



EURO-MILS: Building and certifying modular secure systems

Sergey Tverdyshev, SYSGO
The Euro-MILS consortium

MILS Workshop 2016
19.01.2016 Prague

www.euromils.eu



EURO-MILS Consortium

14 Partners from 6 Countries



Open Universiteit
www.ou.nl



EURO-MILS: Strategy and Objectives

- High-criticality networked cyber-physical systems
 - Drivers are avionics and automotive
 - EURO-MILS delivers cross-domain solutions

- Integration and networking requires trustworthy ICT

- MILS Architecture
 - High-assurance security architecture
 - Scalable and affordable security
 - Compositional design, assurance, security

Business and Legal Foundations for Trustworthy ICT

Trustworthy Design by MILS

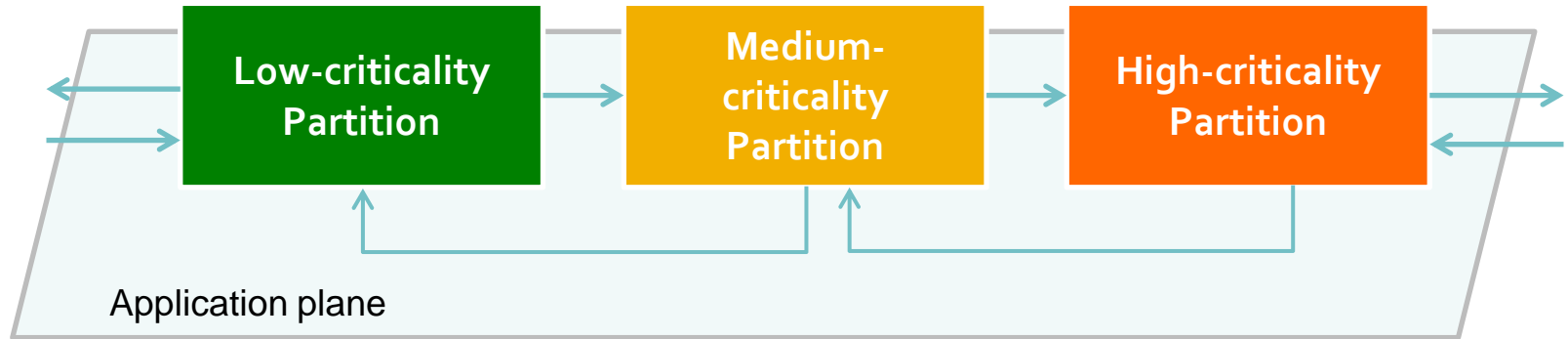
Assurance for End-Users

Trustworthy ICT for networked high-criticality systems

- EURO-MILS: European MILS architecture and certifiable platform

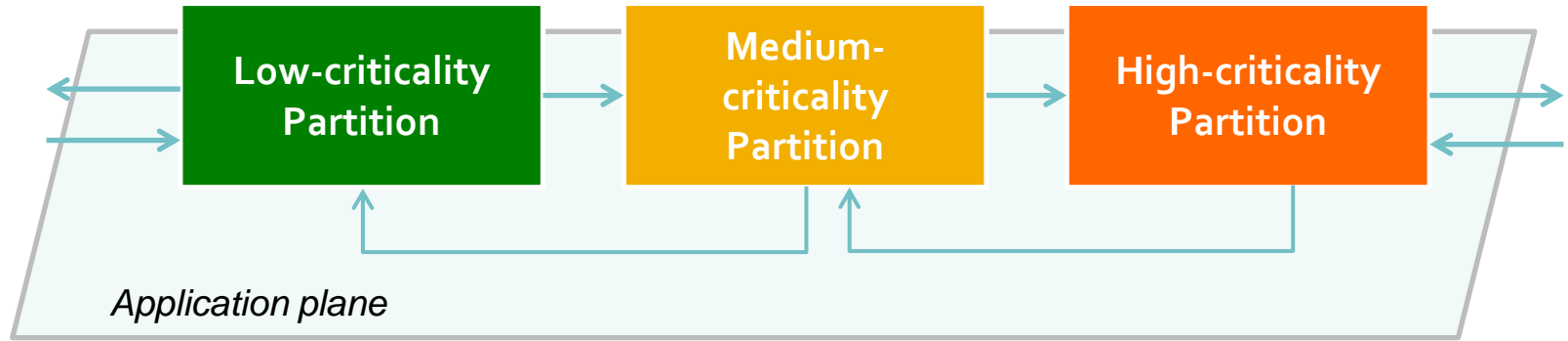
COMPOSITIONAL SYSTEM DESIGN FOR SECURITY AND SAFETY

Developing System Architecture

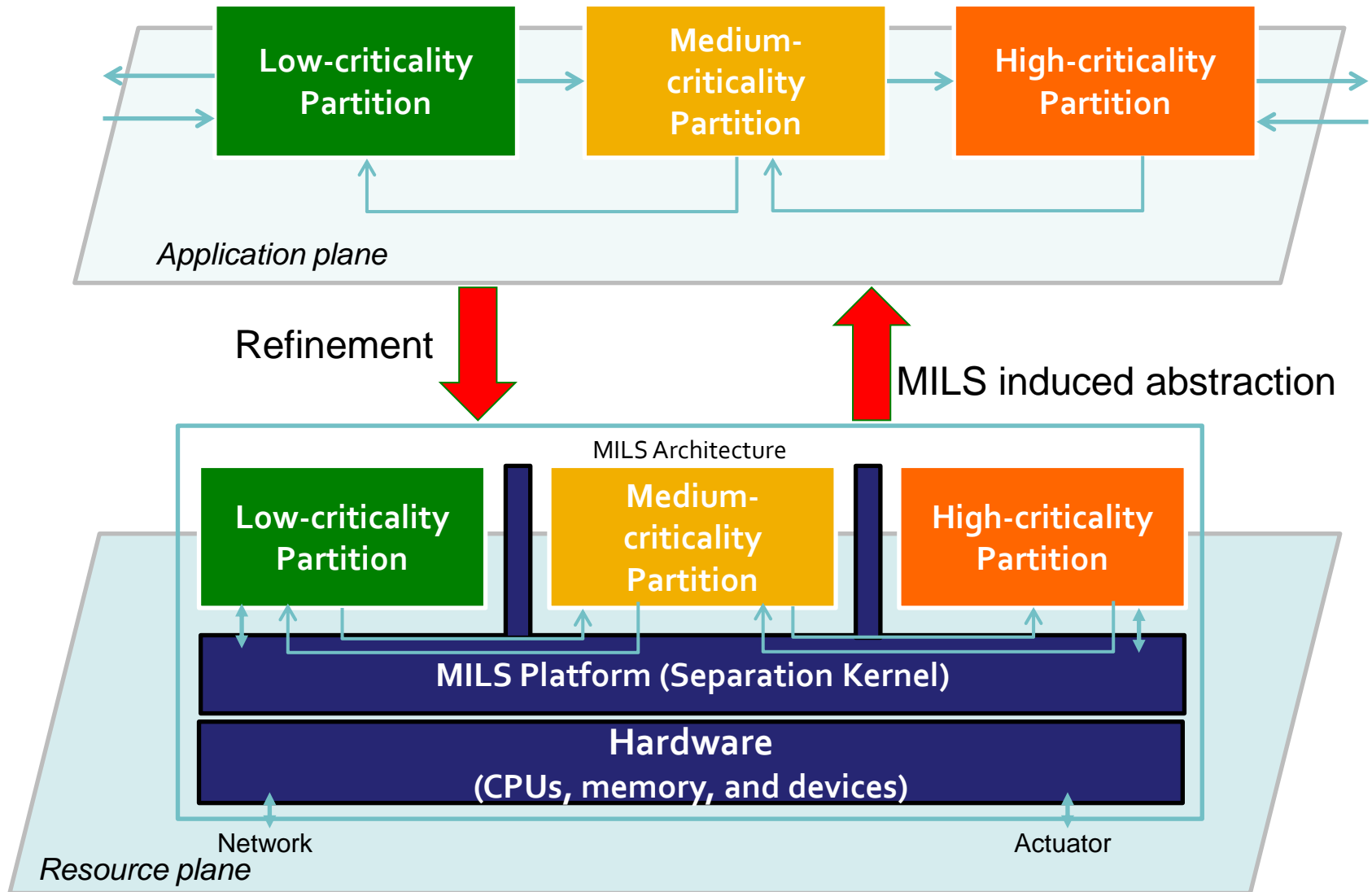


- System is
 - a group of related components that work together
 - possessing a set of properties
- To bring that components to life you need an execution platform
 - Execution platform introduces new components and interfaces
 - Execution platform has (physical) resources
 - Execution platform possesses a set of new properties
 - i.e. refine system design

