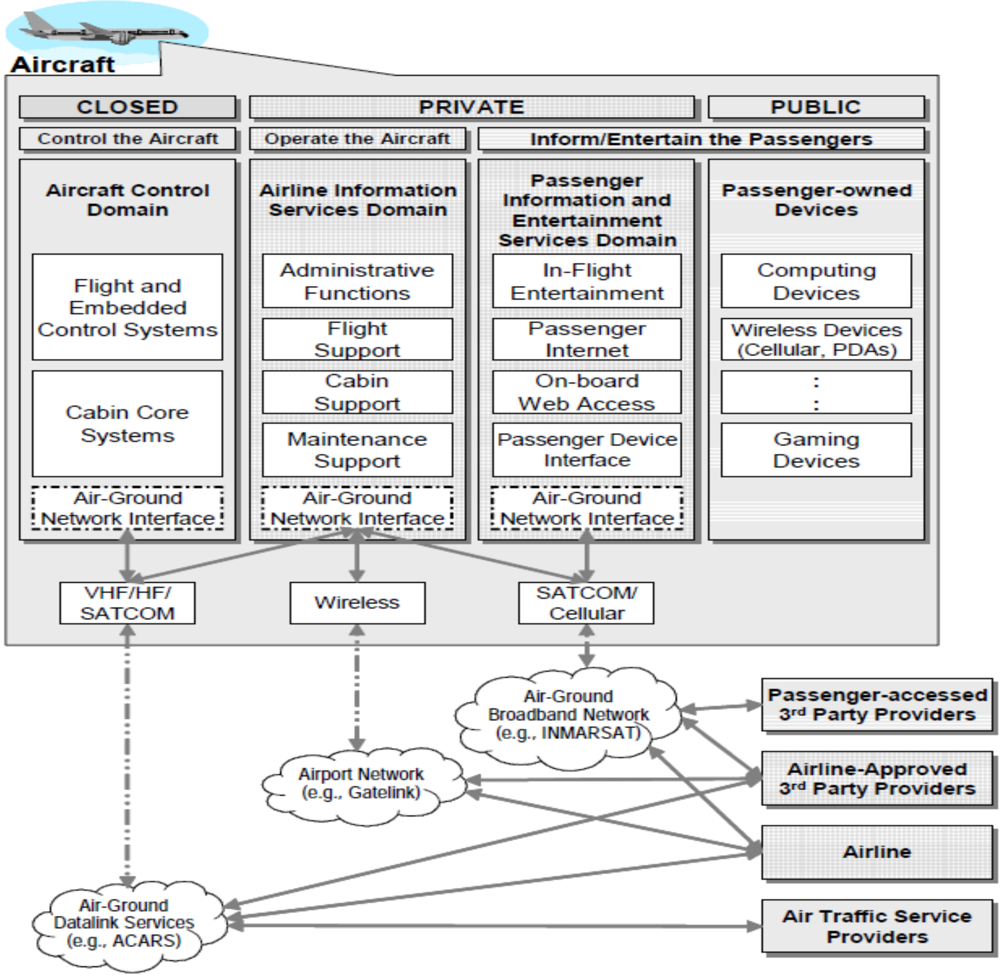
ARINC 429, CAN,….

Ethernet compliant networks
Electrical Physical Layer
10 / 100 Mbit/s
Ethernet PHY+Proprietary MAC

CAN,….

Ethernet / IP
Optical Physical Layer
1 Gbit/s
IP / TCP Protocols
Availability + Real-time

Aircraft Network Domains and Interactions: Another View



Source: ARINC811

How to Achieve Availability and Integrity in a Mixed-Criticality System?

Correctness of implementation important for safety and availability

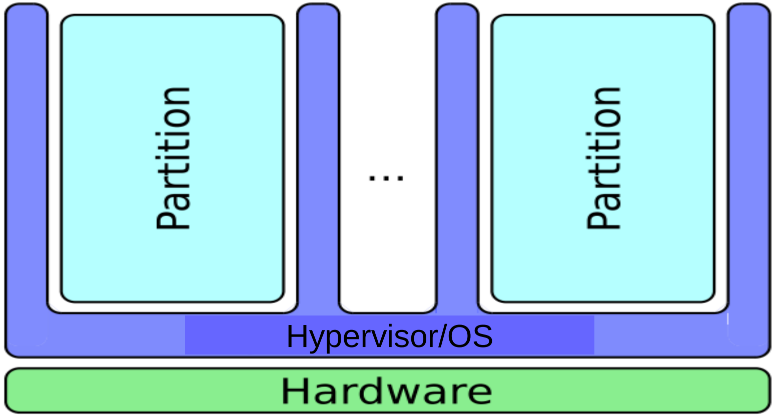
Examples of High-Assurance Requirements

- Domains need to fulfill **separation** requirements despite possible integration on same hardware to ensure proper item integrity and availability
- **Controlled information flow**: Communication between domains need to fulfill rules to ensure proper protection of functions – stronger focus on
  - Integrity and availability of functions
  - Authorized flow definition

Partitioning

Is a concept for spatial and temporal separation/segregation of functionally independent components:

- Prevents interference between two components
- Incremental development



Types of partitioning

- Time partitioning: temporal aspect
- Space partitioning: memory aspect
- I/O partitioning: time and space partitioning for I/O

