
1ST UIC GLOBAL CONFERENCE
ON SIGNALLING
The Evolution of ERTMS
MILAN 2018 26-28 March

# Fusing Safety and Security on a Solid Foundation for ERTMS

## A Platform Approach

THALES

***Reinhard Hametner***, *Michael Paulitsch, and Alexander Szoenyi*
*Contact: reinhard.hametner@thalesgroup.com*

# Safety & Cyber Security

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

**Cyber 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 Rail Systems requires increased attention on Cybersecurity,

- to avoid operational disruption (availability),
- access to user confidential data, and
- ensure safety is not impaired (system integrity).

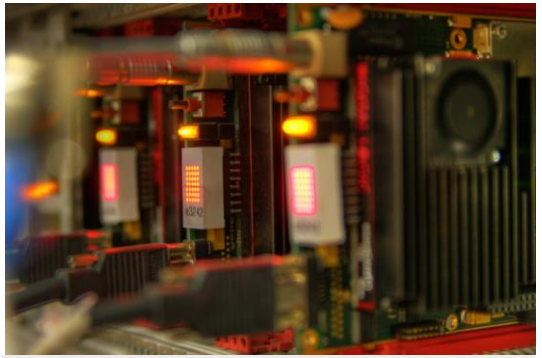
# TAS Platform Use

Interlocking

- Vital HW & SW Platform, common for all Thales signalling applications in Ground Transportation Systems (GTS)
- Enables hardware independent signalling applications
- CENELEC EN50129 SIL4 Certification
- Used in more than 70% of Thales GTS sales:
  - Route control systems: electronic interlocking - LockTrac
  - Field equipment: digital axle counters, warning system
  - Train control systems: ETCS standards L1, L2, L3 - AlTrac
  - Urban rail management control systems - SelTrac
  - Traffic management systems: NetTrac Aramis, operation management centre