Developing System Architecture

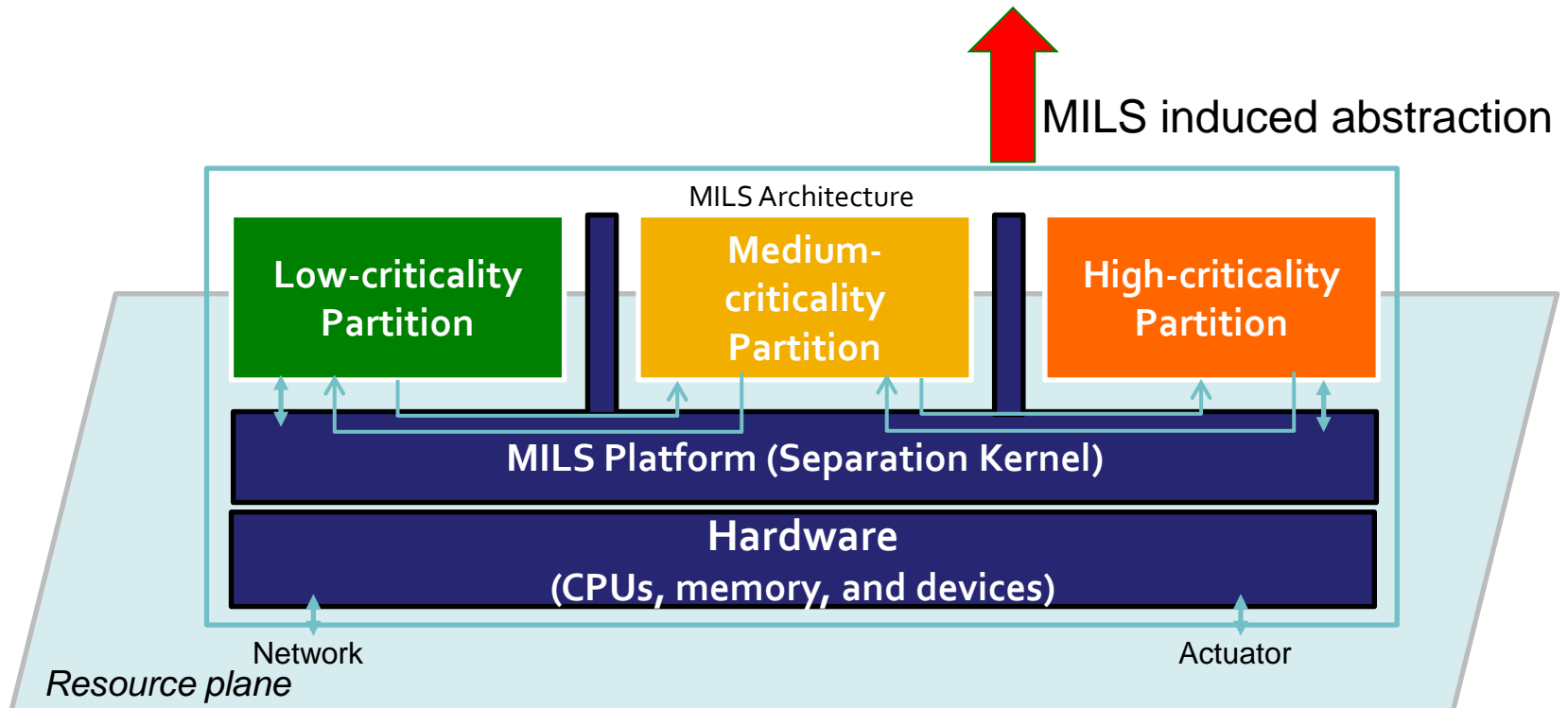


- **Generic problems:**
 - Composition preserving safety, security, assurance arguments
 - Refinement is a composition
 - Mitigate effects of “have to refine”
 - where we need something to execute systems



