SYSGO
EMBEDDING INNOVATIONS

MILS Introduction, Activities and Updates

Dr. Sergey Tverdyshev

Content

- **A Freshman Intro**
  - Where MILS is used
  - Standards
  - MILS Overview
- **MILS Activities**
  - CCUF
  - CITADEL Project
  - certMILS project
- **Summary & Next Steps**

MILS Motivation

Safety and Security

- **Safety – system shall not harm the environment**
  - Example in aircrafts/cars: passengers shall stay alive and unharmed while transportation from start to destination
    - System: aircraft/car
    - Environment: passengers
    - Harm: crash leading to deaths

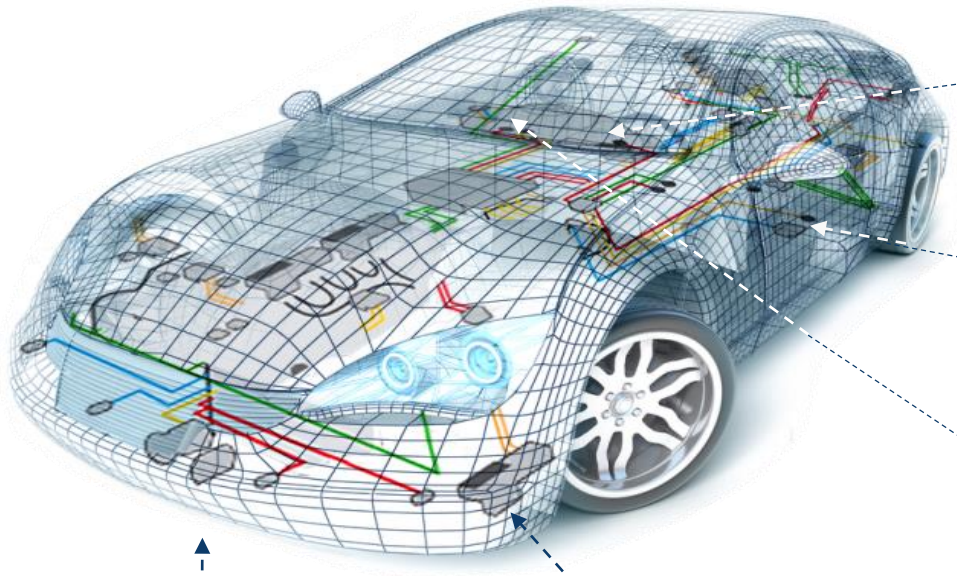
- **Security – environment shall not be capable to harm system**
  - Example in information gateways: information shall only be read/written by authorized subjects
    - System: information processing device
    - Environment: unauthorized subjects (hackers)
    - Harm: modification or leak

SYSGO
EMBEDDING INNOVATIONS

Aircraft Today

- **Aircraft is network based (AFDX & IP)**
- **Increasing usage of common computing resources**
  - IMA, Open World
- **Open World domain with COTS software**
  - Wi-fi products, Linux
- **New IT services**
  - Pilots (tablets), passengers, crew, maintenance
- **Increasing integration and information flows between systems**
- **Aircraft is heavily connected to other IT services**
  - Airlines, ATC
- **Aircraft is connected to INTERNET**

Highly integrated ECUs with COTS SW

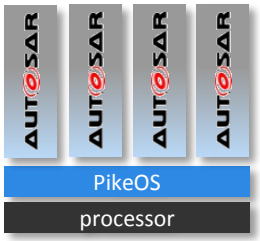


Instrument Cluster

Connectivity Box

Infotainment Head Unit

Domain Controllers



Driver Assistance Systems

Tachograph

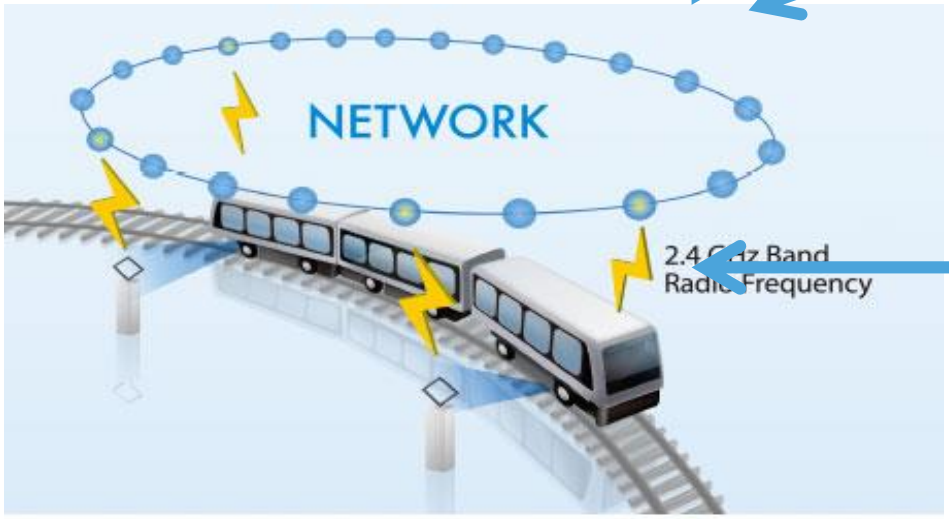
SYSGO
EMBEDDING INNOVATIONS

Railway going online

Field elements

Wired,
public wireless

Interlocking



CBTC (Communications-Based Train Control)

Operation Management and Supervision Systems

SYSGO
EMBEDDING INNOVATIONS

Many Standards same Principles

- **Analysed standards: J3061, IEC 62443, CC, EDSA/SSA/SDLA, IEC 61508, DO-178B, ISO 26262, AUTOSAR, IMA**

- **Security/Safety Domains**
- **Partitioning / Isolation / Separation of**
  - State
  - Data
  - Functions
  - Criticality
  - Assurance
- **Trust boundaries**
  - Explicit internal interactions
  - Explicit interfaces between security domains
  - Attack surface
  - **“No communication” as important as “There is communication”**
- **Platform and Resource Management**

SYSGO EMBEDDING INNOVATIONS

MILS Overview

Open-platforms: Sharing. Sharing is a Challenge

Challenge: Resources sharing

Resources

- CPUs, memory, IO memory
- Files, drivers, devices, buses

Safety

- Integrity, availability
- Isolation, application errors, fail safe

Security

- Integrity, availability, confidentiality
- Possible side channels via shared resources
- Resources and API are attack surface

Challenge: Time sharing

Time

- CPU cycles
- Time effects on shared resources, e.g. bus

Safety

- Availability, determinism, meet deadlines
- Balance between time-/event-based tasks

Security

- Availability, confidentiality
- Timing side channels via shared resources, e.g. caches, busses
- Time is the attack surface

Brief MILS History: 1975 - 2019

1975
- Saltzer and Schroeder "The Protection of Information in Computer Systems"