Axle Counter

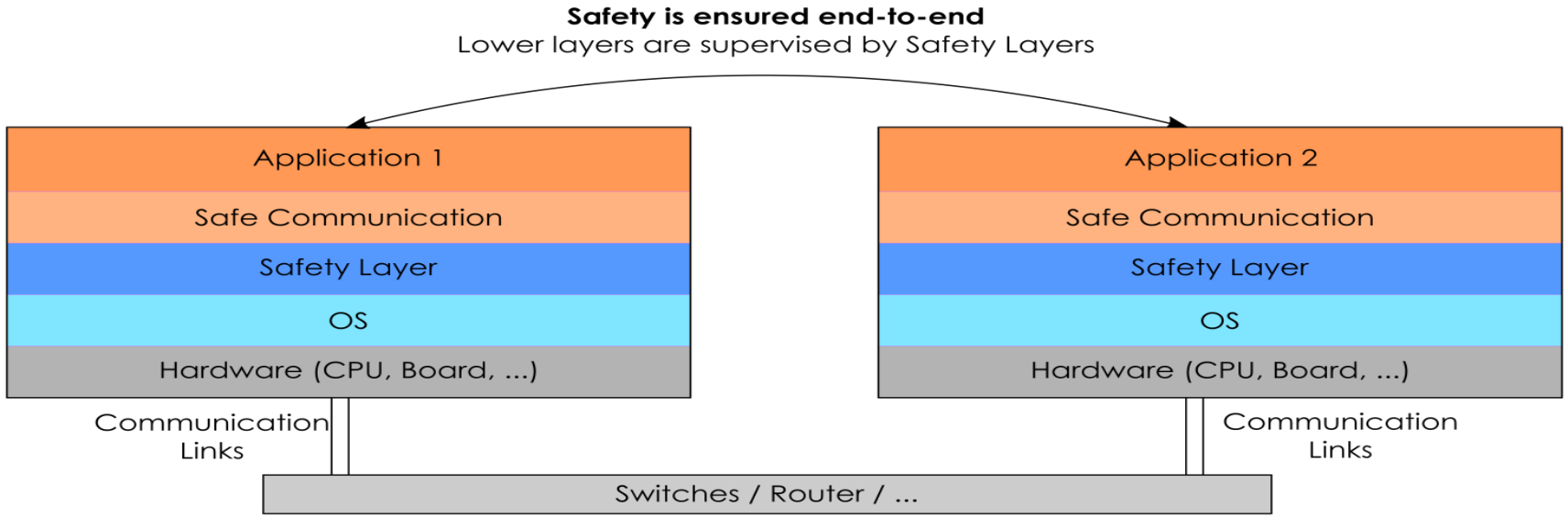
Control Center



ETCS Onboard

# Safety: Layered Architecture and Design

- Currently EN 50159 Cat. 2 for Safety is in place.
- Safety is ensured end-to-end
- Security has not been explicitly focused on in the past
  - Products use COTS security components for encryption



# TAS Platform – A Generic Safety Case

TAS Platform-based products
Main Line Rail

TAS Platform-based products
Urban Mobility


ETCS


Interlocking


On Board


Field Elements

Generic TAS Platform
Generic CENELEC approval

**TAS Platform System Safety Case**
TAS Platform Engineering & Environment

TAS Platform Services

**Safety Application Conditions**

Core System TAS Platform SW

Subsystems: OCS, MNT, J4S

- Check of HW-CS SAC
- Validation on HW-CS
- Approval with HW-CS

**Safety Application Conditions (SAC)**

SW components
- Analyses
- Verification
- Validation

**Safety Application Conditions (SAC)**

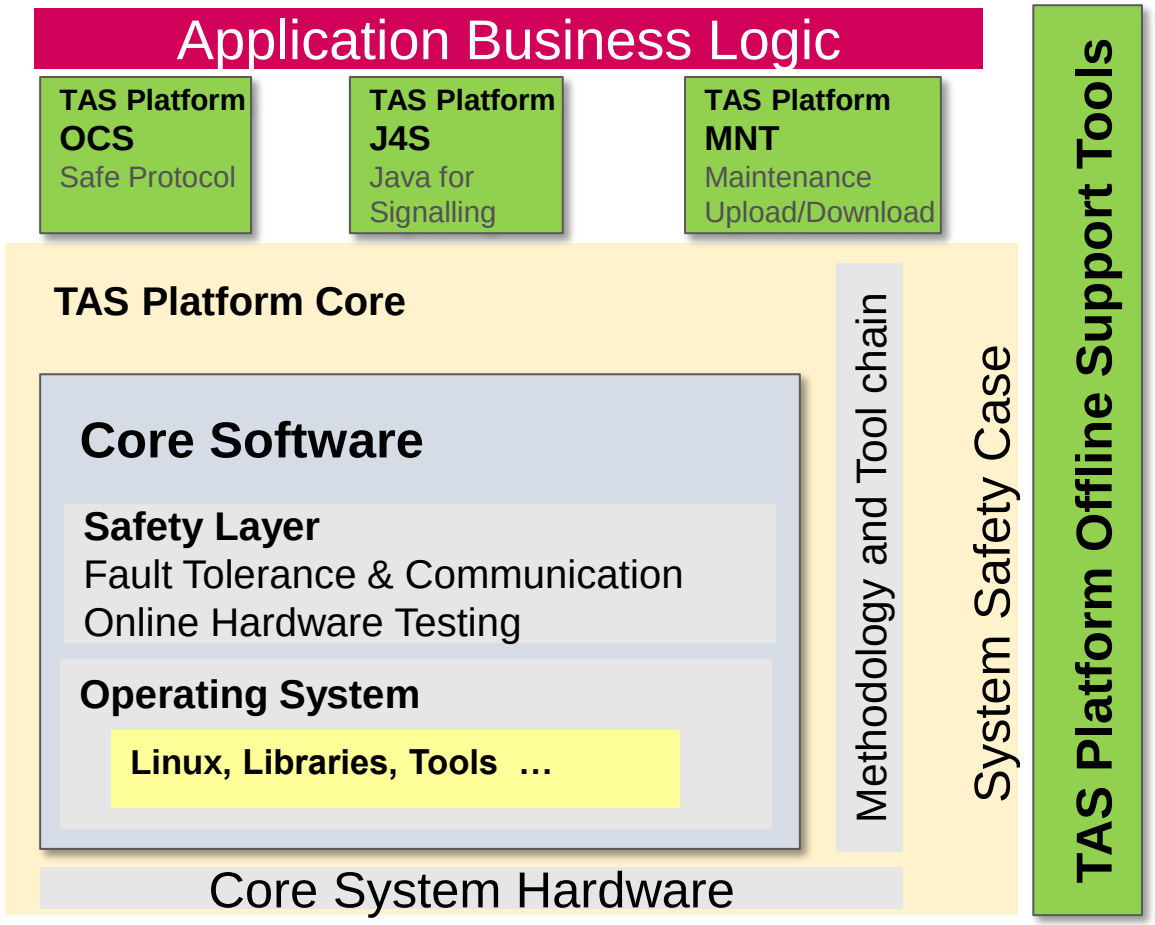
HW components
- Analyses
- Verification/Validation
- Manufacturing