MILS induced abstraction enables truly **compositional**

- Safety and Security
- Assurance
- Evaluation

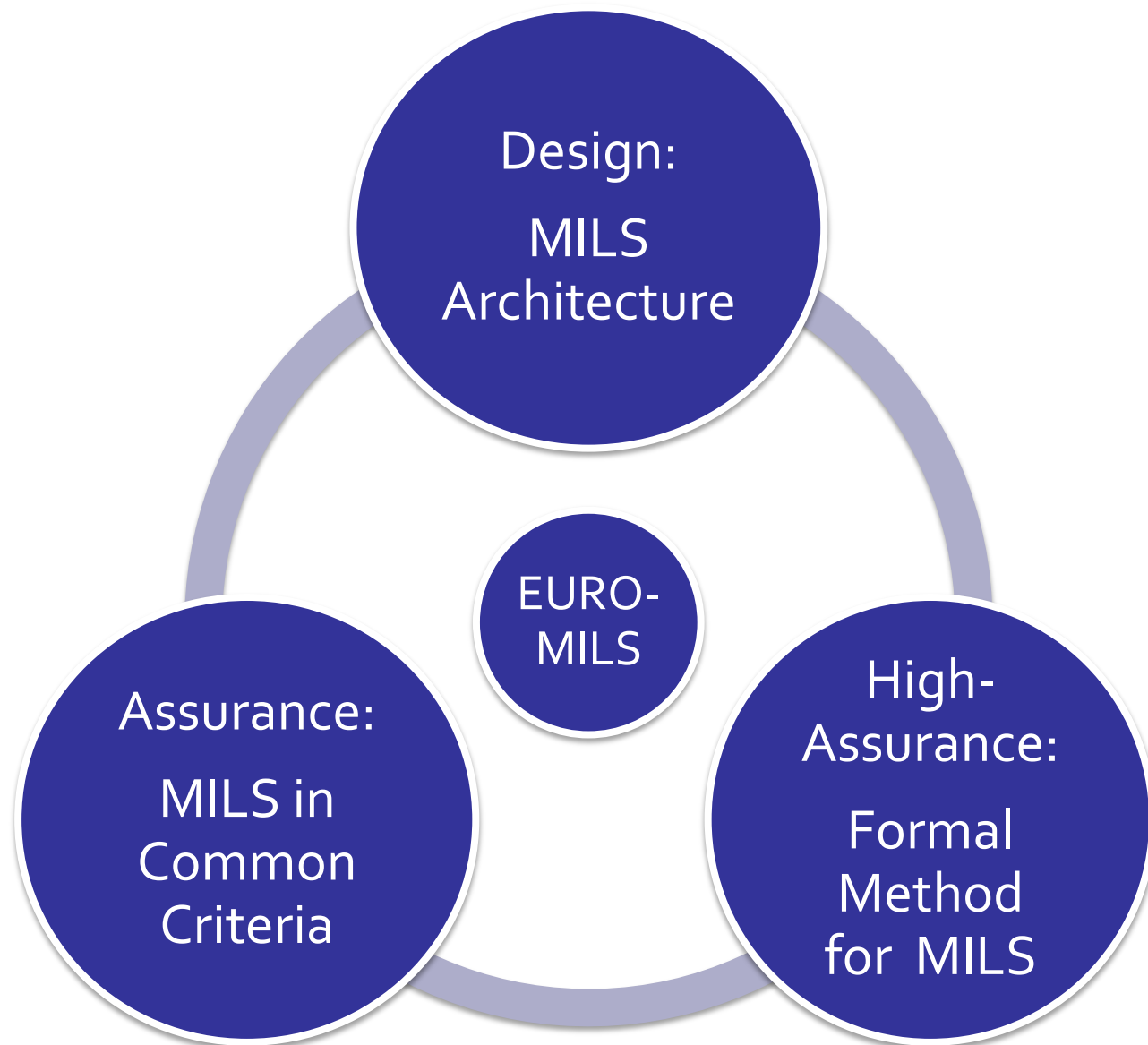


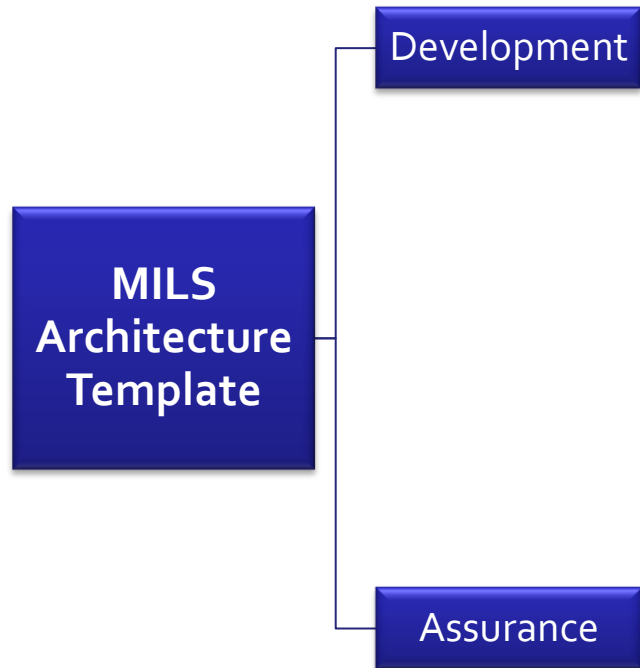
MILS DESIGN AND ASSURANCE FRAMEWORK

MILS Design and Assurance Framework

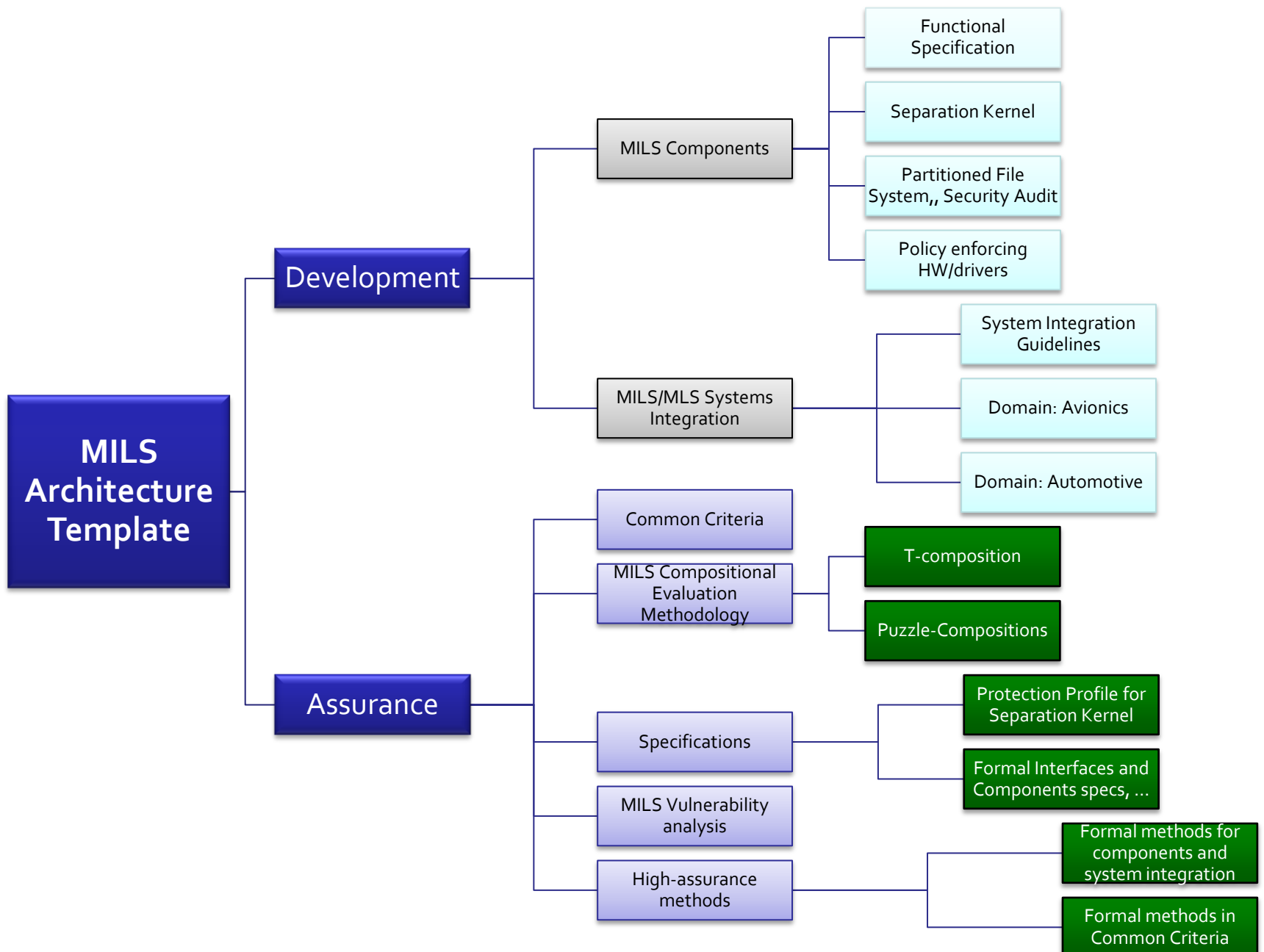
- EURO-MILS focus is to create a framework with focus on
 - Compositional Design/System integration
 - Compositional Assurance
 - Certified MILS separation kernel
- Framework shall cover major life-cycles of system design, integration, validation, evaluation
- EURO-MILS validates framework on industrial applications in avionics and automotive
- **Goal:** create validated MILS Framework as set of
 - specifications, examples, guidelines,
 - evaluation methodology
 - to ease system designing and creating assurance artefacts