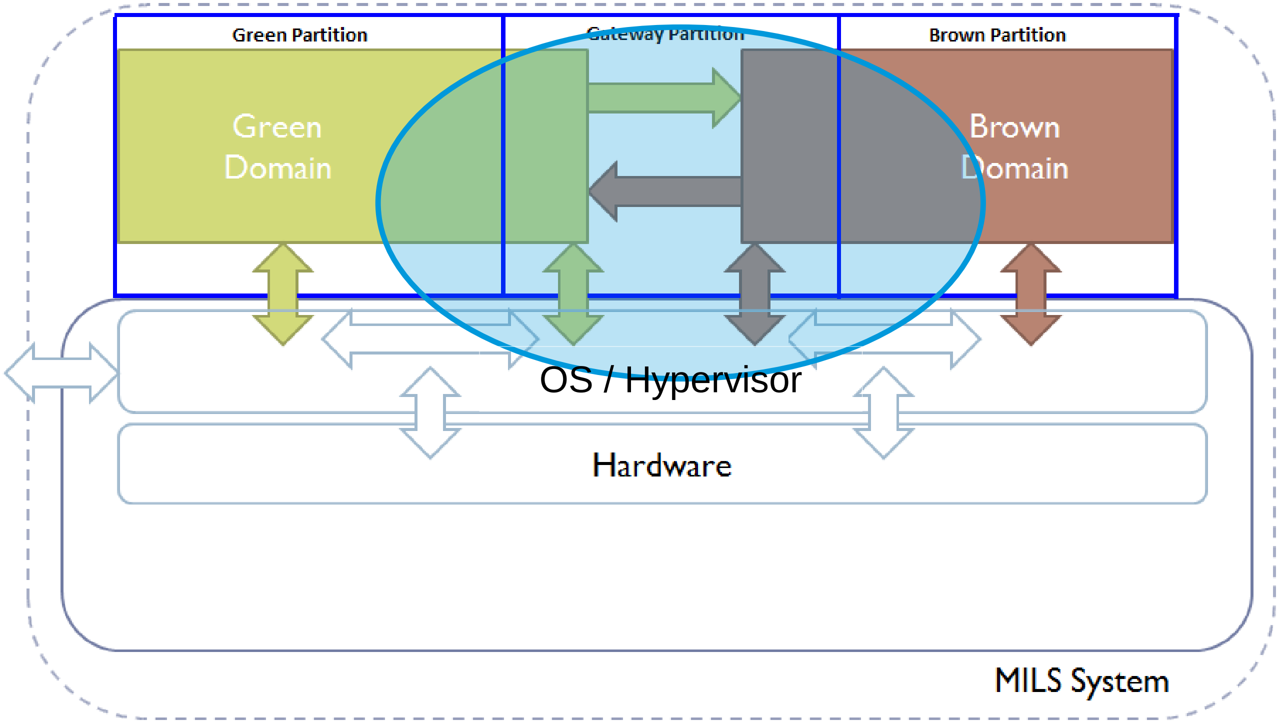
Implementation means

- Partition/process: independent segregated environment
- Separation kernel / Memory Management Unit: control instance
- Temporal partitioning: time slicing; dynamic (fair) scheduling policies

MILS – Multiple Independent Levels of Security
The Security Side of Mixed Criticality

- Architecture for a (software) system processing data of different security domains concurrently
  - Combines trusted and non-trusted apps within the same system
- High-assurance security architecture based on the concepts of **separation** and **controlled information flow**
  - *Separation*: built on time partitioning and spatial partitioning (e.g. periodic processing, memory protection, I/O separation)
  - *Controlled information flow*: white-list based communication between separate partitions
- Created Protection Profile / Security Target and reference implementation
  - EuroMILS and certMILS projects

MILS System Architecture for Controlled Information Flow



Virtualization is Key

ACRN™

Current
Data Center Hypervisors

- Too large for embedded IoT development
- No safety-critical workload considerations
- Requires too much overhead for embedded development

Current
Embedded Hypervisors

- Highly dependent on closed source proprietary solutions
- Expensive
- Makes product longevity difficult
- Hard partition, no ability to share resources

No Open Source Hypervisor solution currently exists that is **optimized for embedded IoT** development

Project ACRN™ Pillars

ACRN™ is a flexible, lightweight reference hypervisor, built with real-time and safety-criticality in mind, optimized to streamline embedded development through an open source platform

Small footprint

- Optimized for resource constrained devices
- Few lines of code: Approx. only 25K vs. <156K for datacenter-centric hypervisors

Built with Real Time in Mind

- Low latency
- Enables faster boot time
- Improves overall responsiveness with hardware communication

Built for Embedded IoT

- Virtualization beyond the “basics”
- Virtualization of Embedded IoT dev functions included
- Rich set of I/O mediators to share devices across multiple VMs

Safety Criticality

- Safety critical workloads have priority
- Isolates safety critical workloads
- Project is built with safety critical workload considerations in mind

Adaptability

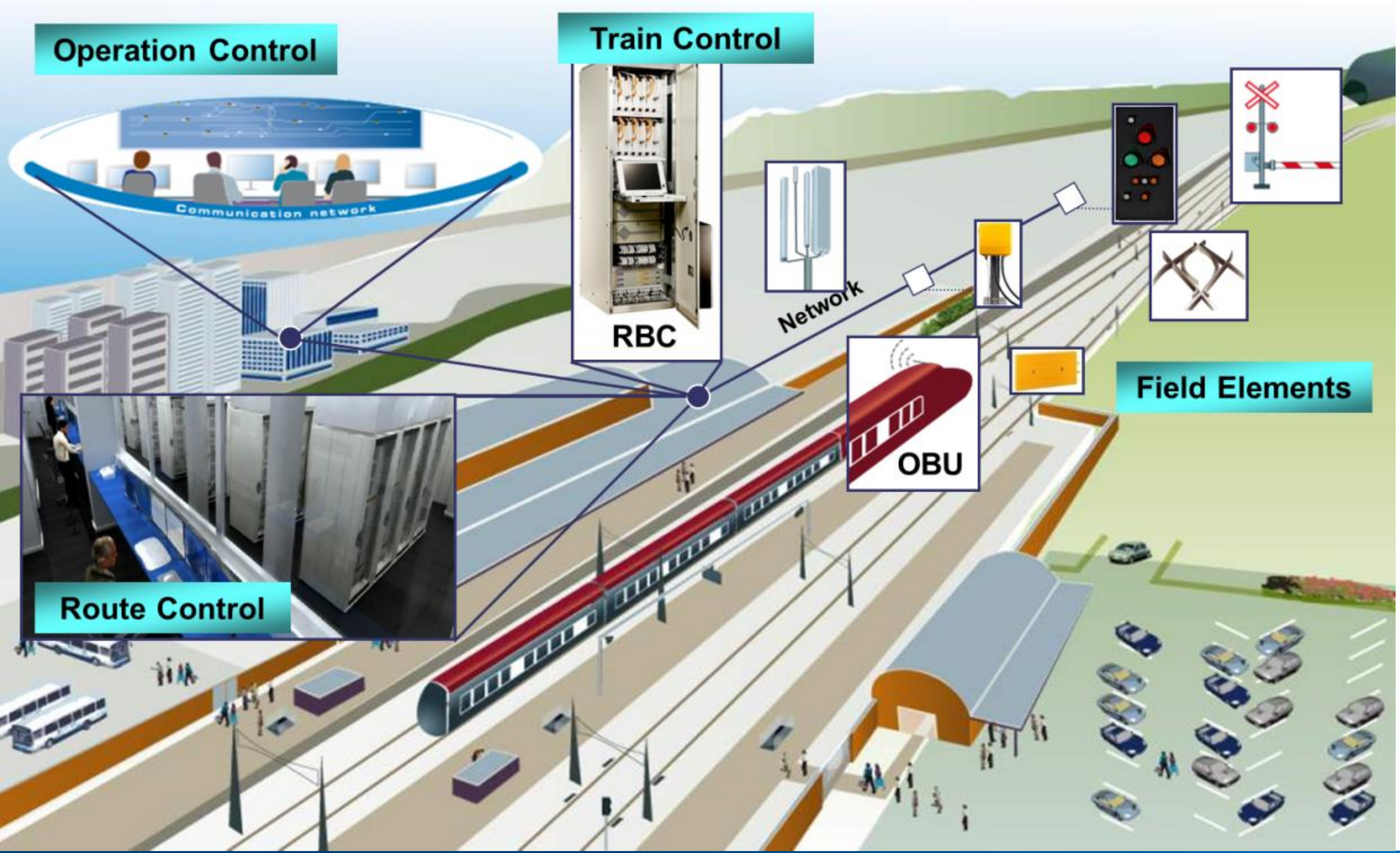
- Multi-OS support for guest operating systems like Linux and Android
- Applicable across many use cases