HW Core System
- Analyses
- Verification/Valid
- Safety Case
- Manufacturing
- Approval

Distributed Development / Maintenance (Thales)

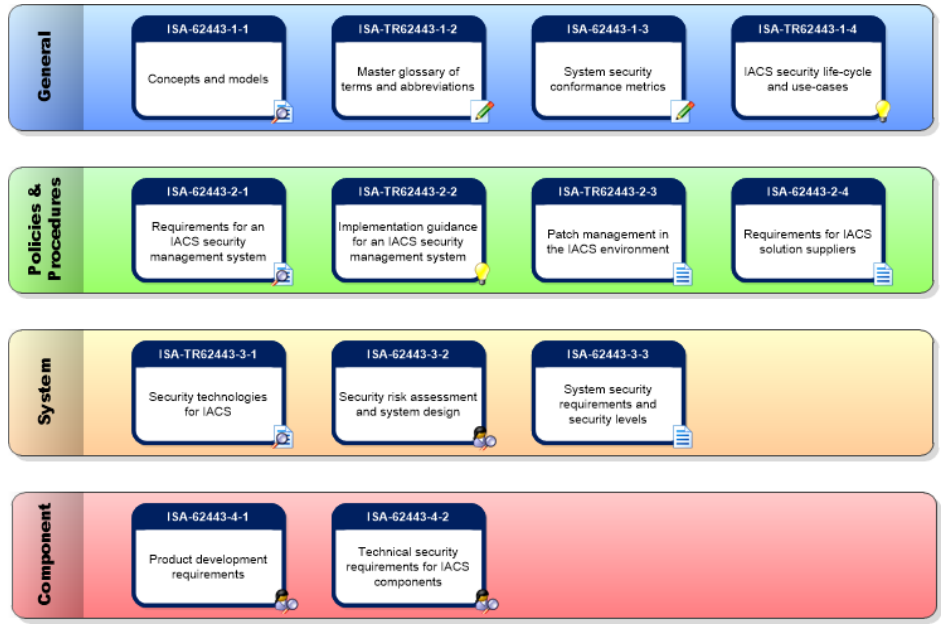
# Overview TAS Platform – A Closer Look

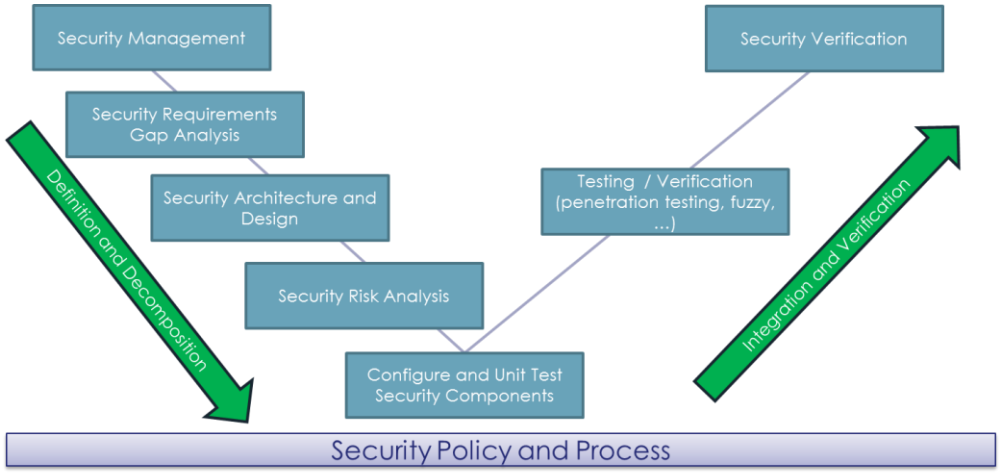
- Safety approval according to CENELEC 50129 SIL 4
- Safety layer
  - Fault tolerance
  - Health monitoring (Online Hardware Testing)
- Board support package
  - Communications interfaces / drivers
- Based on COTS hardware / operating system
  - Kernel patches to address safety, security, and maintainability
- Support 25 years of application business logic (with changing underlying hardware and software)
- Security functions supplied with COTS components (OS and libraries)