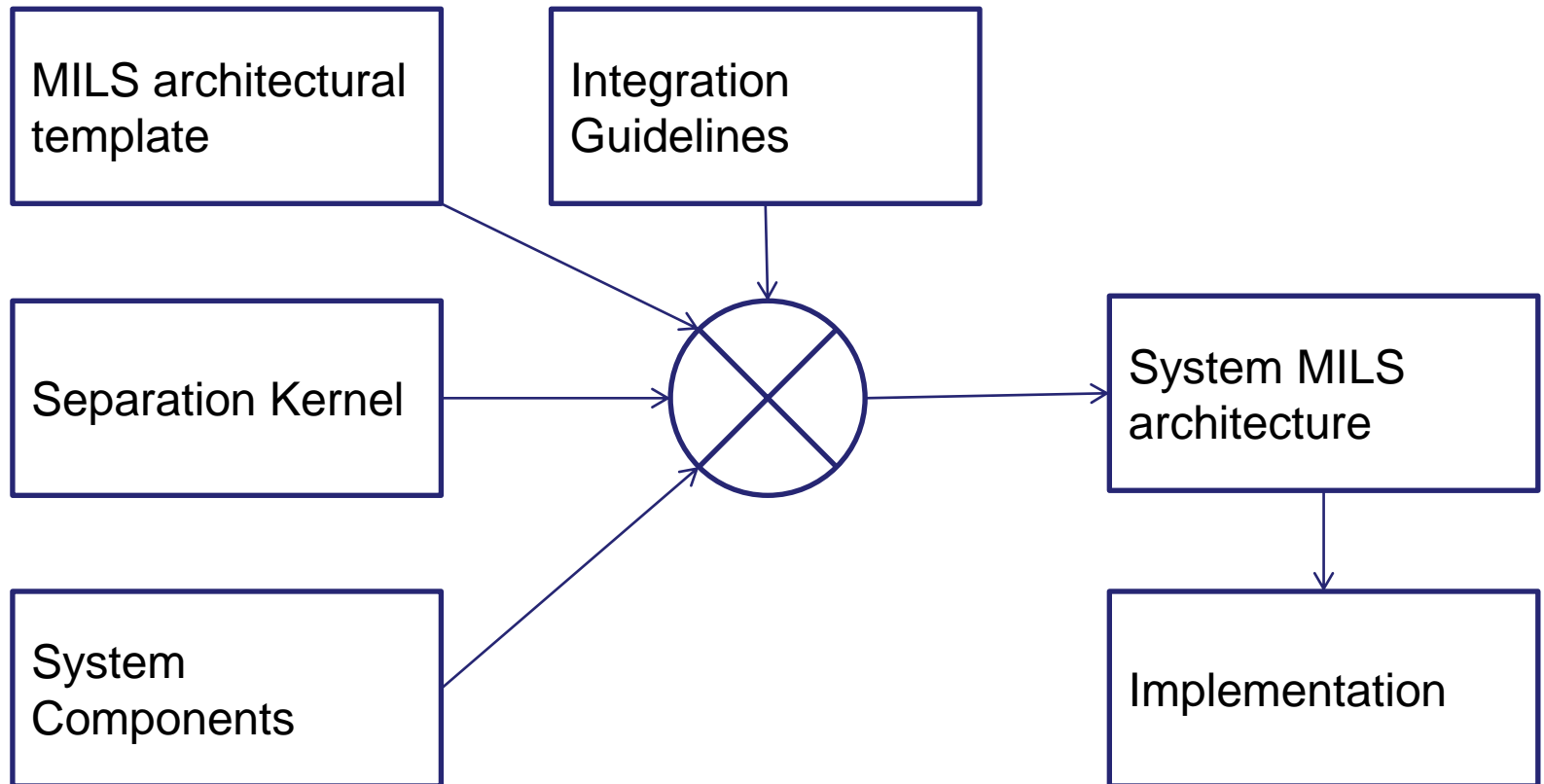
Achieving EURO-MILS Goal



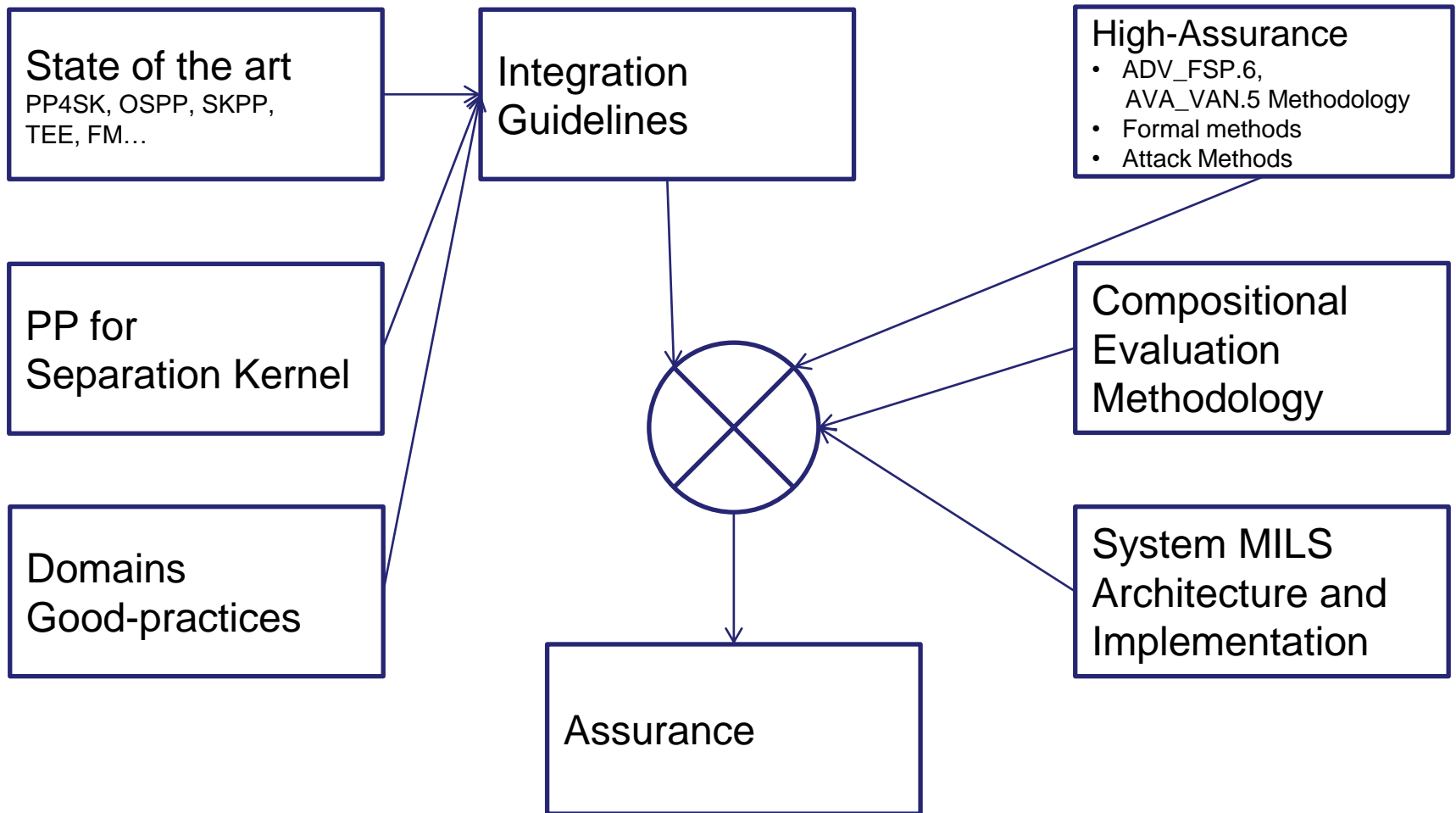


MILS Framework

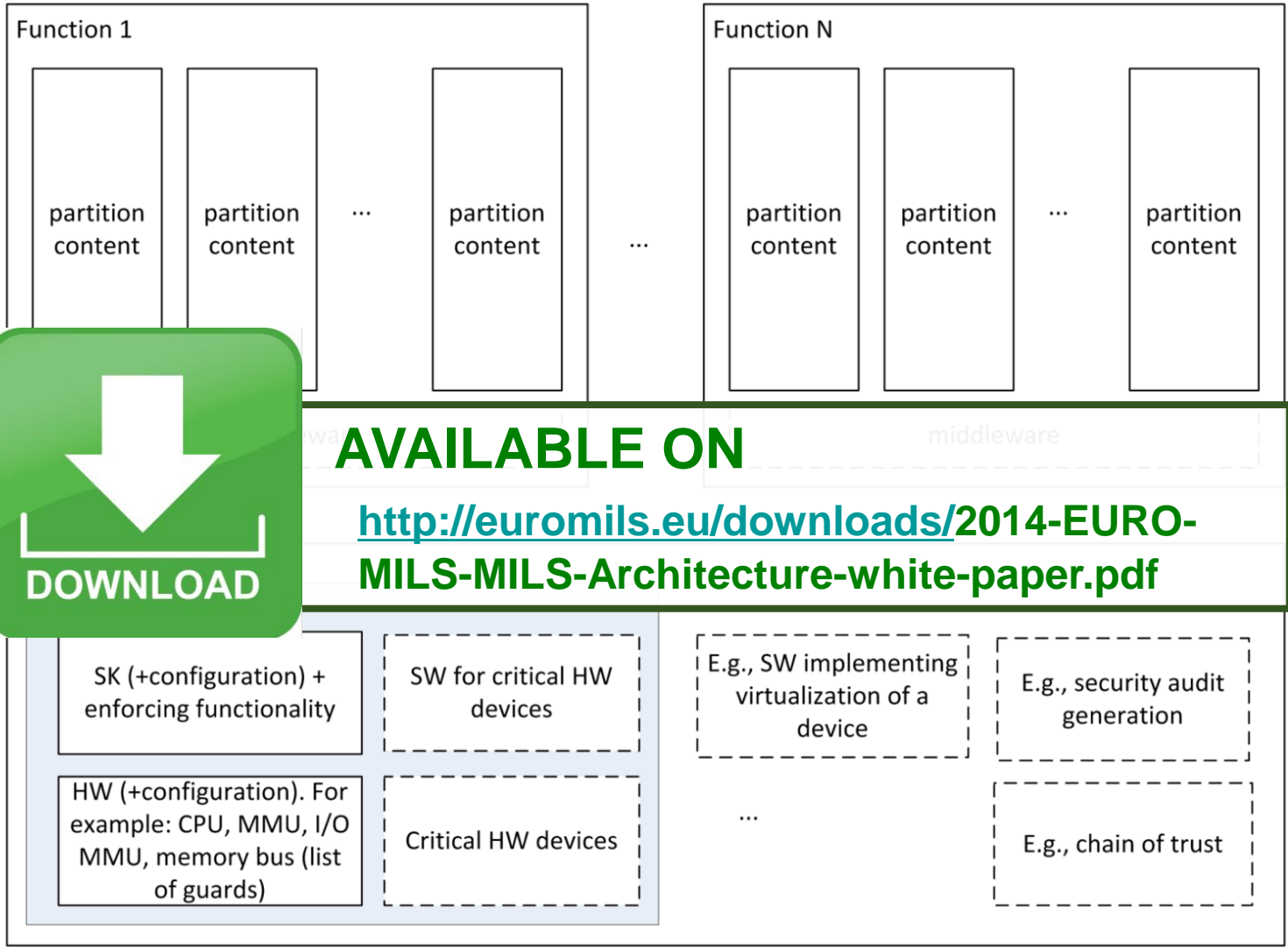




MILS Framework: Assurance track



EURO-MILS RESULTS



EURO-MILS Platform: Common Criteria Certification

An international standard (ISO/IEC 15408) for computer security certification

EURO-MILS Project Goals EAL 5+ (7)

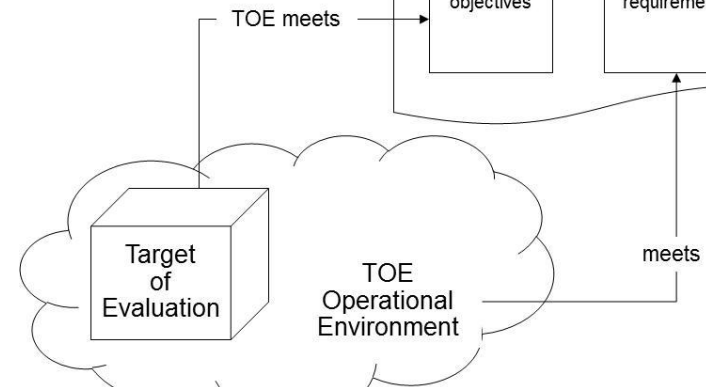
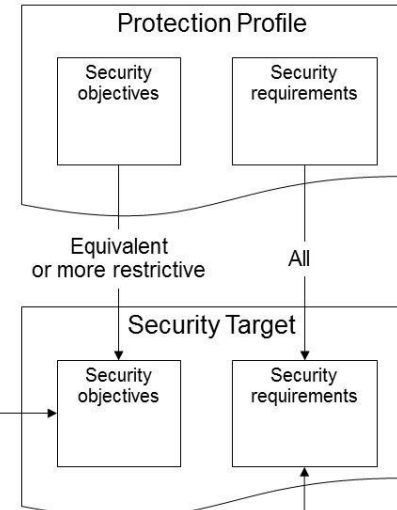
Certification Schemes