1981
- Rushby "Design and Verification of Secure Systems"
- MILS was coined

1992-2005
- IMA concepts, safety focus

2005
- Hardware virtualisation Intel VT-x, AMD-V

2007
- US Separation Kernel Protection Profile

2007-…
- US-based studies
- The Open Group standardisation
- Hardware was not in the focus

2012
- SKPP sun-setted by US government: HW complexity, monolithic eval, politics

2013
- EURO-MILS
  - High Assurance methods
  - Compositional cert
- D-MILS
  - Research on configuration and analysis of distributed MILS

2014
- Founding of the MILS Community
- MILS Architecture
- Protection Profile for Separation Kernel

2015
- 1st MILS Workshop

2016
- CITADEL: adaptive MILS
- Adaptation of MILS systems preserving system properties

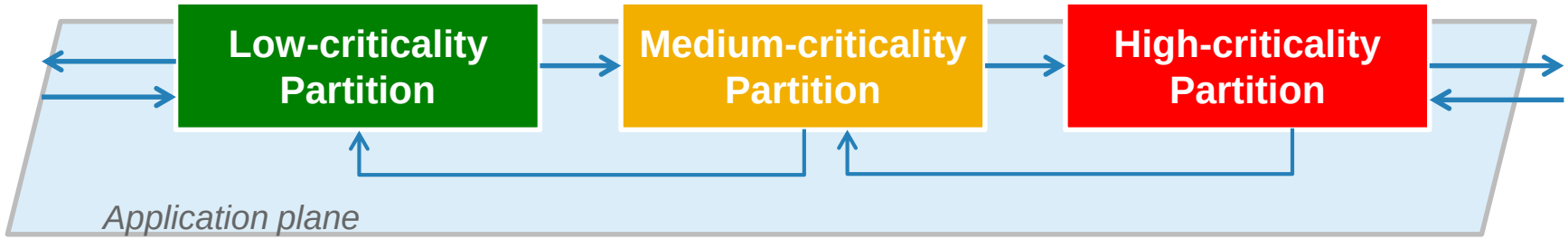
2017
- certMILS: compositional certification of system based on MILS
- Initiating Separation Kernel WG within CCUF

2018
- Joint work with CCUF Hypervisor WG
- Development of ESR and PP

2019
- Two MILS SK products have been certified with the developed PP as base

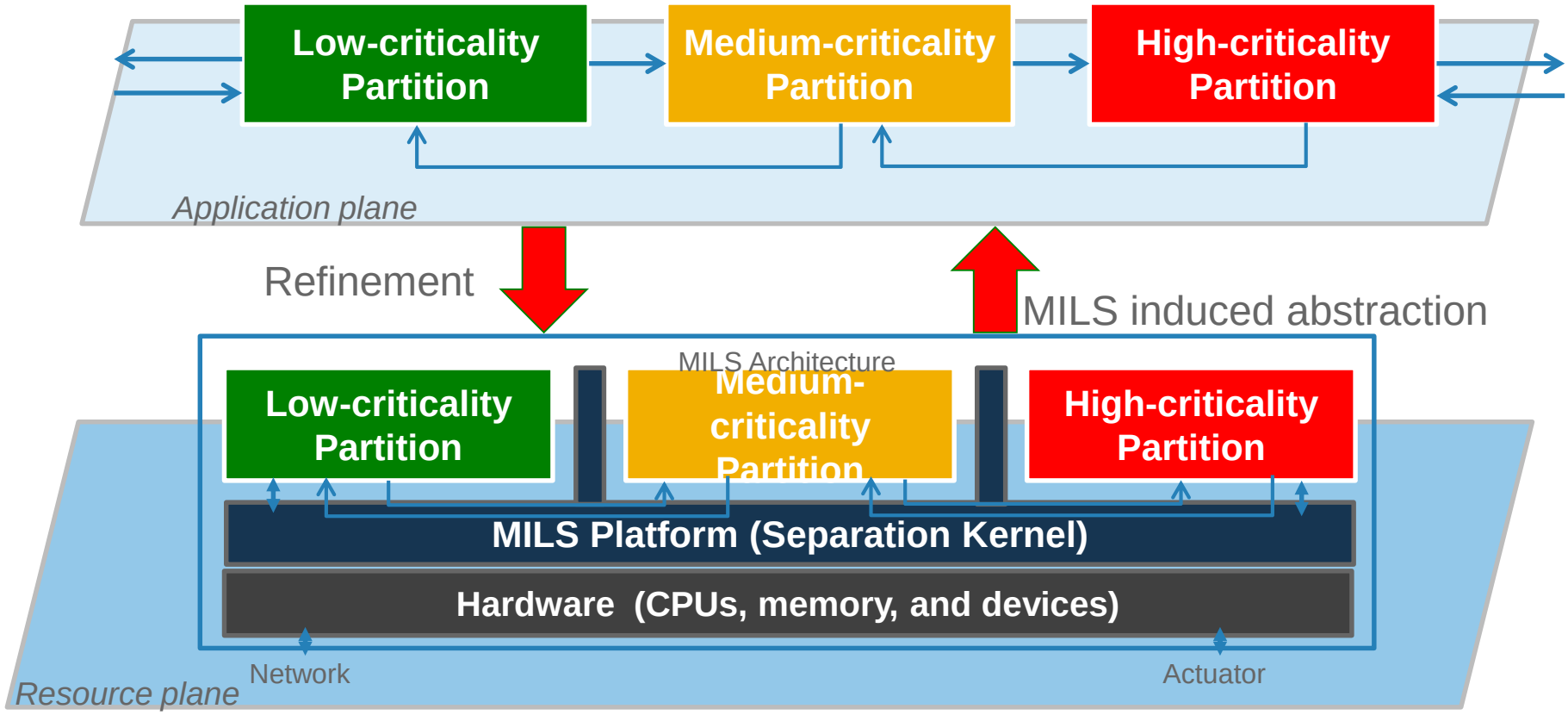
SYSGO EMBEDDING INNOVATIONS

MILS



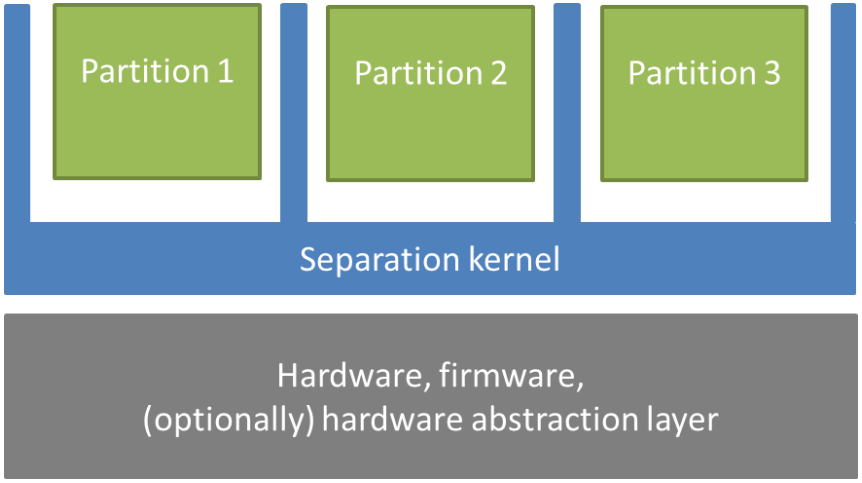
MILS is a **high-assurance security architecture** that supports the **coexistence** of untrusted and trusted components, based on **verifiable separation mechanisms** and controlled information flow