Truly Open Source

- Scalable support
- Significant R&D and development cost savings
- Code transparency
- SW development with industry leaders
- Permissive BSD licensing

Railway

Overview Railway – Signal Control



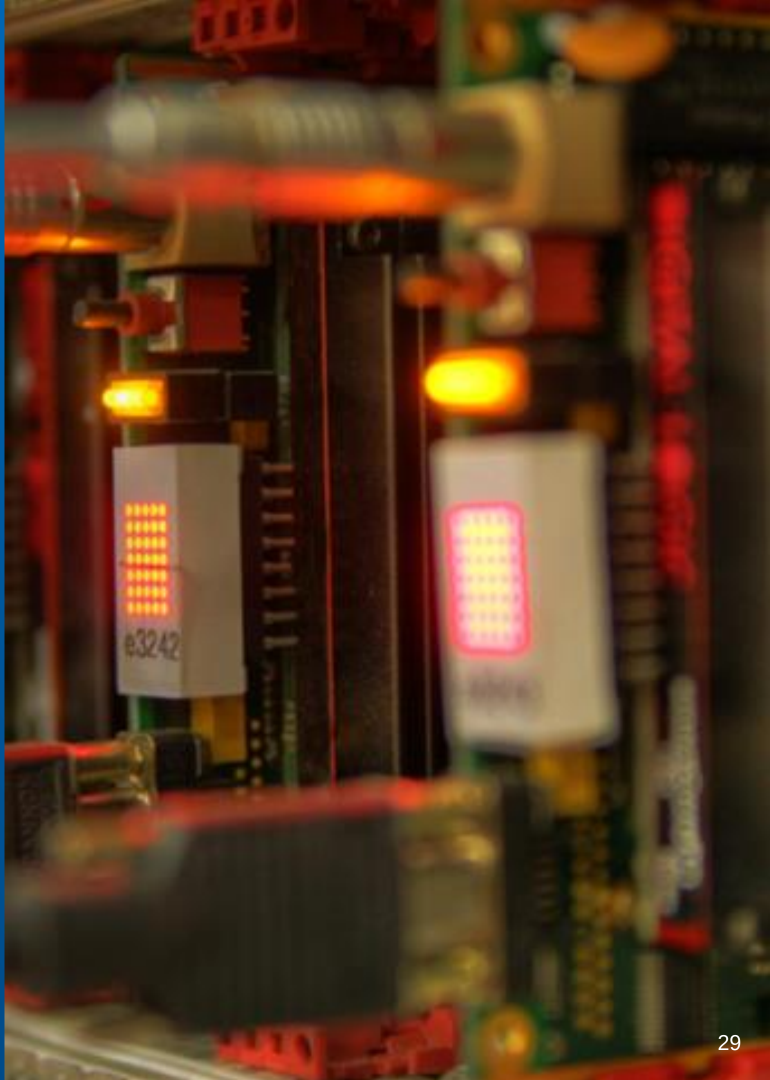
Trends

- Removal of some field elements (signals, …)
- Remote moving authority
- Central operation centers
- Autonomous operation

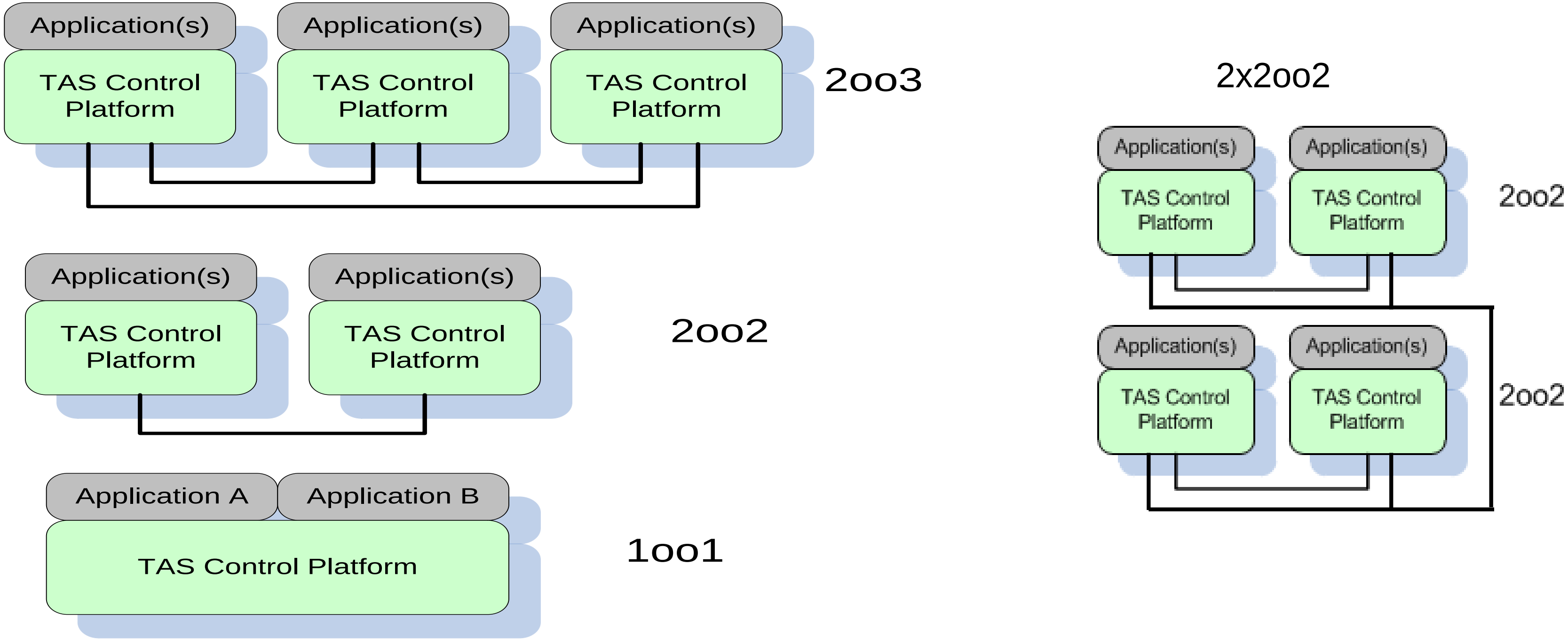
RBC … remote block center
OBU … on-board unit