# Security Management

- Process definition based on ISA/IEC 62443
  - Customer requirements are considered
  - TAS Platform as „Component“
    - ISA/IEC 62443-4-1
    - ISA/IEC 62443-4-2
- Apply defined Security process
- Security process in-line with safety process



# Security Vulnerability Management

- Part of the security process
- CVE management tool developed by Thales
- Automatic scan of used Linux packages for possible affected CVEs
- Based on CVE NIST database

**CVE Statistics**

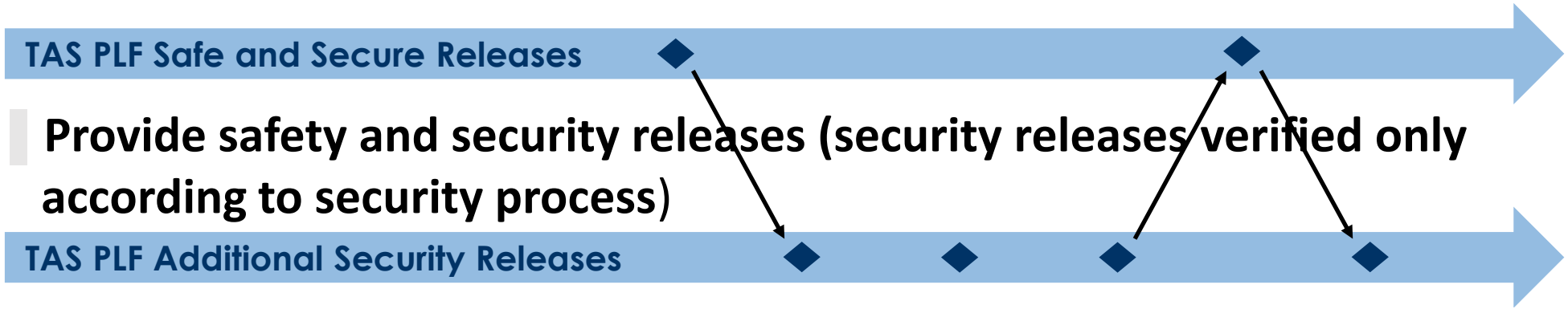
| | | Count | percent |
|---|---|---|---|
| CVEs with pending analysis | | 28 | 6.0% |
| Reviewed CVEs | | 363 | 87.0% |
| | Affected CVEs | 234 | 56.0% |
| | Not Affected CVEs | 117 | 28.0% |
| | Ignored CVEs | 12 | 2.0% |
| | Not proccessed due to error | 0 | 0.0% |
| Fixed CVEs | | 24 | 5.0% |
| Summarized CVEs | | **415** | 100% |

# TAS Platform in Unsecure Networks

- Several security requests received (partly implemented, in implementation, or planned)
  - **Move to "category 3" networks** according to CENELEC EN 50159 (unsecure networks)
  - Deployment of **system development processes** which consider security throughout the development
  - Additional "typical" requirements: Logs, patch management, authentication modules, …
- Challenges:
  - Long-term availability in field and safety conservative **update challenge** system security (legacy)
  - Legacy applications (need **continued support**) – "don't change interface/hardware/…"

# TAS Platform Security – Patch Management

- Following standards: IEC TR62443 2-3 for Patch Management
- Separate safety and security life-cycles
  - Using suitable architectures and processes or physical separation of security and safety functions