MILS Architectural Approach

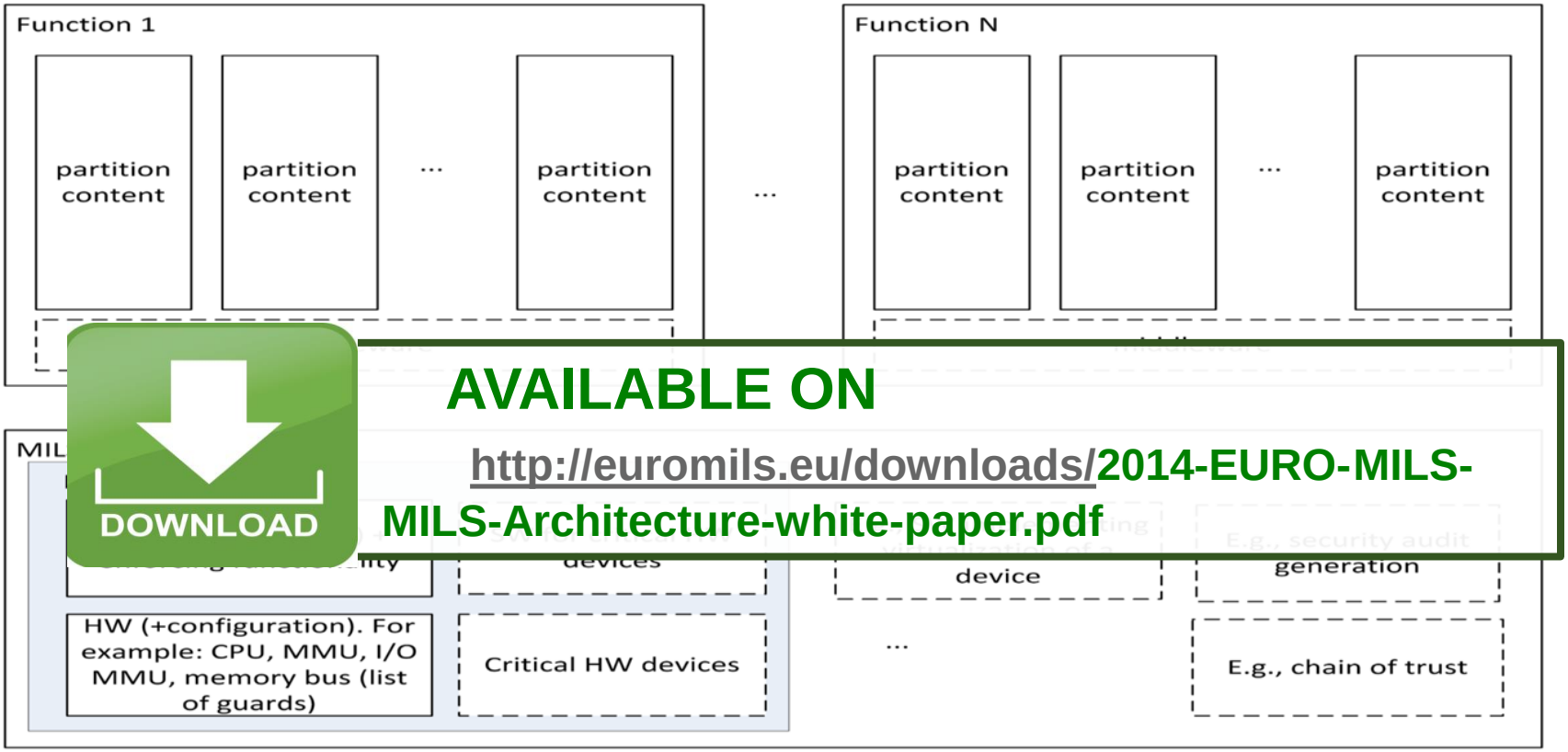


MILS in a nutshell

- **MILS system consists of**
  - Separation kernel
  - Separation supporting HW
  - Partitions
- **MILS Objectives**
  - Compositional security
  - Compositional assurance
- **MILS**
  - Used today as a proper noun
  - Historically, stand for “Multiple Independent Levels of Security / Safety”