Thales - TAS Platform

- Vital Hardware & Software Platform, common for all signalling applications in Ground Transportation Systems (GTS)
- Enables hardware independent signalling applications

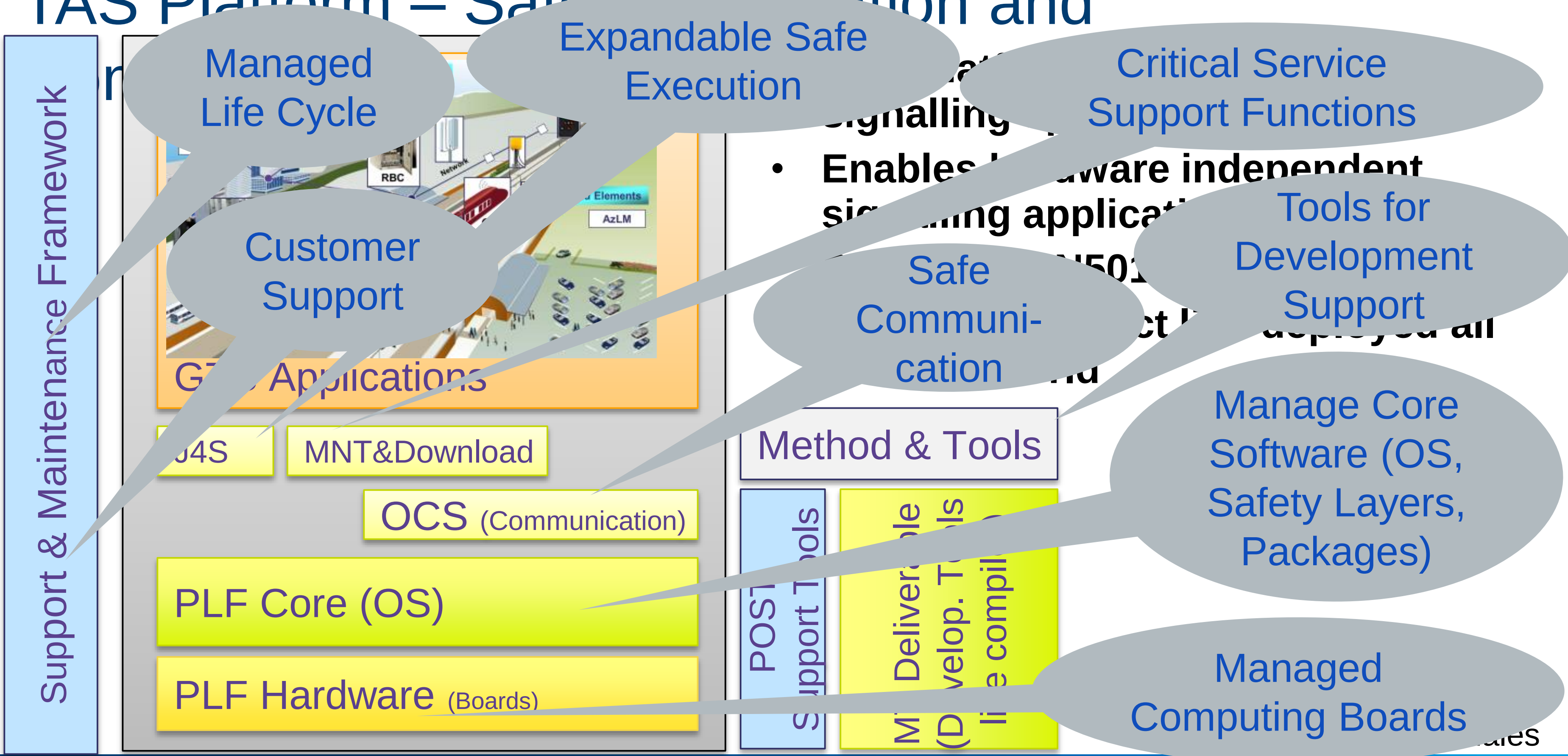


TAS Control Platform: Supported Redundancy Architectures



TAS Platform – Safe C… tation and

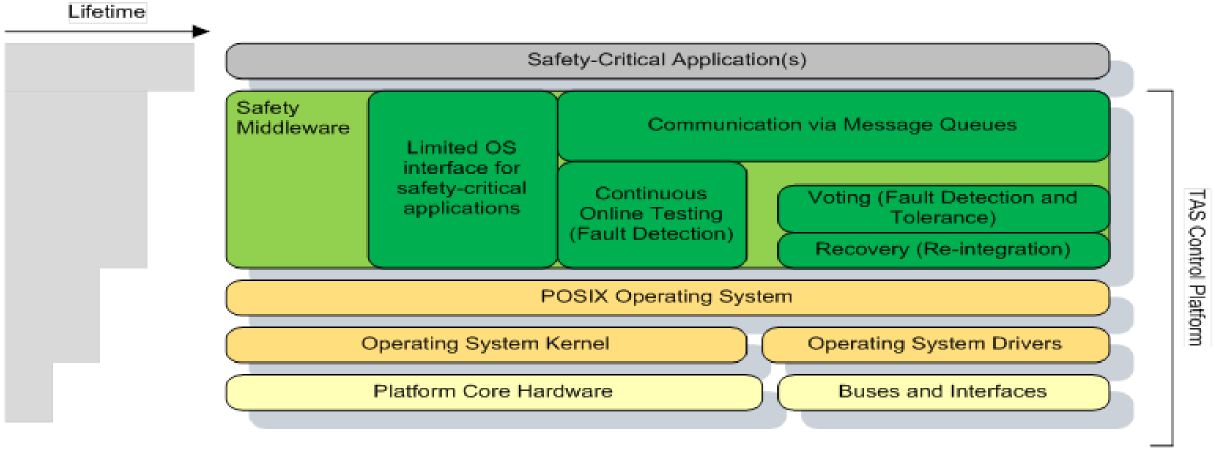
- Enables h… ware independent sig… ling applicat…



TAS Platform is Based on Linux

In addition to safety layer and functional services (communication)

Use existing COTS security packages of Linux possible

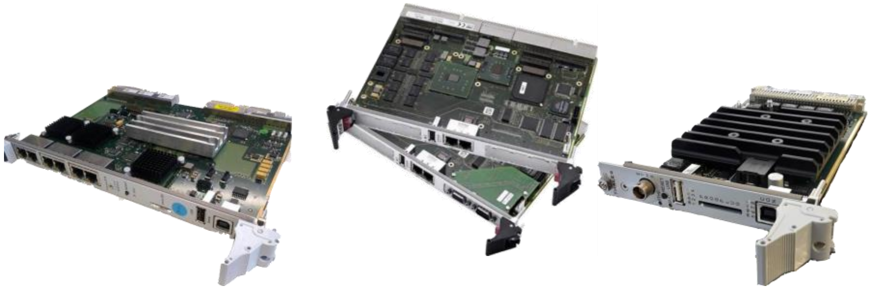


Layered safety approach allows integration of security and implement safety functions