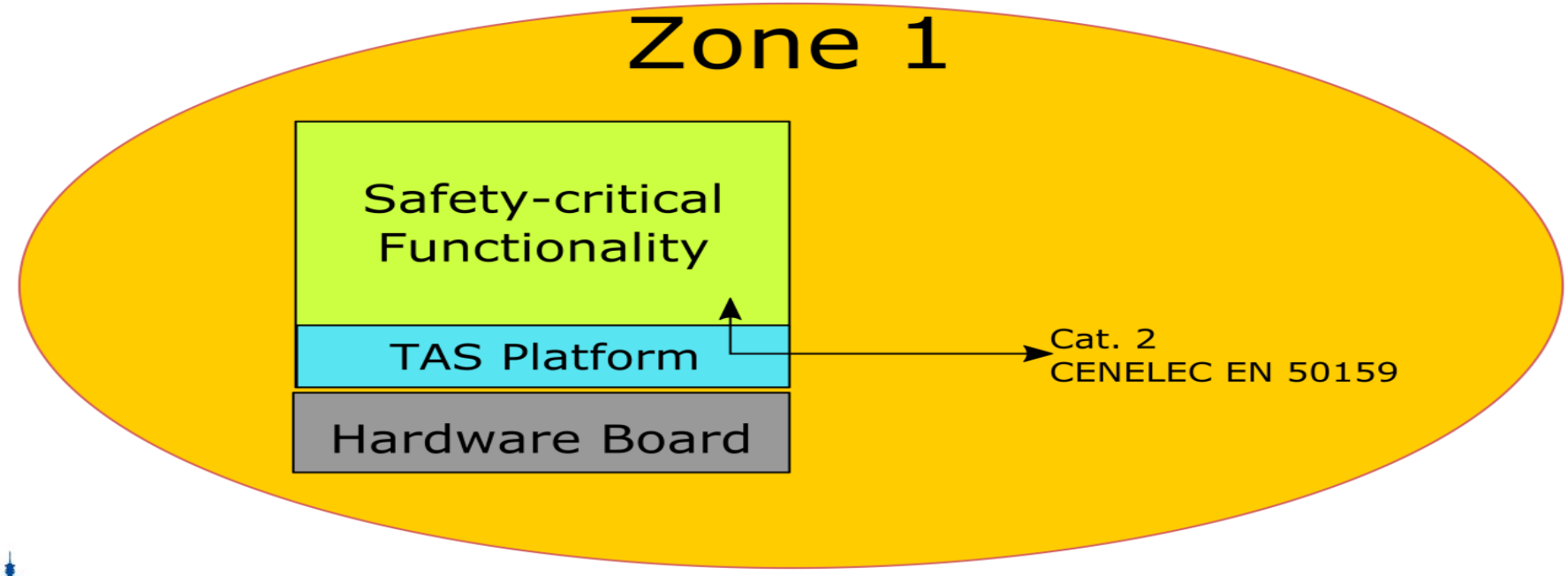

*Comment in draft norm (prEN50129:2016)*

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**

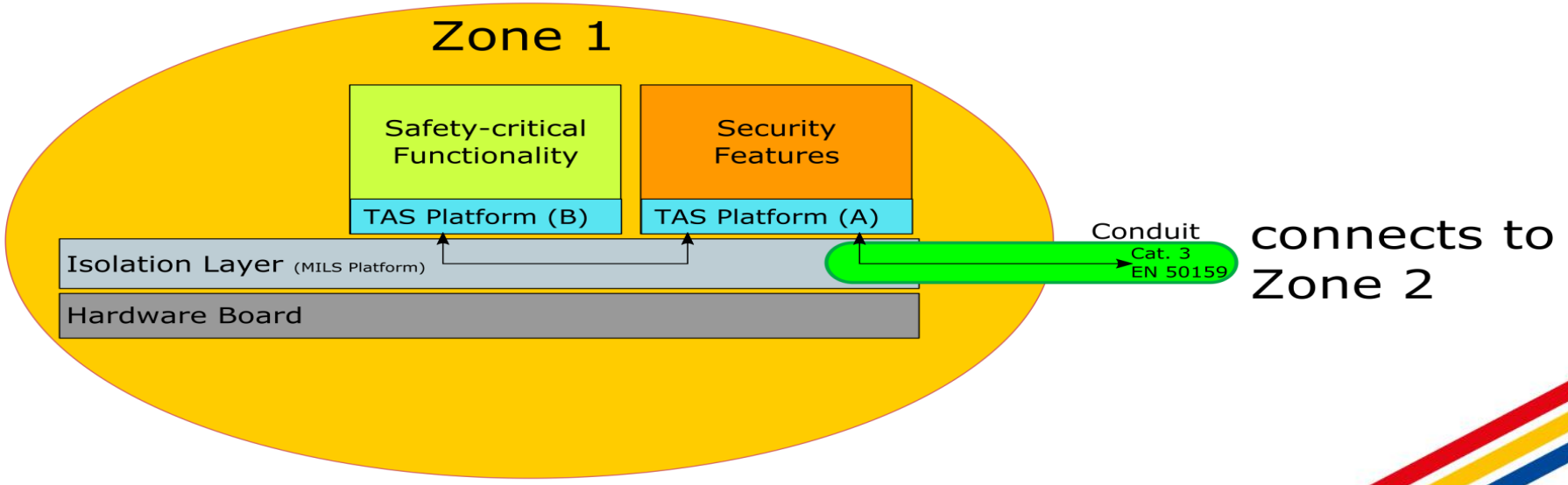
# Security Zone and Conduits #1

- Zones and conduits defined according to ISA/IEC 62443-3-3
- Up to now all components are in one zone
- Only up to EN 50159 Cat. 2 network is possible



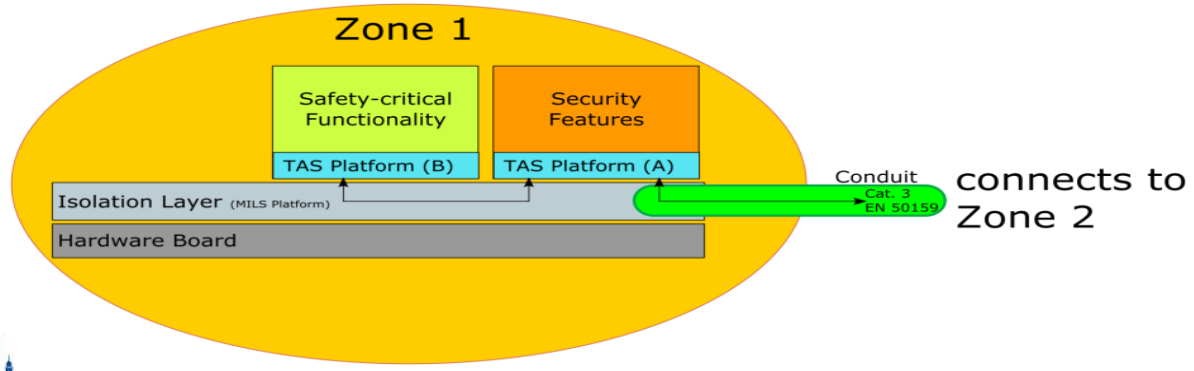
# Security Zone and Conduits #2

- Security Features (CyberGate as integrated firewall)
- Connection to other zones possible by conduits
- Enabled for EN 50159 Cat. 3 network
- TAS Platform (A) is exchangeable without re-certification of safety-critical functionality and TAS Platform (B)



# Security Zone and Conduits #3

- Isolation Layer / MILS Platform (Multiple independent levels of security)
  - Separate security from safety
  - Performance / resource usage by security features must be restricted and predictable
  - Availability through redundancy (independent boards, links, and CyberGate instances)
  - Safety-critical functionality is always provided with redundancy



# Summary

- Security is becoming a real concern
- Multiple security assessments and customers have driven and are driving improvements of Thales applications and TAS Platform
- TAS Platform architecture has already been ready for security extensions – simple integration of security functions
- Overlaps in processes in achieving security and safety

**We are ready!**
**And, never stop improving …**

THALES

# CERTMILS Contract No: 731456

"This work/project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731456."

If you need further information, please contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, AUSTRIA

Tel: +43 4242 233 55 Fax: +43 4242 233 55 77

E-Mail: coordination@certmils.eu