- ANSSI (FR) and BSI (GE)

Confidence / Assurance ↑



EAL 7	Formally Verified Design and Tested
EAL 6	Semiformally Verified Design and Tested
EAL 5	Semiformally Designed and Tested
EAL 4	Method. Designed, Tested and Reviewed
EAL 3	Methodically Tested and Checked
EAL 2	Structurally Tested
EAL 1	Functionally Tested

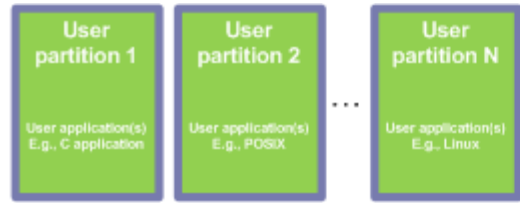


EAL: Evaluation Assurance Level

Protection Profile for Separation Kernel

- **Protection Profile** defines a MILS separation kernel
- **Protection Profile** defines
 - a special kind of operating systems for embedded systems
 - with support for real-time
- **MILS separation kernel** allows separation of applications running on the same platform from each other
 - User applications can be malicious and be developed by arbitrary developers

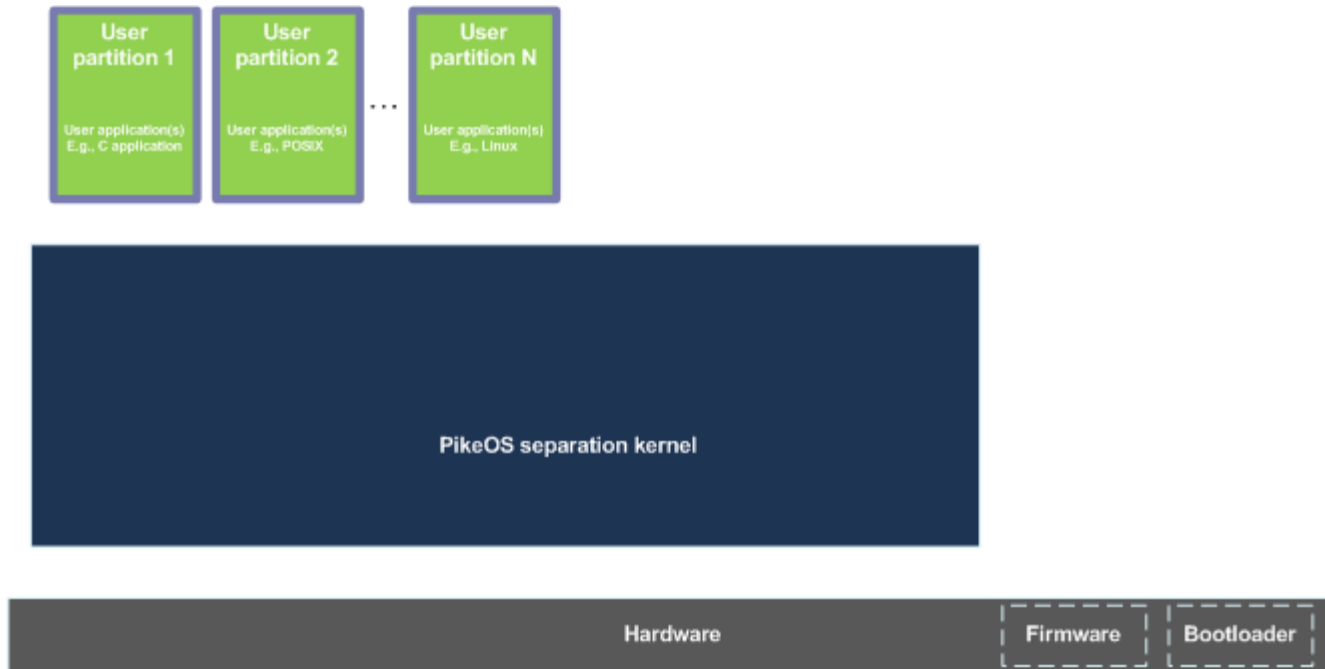
TOE Physical Boundaries



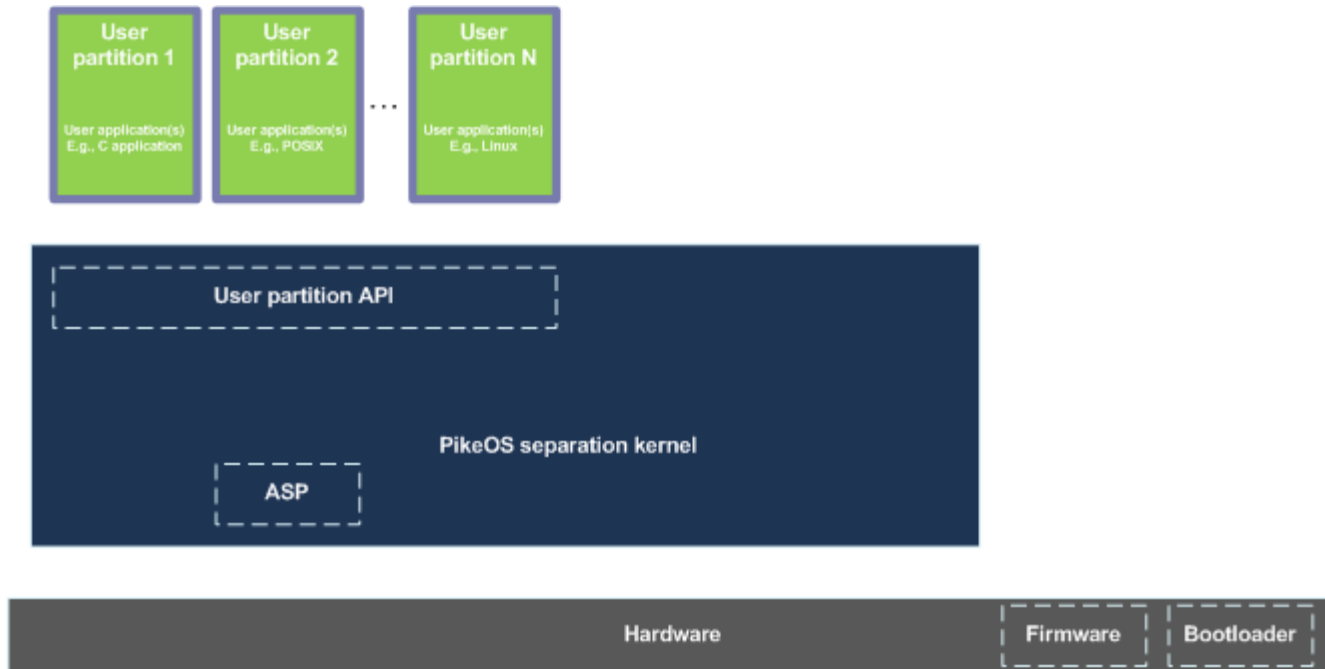
TOE Physical Boundaries



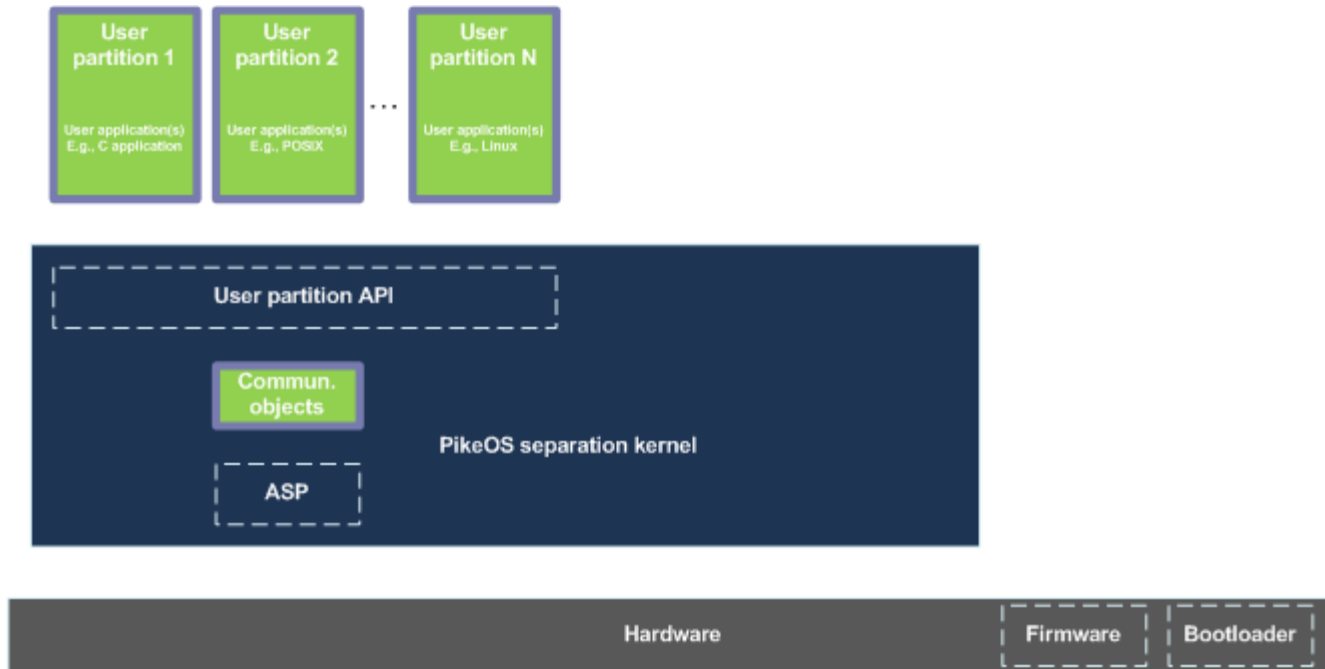
TOE Physical Boundaries



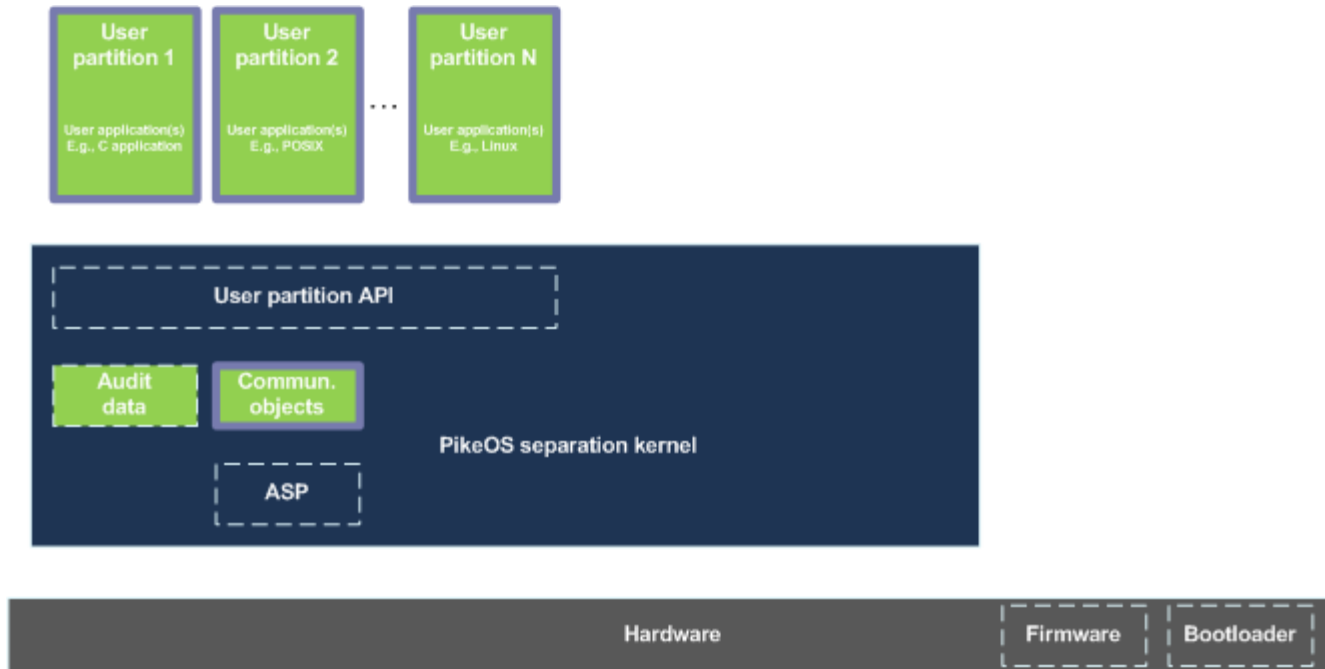
TOE Physical Boundaries



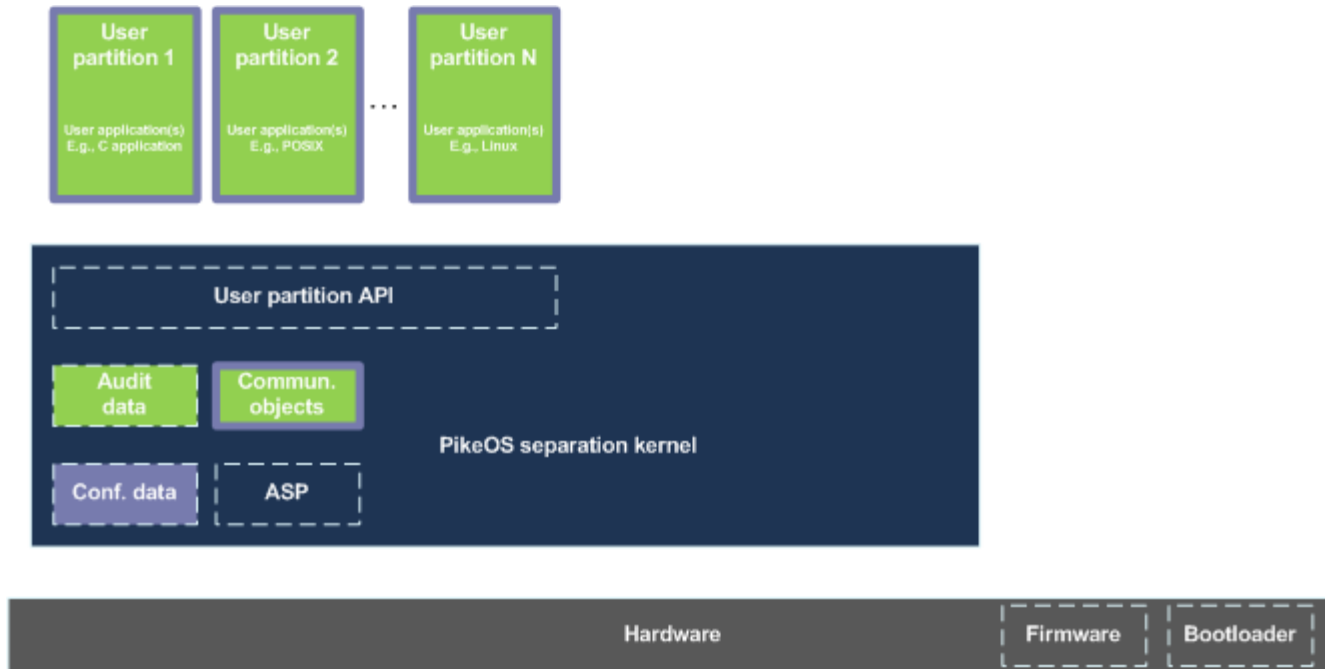
TOE Physical Boundaries



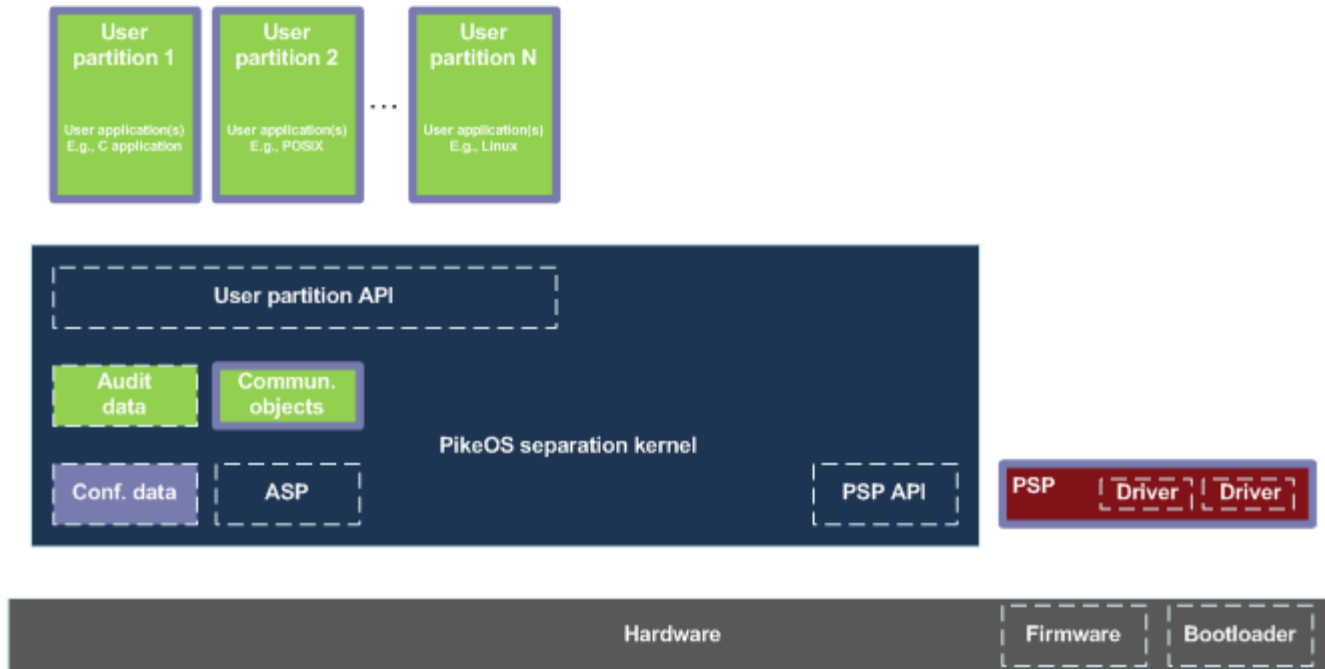
TOE Physical Boundaries



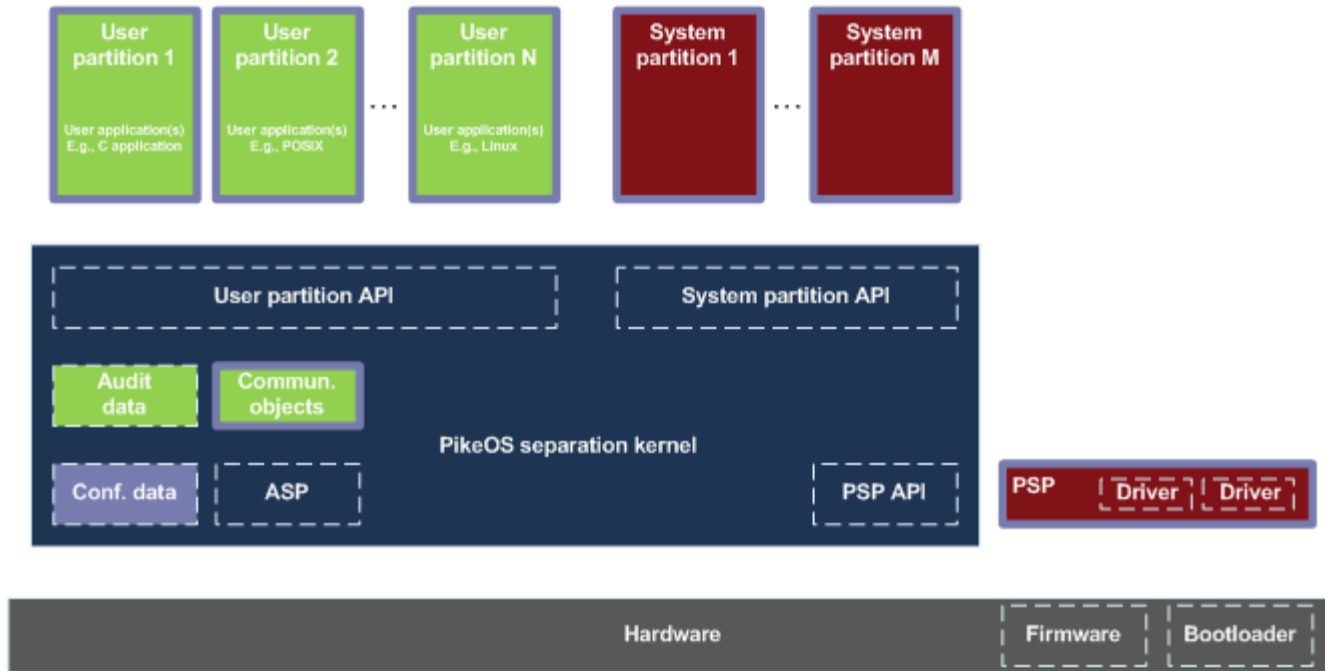
TOE Physical Boundaries