Example: TAS Platform in Used in Applications

Interlocking

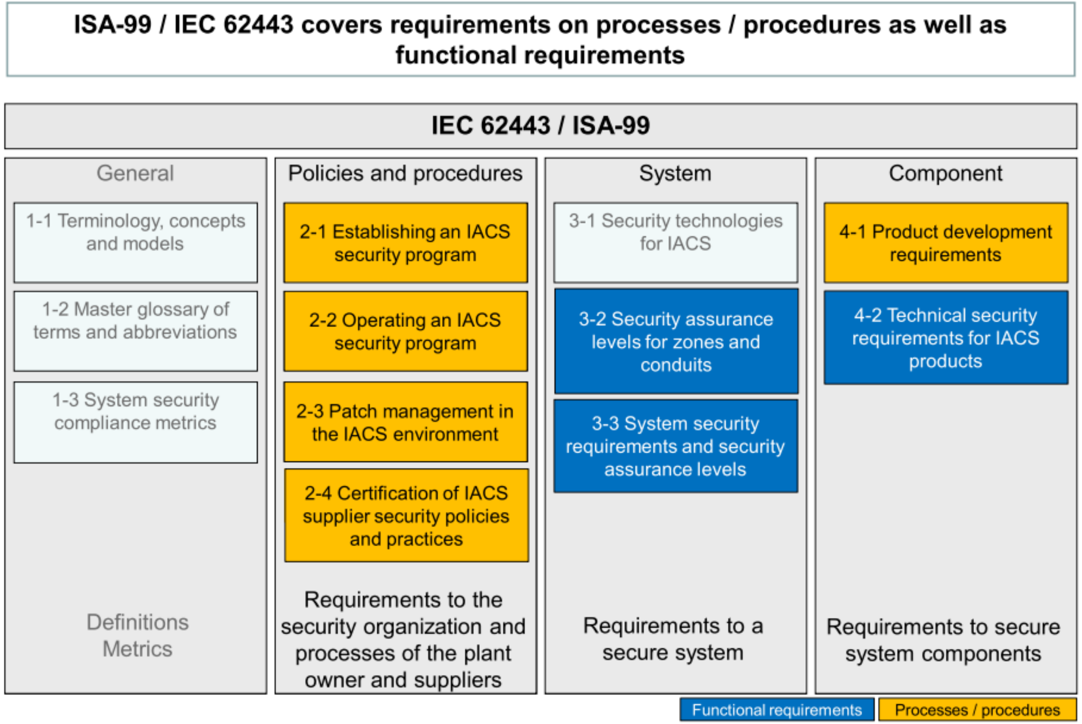
Onboard System (ETCS)



Exemplary boards

© Thales

IEC 62443 – An Applicable Security Standard Process is Key

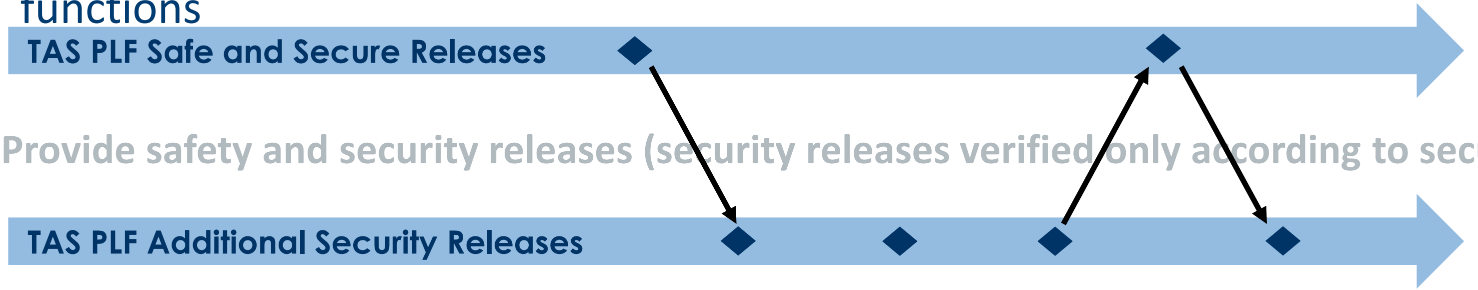


Typical Security Management – Patch Management

Removal of zero-day vulnerabilities following standards: IEC 62443 2-3 for Patch Mgmt

Separate safety and security life-cycles

- Using suitable architectures and processes or physical separation of security and safety functions



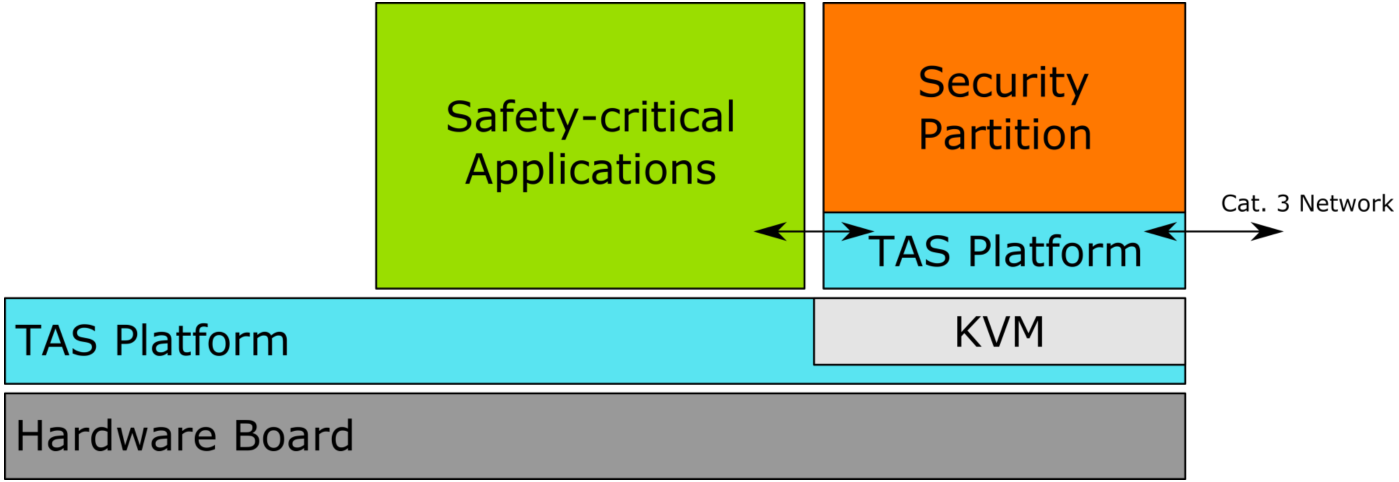
Comment in draft norm (prEN50129: 2016)

NOTE 3 Sometimes it can be necessary to balance between measures against systematic errors and measures against security threats. An example is the need for fast security updates of SW arising from security threats, whereas if such SW is safety related, it needs to be thoroughly developed, tested, validated and approved before any update.