MILS Architecture

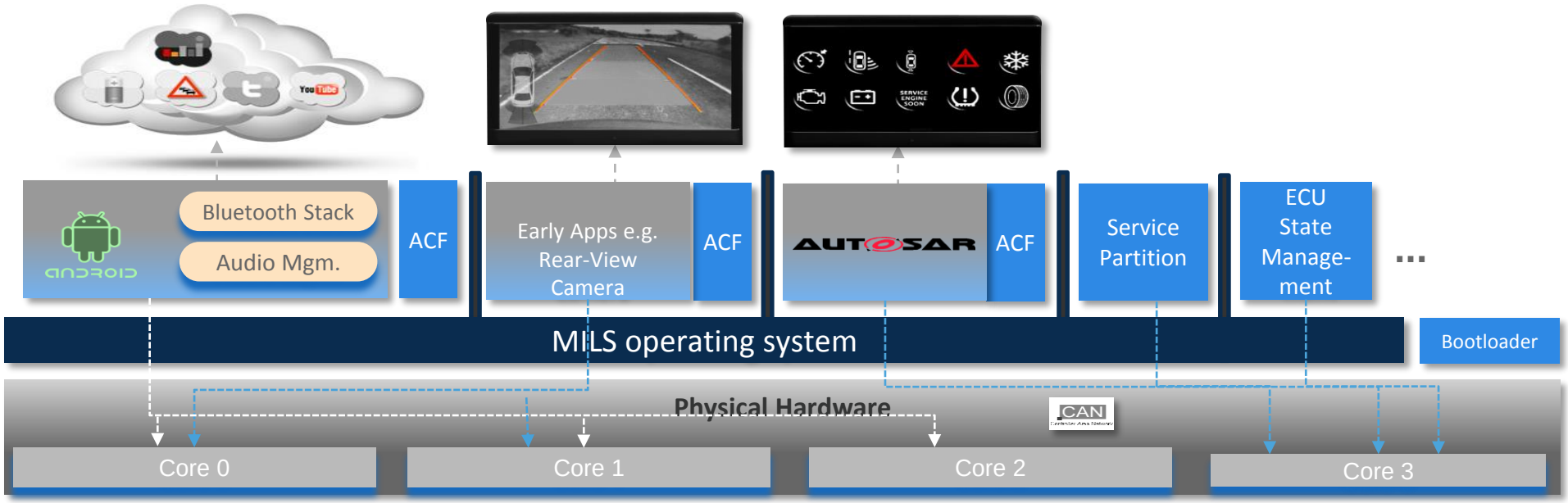


DOWNLOAD

AVAILABLE ON

http://euromils.eu/downloads/2014-EURO-MILS-MILS-Architecture-white-paper.pdf

Quick Example Automotive:
Secure Android-based Head-Unit + Payment Services



Challenge: Developing an Assurance Case

- **Challenge: Develop assurance considering critical low level components such as hardware and system software**
- **Amount of software used in a typical AI/ML project is huge**
  - Avionics system can do it but it is expensive
  - However, Boeing 737 Max 8 was a very disappointing deviation of the industry norms
  - It is yet too see how a assurance case for autonomous driving would look like
- **An assurance case should be always very close to the design and implementation**
  - There are approaches for weaving assurance case from designs
    - Some domains can question these approaches
  - Formal modelling of assurance case with links to design
- **Formal verification is still challenging for “hardly abstractable” systems**

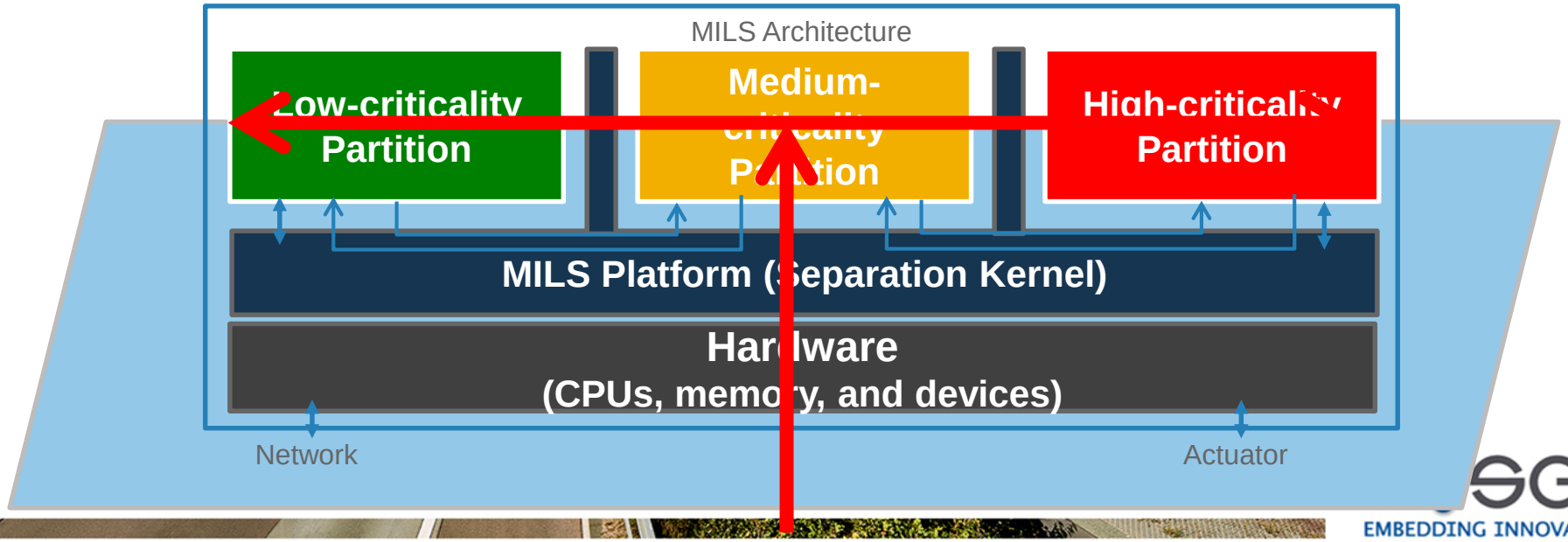
- **Design approaches can support/ease assurance case development, e.g.**
  - MILS as used in avionics, railway, security CPS

SYSGO EMBEDDING INNOVATIONS

Compositional Certification: Scenario-T

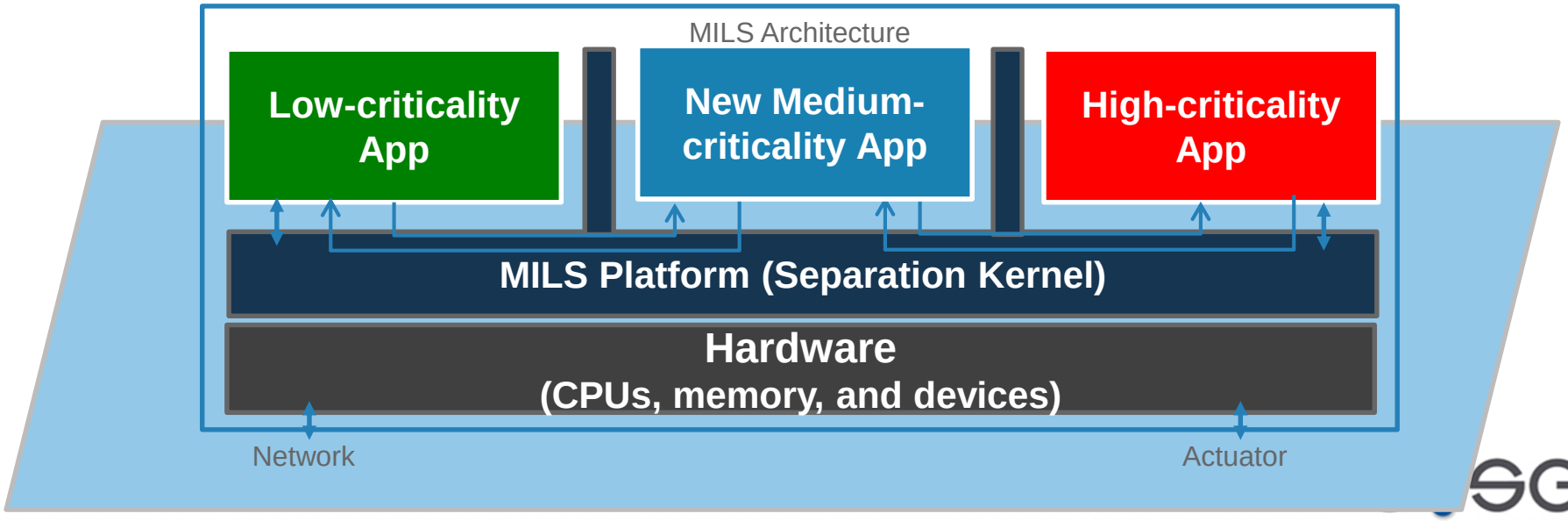
- The core is Separation Kernel
- Components under certified composition
  - Hardware, Separation kernel, Applications