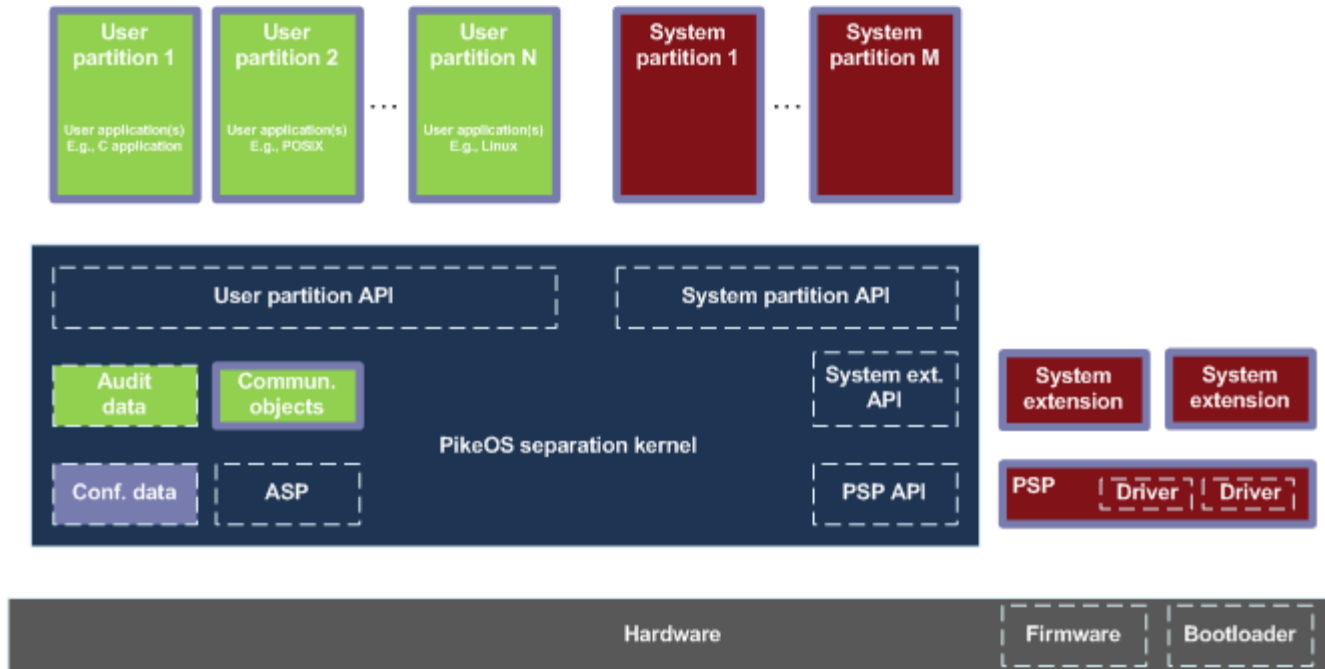
TOE Physical Boundaries



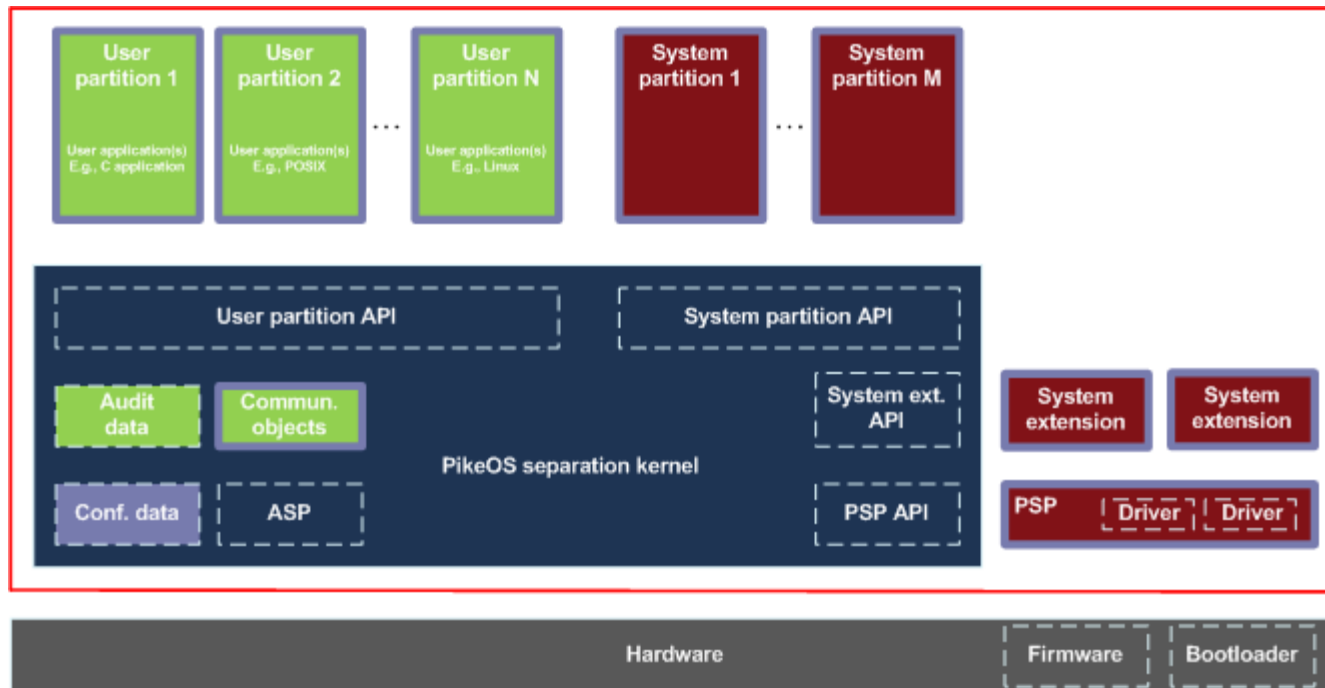
TOE Physical Boundaries



TOE Physical Boundaries

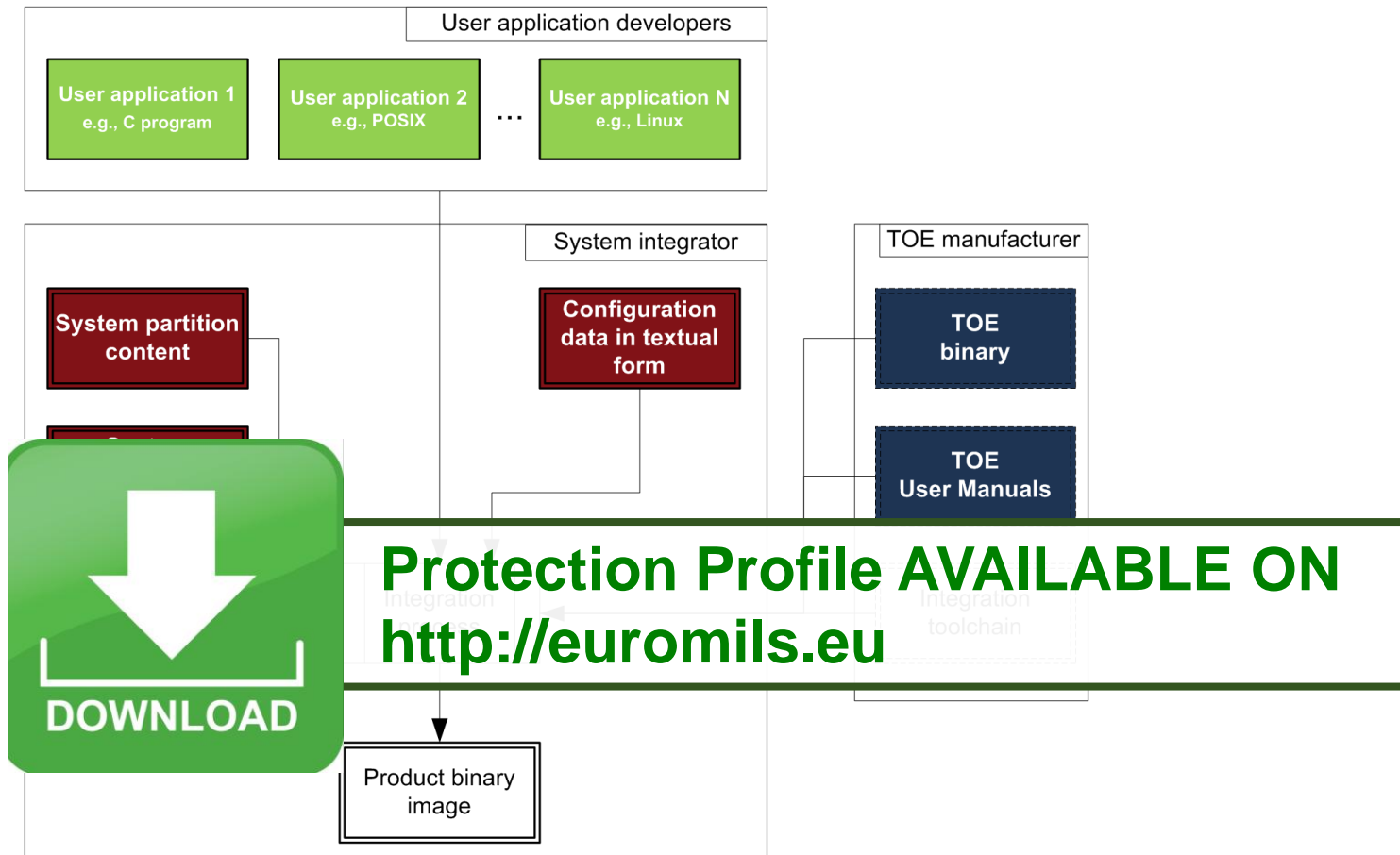






TOE Physical Boundaries



- TSF
- User partition *content*, arbitrary user data; communication objects *content*, arbitrary user data; audit data
- TSF data, incl. amongst others, configuration data and *shapes* of user partitions, communication objects, system components
- System component *content*, user data that has to be approved by the system integrator
- Operational environment
- TOE boundary

System Integration and Roles



-  Parts of the TOE, provided by the TOE manufacturer
-  Integration tool chain, provided by the TOE manufacturer
-  Content of user partitions, this content can be arbitrary (from security point of view) and also be applied by any 3rd party
-  Content of system components and configuration data (in textual form); these elements, even if supplied by a 3rd party, are under sole responsibility of system integrator and shall be approved by him/her; see OSP P.SYSTEM_INTEGRATOR below.

MAIN PP IMPROVEMENTS FROM ITS APPLICATION

FDP_ACC.2.1: The TSF shall enforce the **System Security Policy (SSP)** on **all subjects and ‘user partition content’ as object** and all operations among subjects and objects.