Safety and Security Life Cycle is Different

Possible TAS Platform Safe Security Approach

Virtualization for security and safety life cycle decoupling

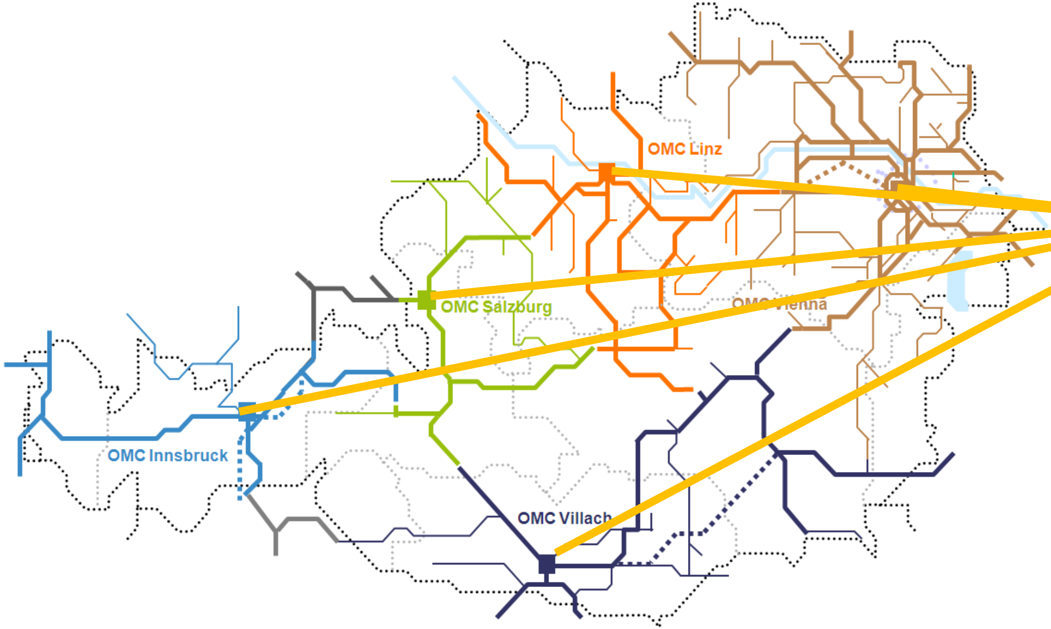


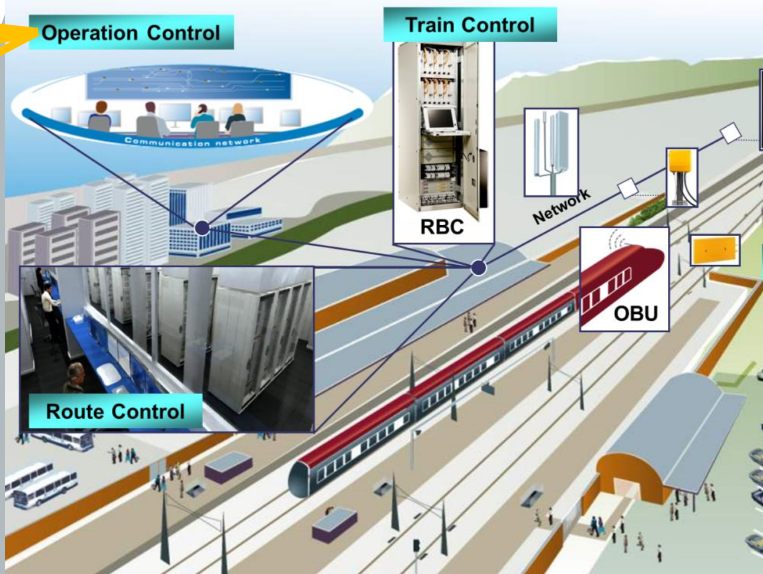
- Integration of Safety and Security

Legend:
KVM … Kernel-based Virtual Machine

THALES

Operation Management





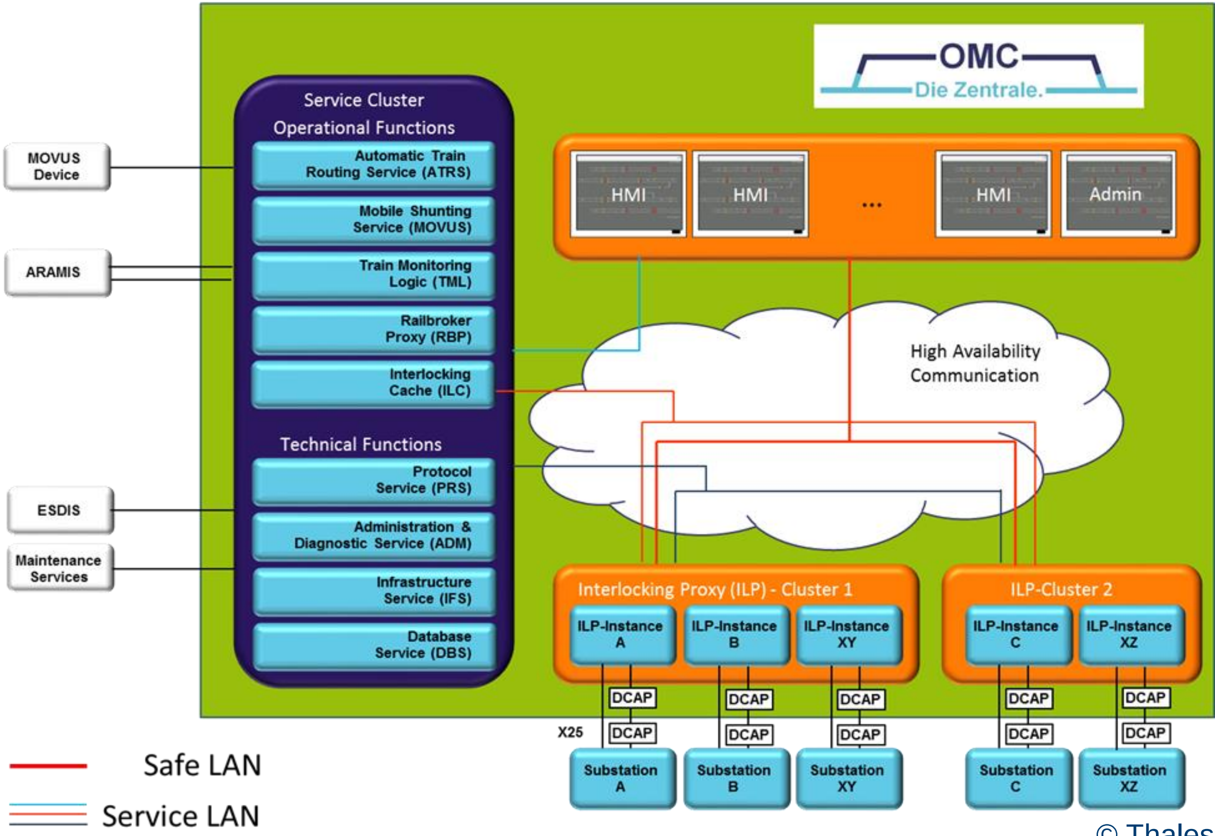
Traffic Management: User Interface

© Thales

Operation Management Center

Key element in OMC architecture