T - composition



Compositional Certification: Scenario-P

- **Puzzle Composition**
  - Exchange system component with interface/function-compatible one
  - Use-cases
    - Product from Vendor-A is replaced by product from Vendor-B
    - Flexible in-the-field update



MILS Activities

CCUF
CITADEL
certMILS

MILS.COMMUNITY

selected members and research partners

AIRBUS
altran
UniControls
Transport and Industrial Control Systems
IK4 IKERLAN
Research Alliance
T · · Systems ·
Continental
Universität Rostock
Traditio et Innovatio
fortiss
TU/e Technische Universiteit Eindhoven University of Technology
THALES
mcn
Always reliable. Always ahead.
THE Open GROUP
OPENSYNERGY
@sec
the information security provider
NXP
SYSGO
EMBEDDING INNOVATIONS
FONDAZIONE BRUNO KESSLER
Schneider Electric
FREQUENTIS
UNIVERSITÉ PARIS SUD
TECHNIKON
TTTech
KASPERSKY lab
EPOCHE & ESPRI
Fraunhofer
ezü elektrotechnický zkušební ústav

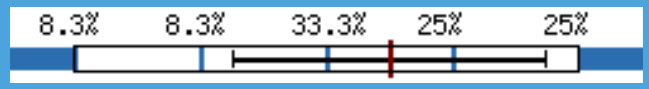
SYSGO EMBEDDING INNOVATIONS

CCUF: SK TC/WG: Updates 2019

- **CCUF SK TC/WG**
  - Members: from France, Germany, Italy, Poland, USA, Denmark, Singapore, China, USA
  - Separation kernel vendors, System Integrators, OEM and Tier-1/2. Security Evaluators, Certification agencies, National Agencies, Universities
- **Questionnaire on separation kernel PP**
  - Integration of feedback on separation kernel PP
- **Interaction with CCUF Virtualization PP**
  - Discussion
    - One core part of hypervisors is isolation by access control via reference monitor
    - This holds for large hypervisors, MILS separation kernels, HW-implemented hypervisors
    - Discussion on role of/need for remote administration built in which is built into many large hypervisors

Questionnaire

Do you already have experience with the CC certification of a Separation kernel?



none — extensive

- **certMILS, Univ of Rostock**
- **Persona:**
  - 11 answers
    - *separation kernel developer* (4)
    - semiconductor/HW platform/SoC provider (2)
    - followed by "*CC certifier*", "*certification body*", "*security researcher*", "*someone who has worked extensively on separation kernels, ISO 15408, etc.*", "*possible stakeholder (interested on separation kernel products, interested by CC certifications*"
- **Objectives**
  - Valid[illegible]n understandability and modularity, validate focus on access control, find [illegible] partitioning
- **Insigh[illegible]**
  - Acce[illegible])
    - modular approach and
    - focus on access control
  - Open points / feedback
    - include core pinning as a time partitioning mechanism
    - Is attacker always sitting within a partition
    - Interest in residual information protection for shared resources

DOWNLOAD

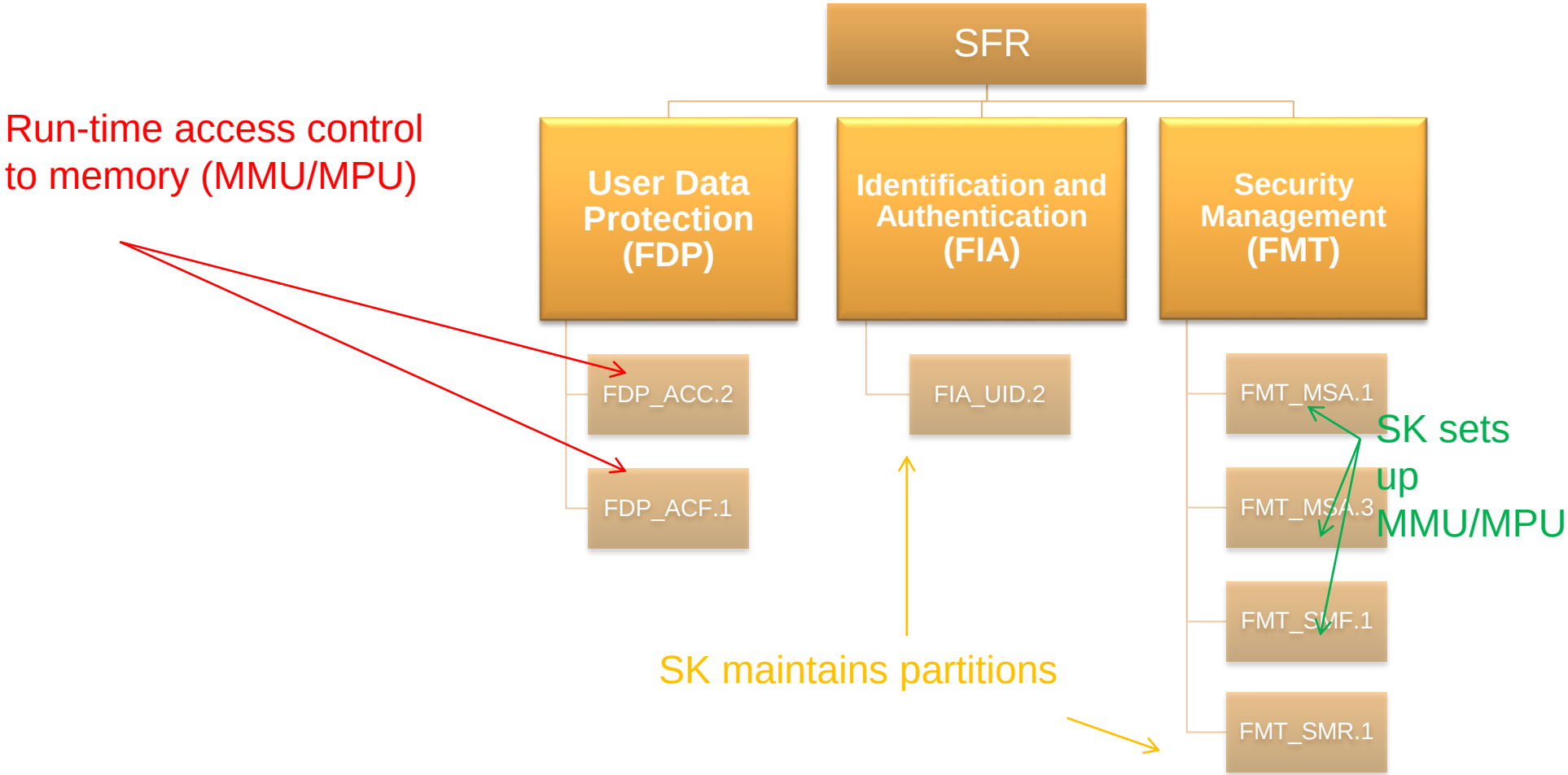
AVAILABLE ON

Summary report: https://zenodo.org/record/2541464

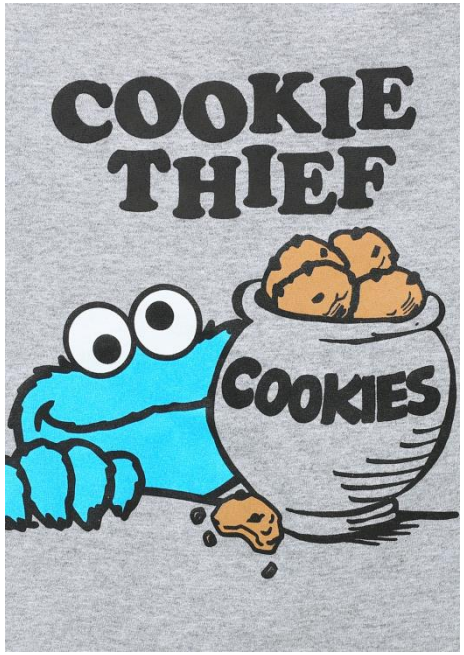
SYSGO EMBEDDING INNOVATIONS

Separation in space

What it would mean in CC Security Functional Requirements



PP SK: Assets and Attackers



Assets

- Memory
  - Physical or virtual memory
- CPU time
- Objects, e.g.
  - files, CPU cores, devices, interrupts, communication ports etc.

Attacker

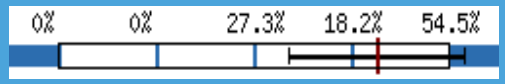
- **Attacker is any application executed in a partition**
  - in a system with privileges (e.g. trusted, non-trusted), it is at least applications in a non-trusted partition

- **Attacker Resources**
  - Arbitrary amount of time to examine offline and attack the embedded component's physical and logical interfaces both online.
  - Binary code of the separation kernel and possibly also its source code.
  - Commercially and/or publicly available software, knowledge, equipment

SYSGO
EMBEDDING INNOVATIONS

PP Extensions/Modules

Do you agree with the strategy to produce a modular separation kernel PP and its proposed scope?

N 

Y

Follow CC 3.1 rev 5 module approach

- **Identified modules**
  - Cryptographic services
  - Secure boot
  - Sec
  - Sto
  - Rea
  - Network interface partitioning
  - Information flow
  - Management module
  - Secure audit
  - I/O MMU
  - HAL

Pick&Mix

Base
MILS Separation Kernel
Protection Profile

DOWNLOAD

AVAILABLE ON

https://zenodo.org/record/2586507

ST

SYSGO
EMBEDDING INNOVATIONS

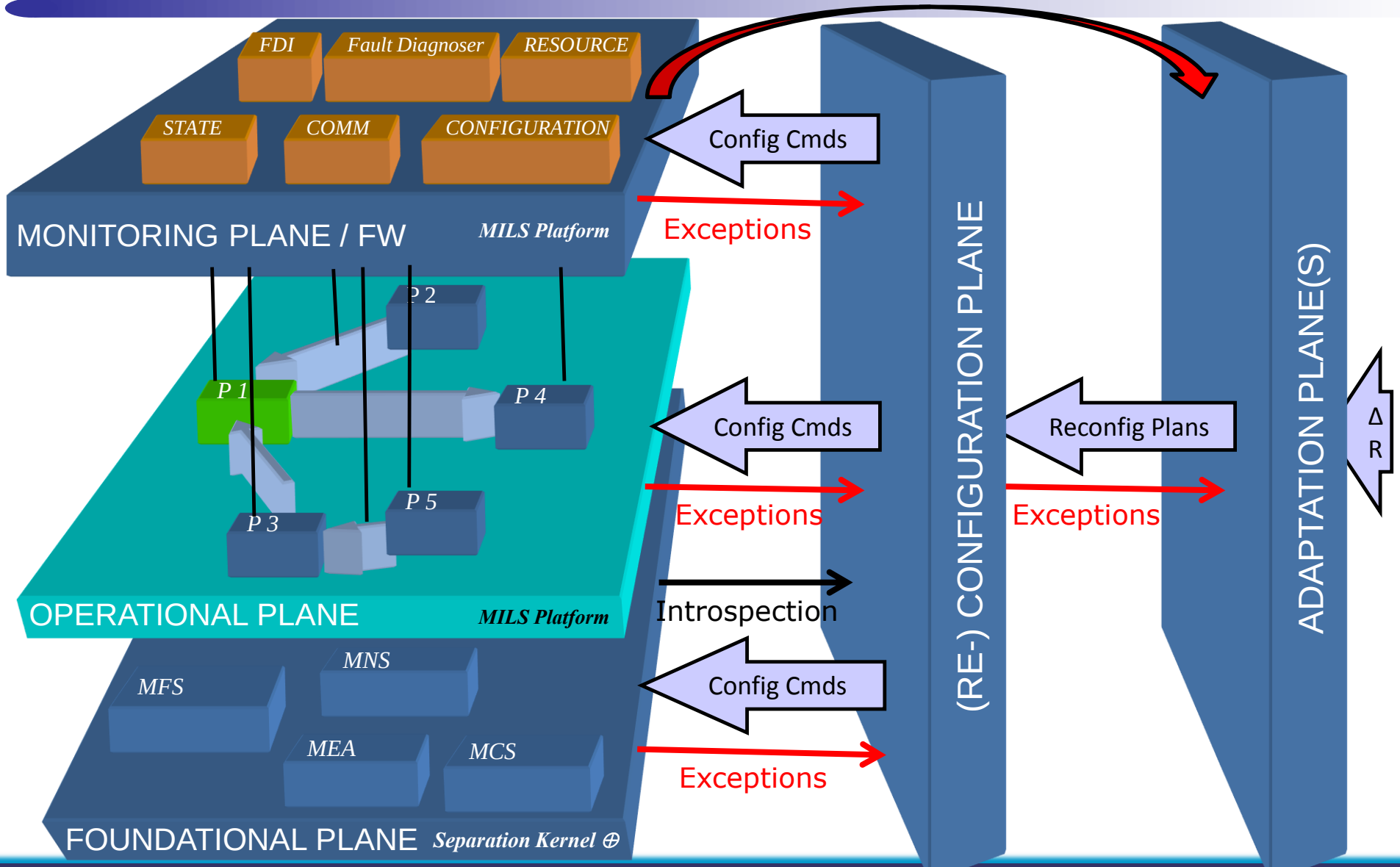
CITADEL: Dynamic MILS Platform

- MILS platform capable to reconfigure dynamically
  - Separation kernel reconfiguration extensions
  - TSN Network reconfiguration extensions
  - Runtime agents for resource management policy enforcement
  - Runtime of the Dynamic MILS Platform acts as a Reconfiguration Reference Monitor, and includes:
    - Configuration Change Agent
    - Reconfiguration Policy Agent