- Breakdown of functionality in smallest replaceable units (SRU) enables continuous service despite failure of SRU.
- Clean separation of safe and non-safe components

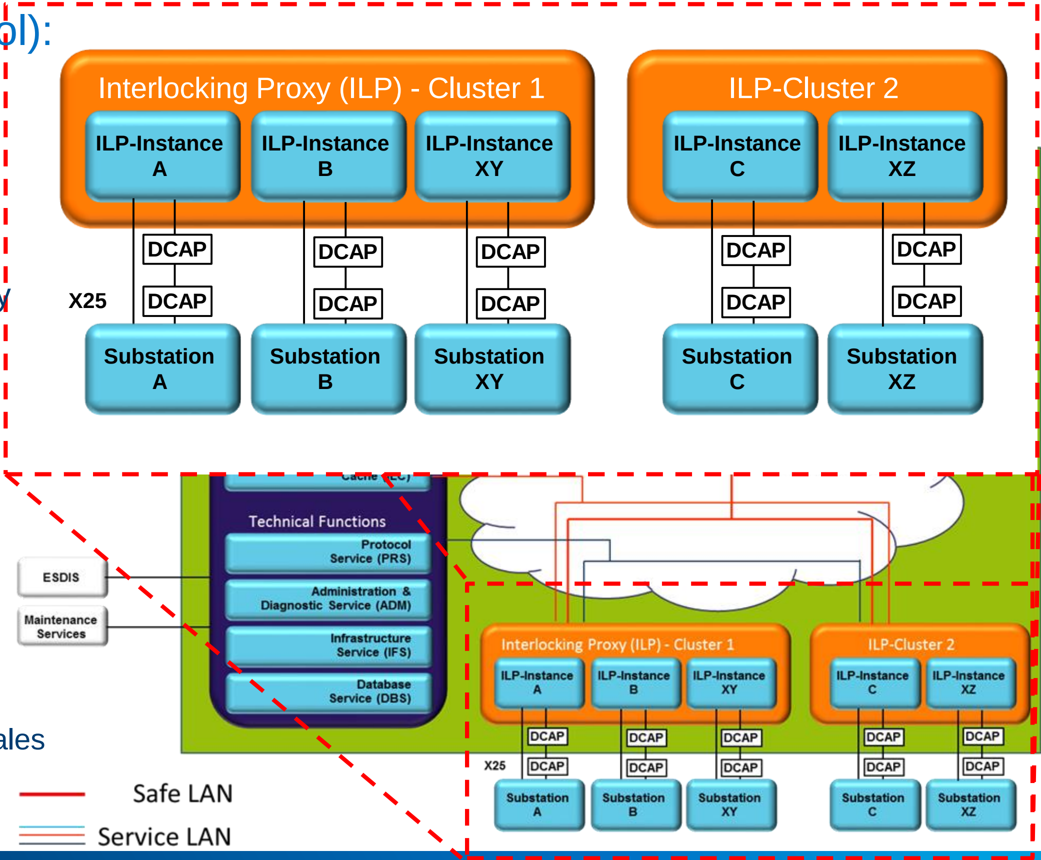


Communication to Interlocking Proxy (ILP)

Two X25 channels (special comm. protocol):

- Closed channel
- Open channel (with use of data cryptors (DCAP))
  - X25 protocol itself does not include any security measures suitable for open network communication

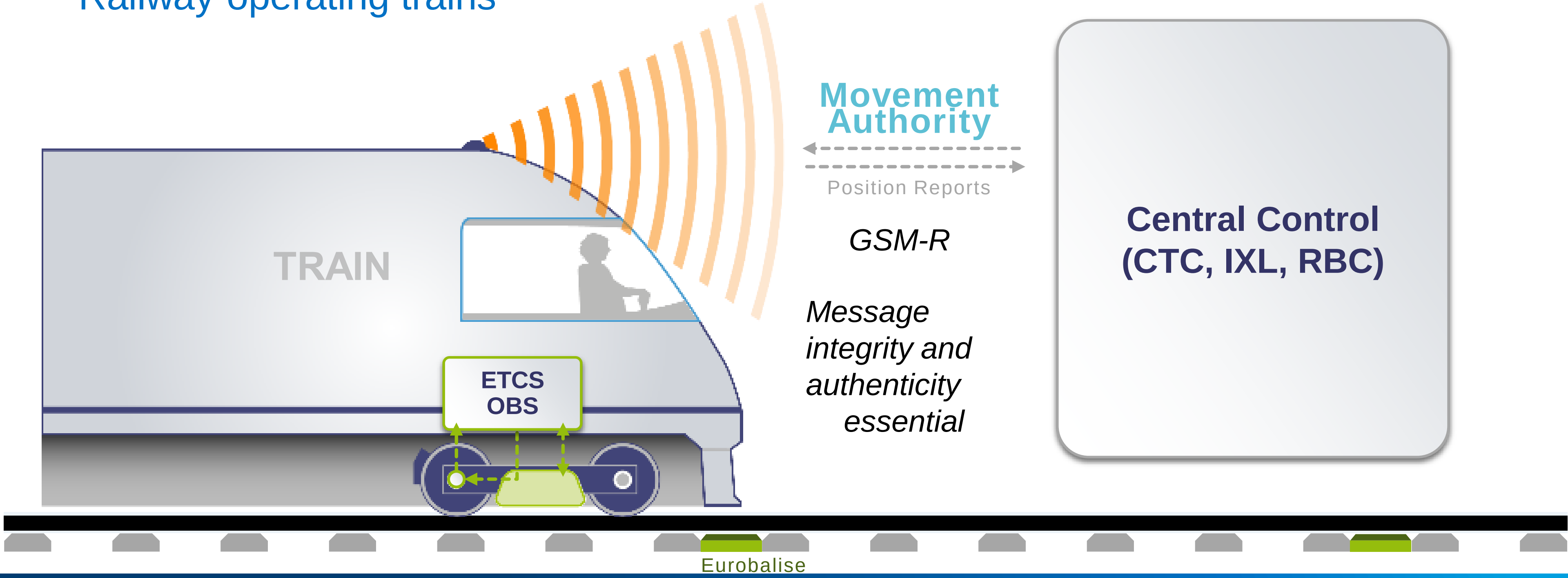
DCAP:



European Train Control System L2/L3 & Autonomy

operating central control

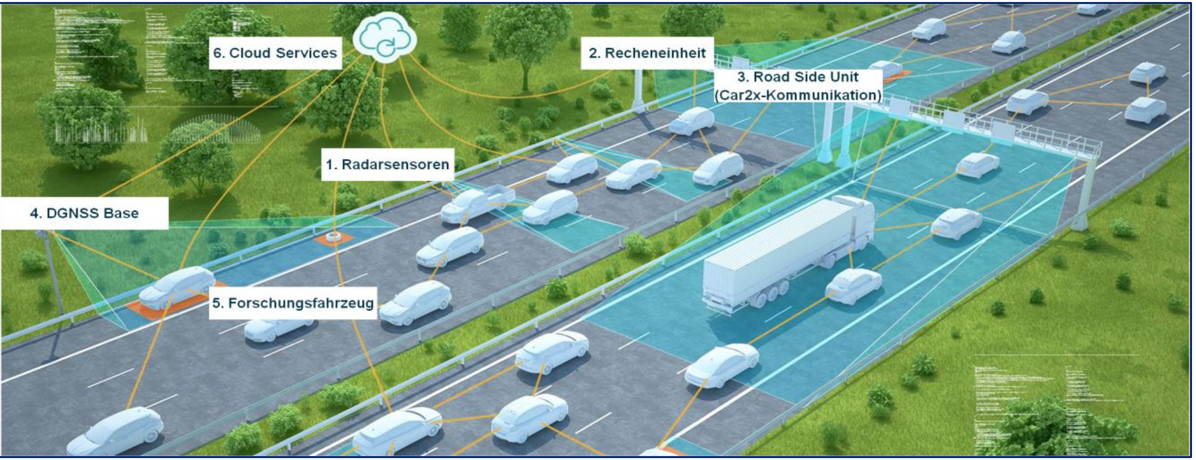
Railway operating trains



AT INTEL

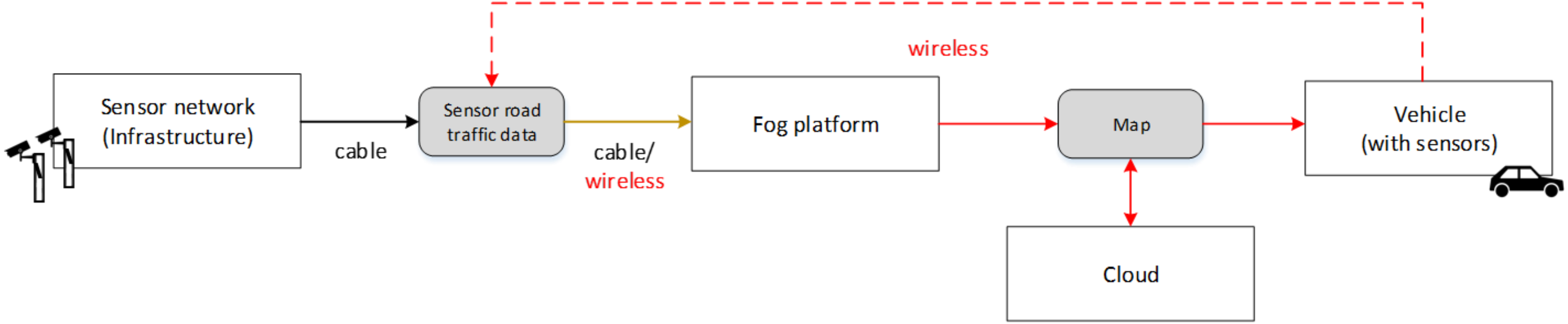
WE'RE POWERING THE FUTURE OF COMPUTING AND COMMUNICATIONS, DELIVERING EXPERIENCES ONCE THOUGHT TO BE IMPOSSIBLE.

Vehicle to Infrastructure (V2I) Complexity

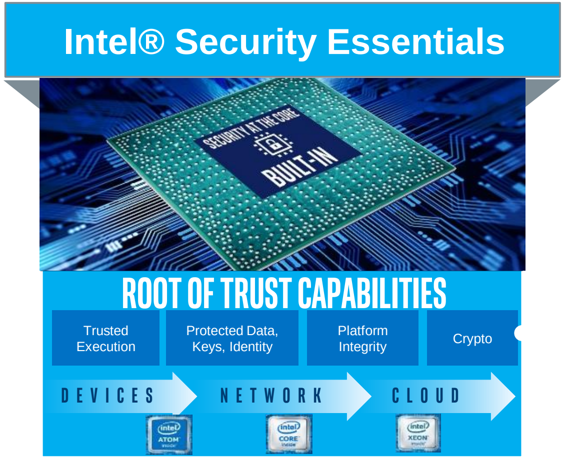


Complex cyber-physical system

How to assess/guarantee security and safety?



Re-Cap & Future (1)



Safety-critical architectures will need to consider security

Processes converge (integration security and safety)

Some common architectural approaches safety and security and real-time (MILS+IMA)

- Small footprint (essential services)
- Partitioning incl. consideration of temporal aspects

Diagnosis info and operational management approach key to current and future IoT (incl. safety-critical systems) lead to connectivity needs and potential vulnerabilities

Re-Cap & Future (2)

ACRN™

Updates are the norm: Updates for security purposes (removal of zero-day vulnerabilities)

Application-level fault tolerance aspects often driving factor e.g. image processing: degree of correctness

- With learned behavior improvements for safety reasons safety update process changes
- SOTIF (Safety Of Intended Functionality)
  - NEW: updates to improve safety!!
- Leads possibly to “joint goal” of frequent updates due to safety and security improvements

Also may need updates for safety (emerging knowledge affecting safety) – defense-in-depths approaches for security and safety

Some Other Thoughts on Emerging Issues

Hard challenges:

- Virtualization: Hard challenge is guarantee of safety on top of virtualization (w/o hardware knowledge)
- Long-term guarantees of dependability: 10 to 15 years or more
- Automated safety approaches (automated verification and validation approaches)
- Guaranteeing availability will be tough research questions e.g. with correctness of design (integrity is much easier)

Defense in depths approaches for security and safety (updates)

Dependable power architectures becomes more important intel®