CITADEL: Adaptive MILS Systems

- Adaptive MILS system includes mechanisms to utilise dynamic reconfiguration to maintain safe and secure operation despite environmental change or failures
  - Analog of the lower-level reconfiguration runtime plus ability to plan configuration changes to meet conditions
  - Mechanisms to monitor operations and environment change
  - Adaptation Change Agent – runtime subject authorised to invoke the MILS Platform Configuration Change Agent
  - Adaptation Policy Agent– a runtime mechanism that decides whether a pending reconfiguration plan is consistent with the overarching operating policy

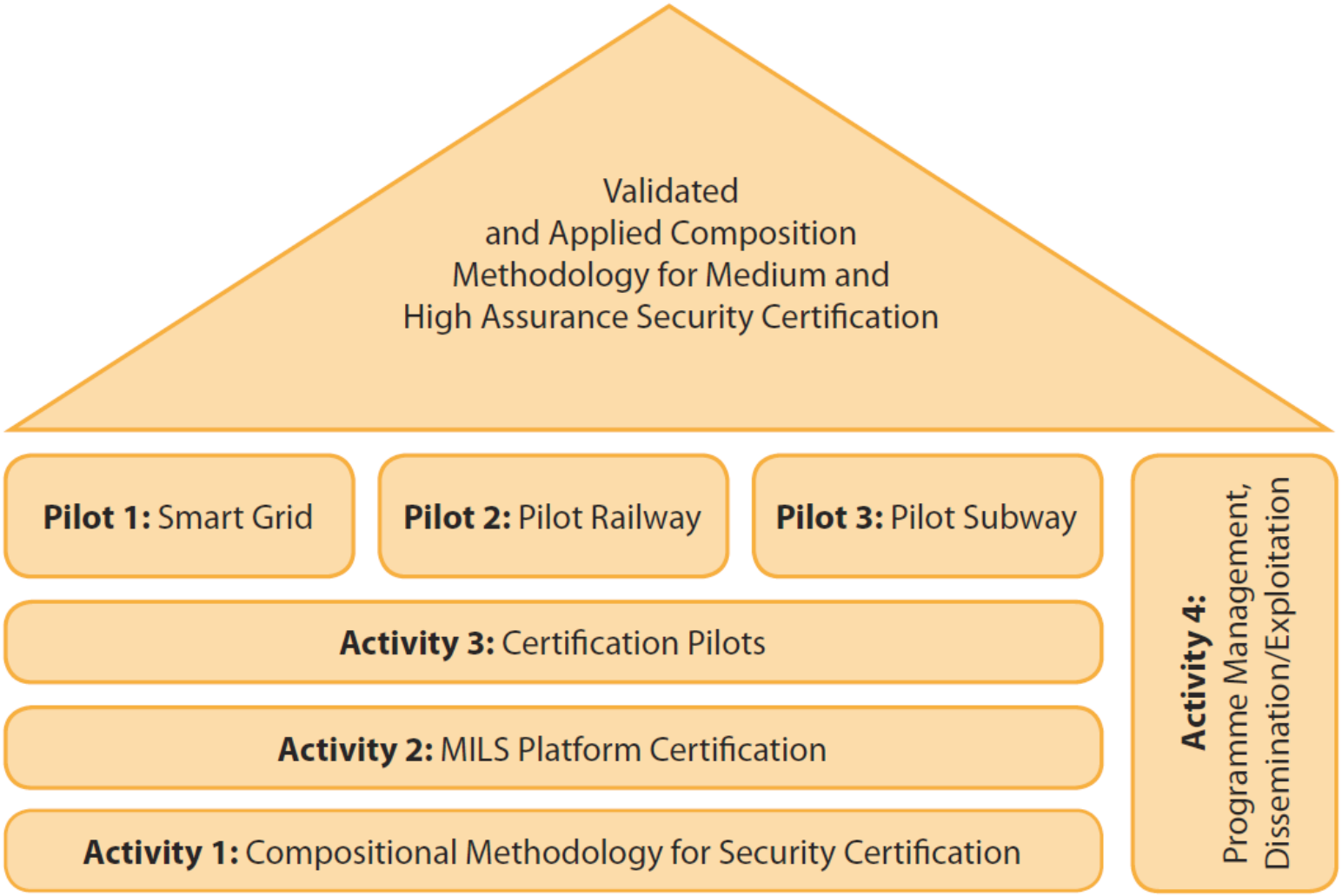
CITADEL: Interaction of Monitoring, Configuration and Adaptation Planes



Implemented Demonstrators

- Air Traffic Management (FREQUENTIS)
  - Voice and Data information flow via operators and towers
  - Mixed-critical application, e.g. time sensitive and overview map
- System-Fail-tolerance for a Subway Control System (UniControls)
  - Introspection of nodes
  - Detection of fails and “respawn” applications

certMILS Project Overview



Objectives

Objective 1. Transfer know-how in compositional safety certification to security certification

Objective 2. Make certification of composed systems affordable

Objective 3. Preservation of certified assurance throughout operational deployment

Objective 4. Involvement of all stakeholders in different industry domains

Objective 5. Certified European MILS platform

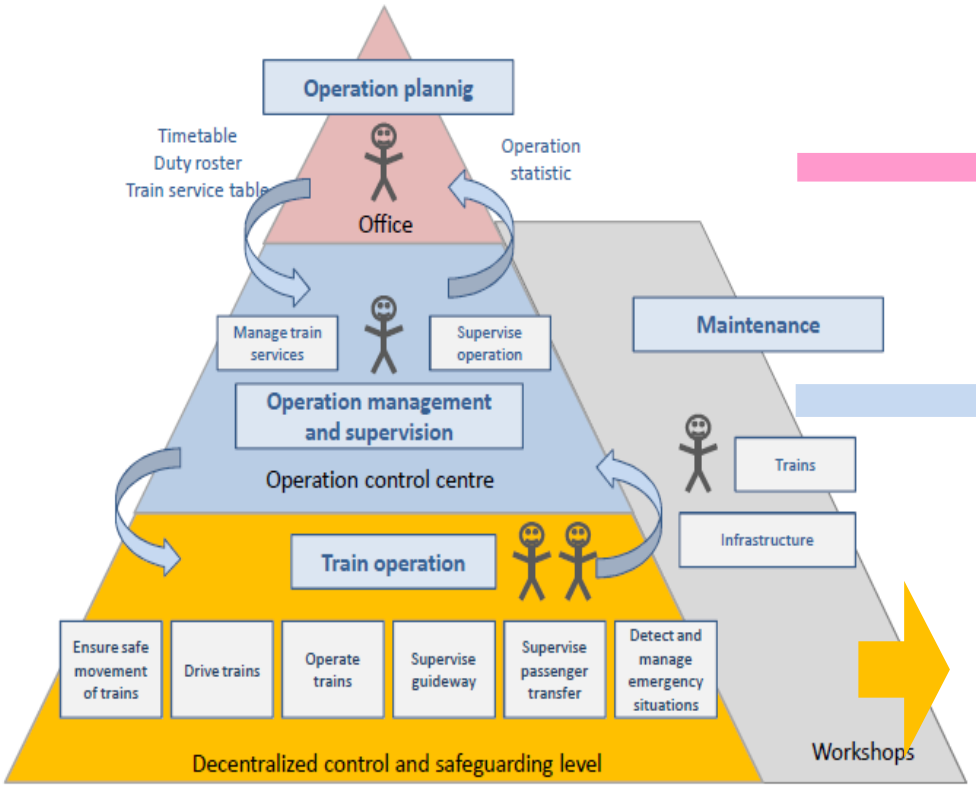
Objective 6. Develop and apply compositional certification methodology on three industrial pilots

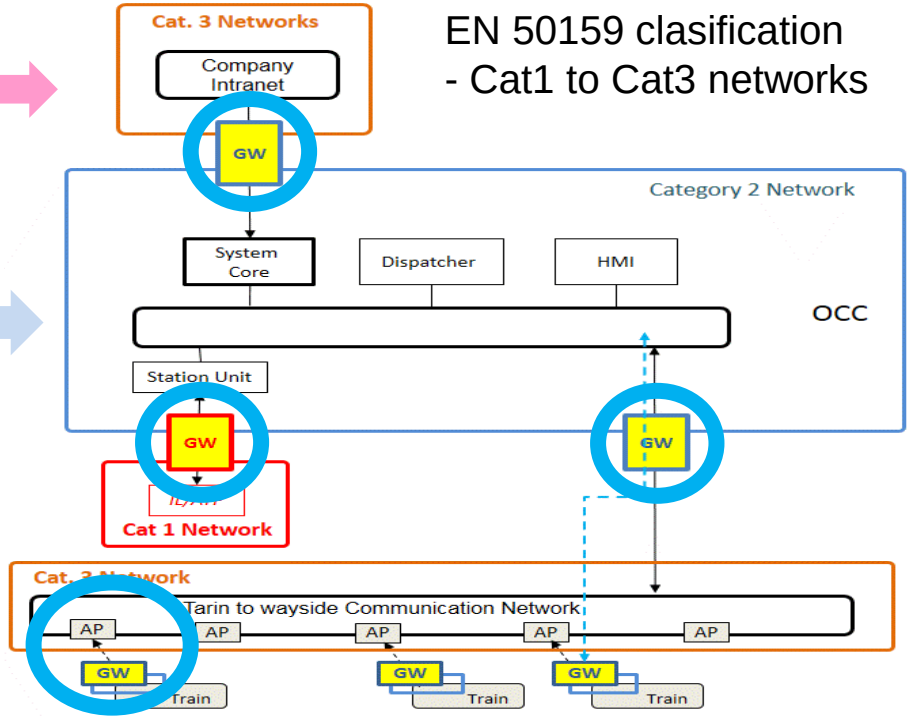
PP Interop

Objective 7. MILS Platform Protection Profile

Objective 8. Guidelines and templates for MILS certification

Pilot 1: Prague Subway – Mixed criticality gateway





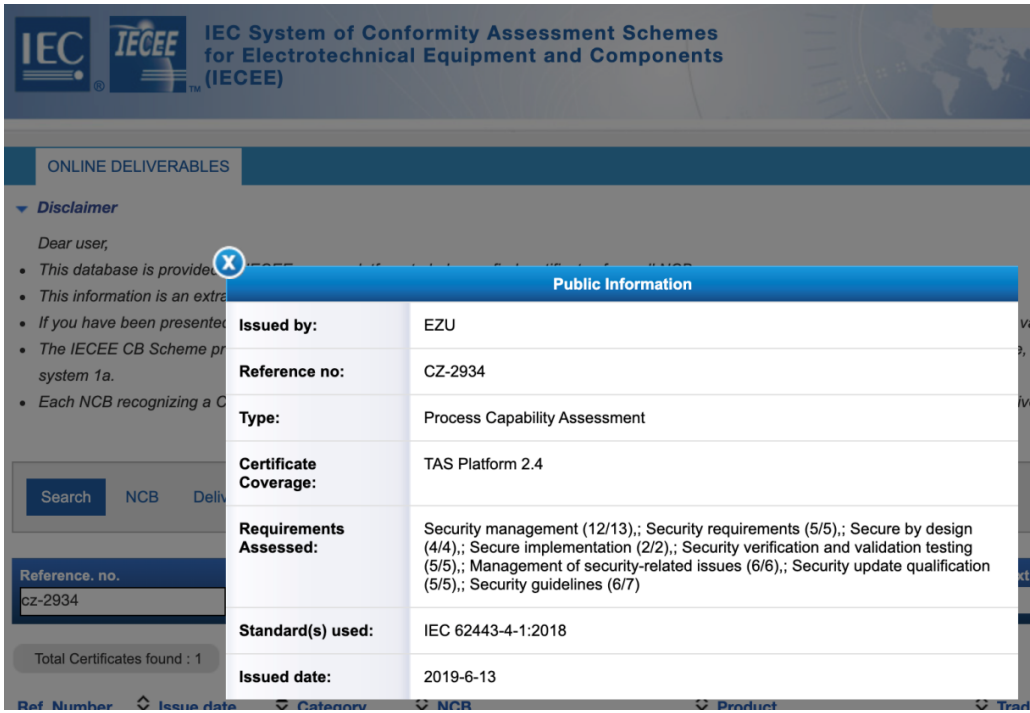
EN 50159 clasification
- Cat1 to Cat3 networks

EN62290 Standard

Recent Highlights

- Developed approach for compositional assurance

- Compositional assurance is being applied in two railway and one smart grid projects.
  - Systems have been developed
  - Compositional certifications are in progress



- First world wide IECEE 62443 4-1 certificate achieved

Summary

How To Be Involved and Contribute

- **Join MILS.community**
  - www.mils.community
  - All MILS topics
- **Annual MILS workshop**
  - workshop.mils.community
- **Separation Kernel Standardisation WG**
  - Join CCUF WG/TC
  - www.ccusersforum.org
  - **Next meeting: Spring, 2020**
- **Certification Updates**
  - International Common Criteria Conference
  - **20-22 Oct 2020, Madrid, Spain**

SYSGO EMBEDDING INNOVATIONS

SYSGO

EMBEDDING INNOVATIONS

Thank you for your attention!

More information on www.sysgo.com