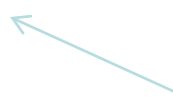
FDP_ACC.2.2: The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1.1: The TSF shall enforce the **SSP** to objects based on the following: **the subjects and objects defined in Section 3.1 and the respective security subject attributes “role”, “subject identity” and object security attributes “asset”, “object identity”**.

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **a subject with the attribute “role” set to “user application” is allowed to treat the object with attribute “asset” set to “user partition content”, if and only if the “subject identity” is in the “user partition shape” linked to the “user partition content”**.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **the subject with the attribute “role” set to “system application” is always allowed to treat the object with attribute “asset” set to “user partition content”**.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.



2013 claim:
access
control
enforced by
MMU (not
done by OS)

2015:
MMU
config
done by
OS

FMT_MSA.1.1: The TSF shall enforce the **SFP-SEC-ATTR** to restrict the ability to *read and write* the security attributes **role, subject identity, object identity, and SSP enforcement data** to the TSF acting on behalf of user applications.

FMT_MSA.3.1: The TSF shall enforce the **SFP-SEC-ATTR** to provide **well-defined** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow **no one** to specify alternative initial values to override the default values when an object or information is created.



FMT_MSA.2.1: The TSF shall ensure that only secure values are accepted for security attributes: **SSP enforcement data.**

Some dynamic aspects are not implemented by other separation kernels, if FMT_MSA.2 at all in PP then make explanatory note that not all systems need to implement it.

SSP

- System Security Policy
- configuration of separation kernel
- Defined by system integrator

SFP

- Security Functional Policy
- set of rules in SK implementations parameterized by SSP

The behaviour of SK depends on both SFP and SSP

6.1.3.2.1 FDP_ACF.1/AS.COMMUN_OBJ_CONT for Asset: ‘Communication Object Content’ as Object

Hierarchical to: No other components.

Dependencies: FDP_ACC.1: hierarchically fulfilled by FDP_ACC.2/AS.COMMUN_OBJ_CONT; FMT_MSA.3: fulfilled by FMT_MSA.3.

SFP

FDP_ACF.1.1: The TSF shall enforce the **SFP-COMMUN-OBJ** to objects based on the following: **subject security attributes “role”, “subject identity” and object security attribute “object identity”**.

SSP

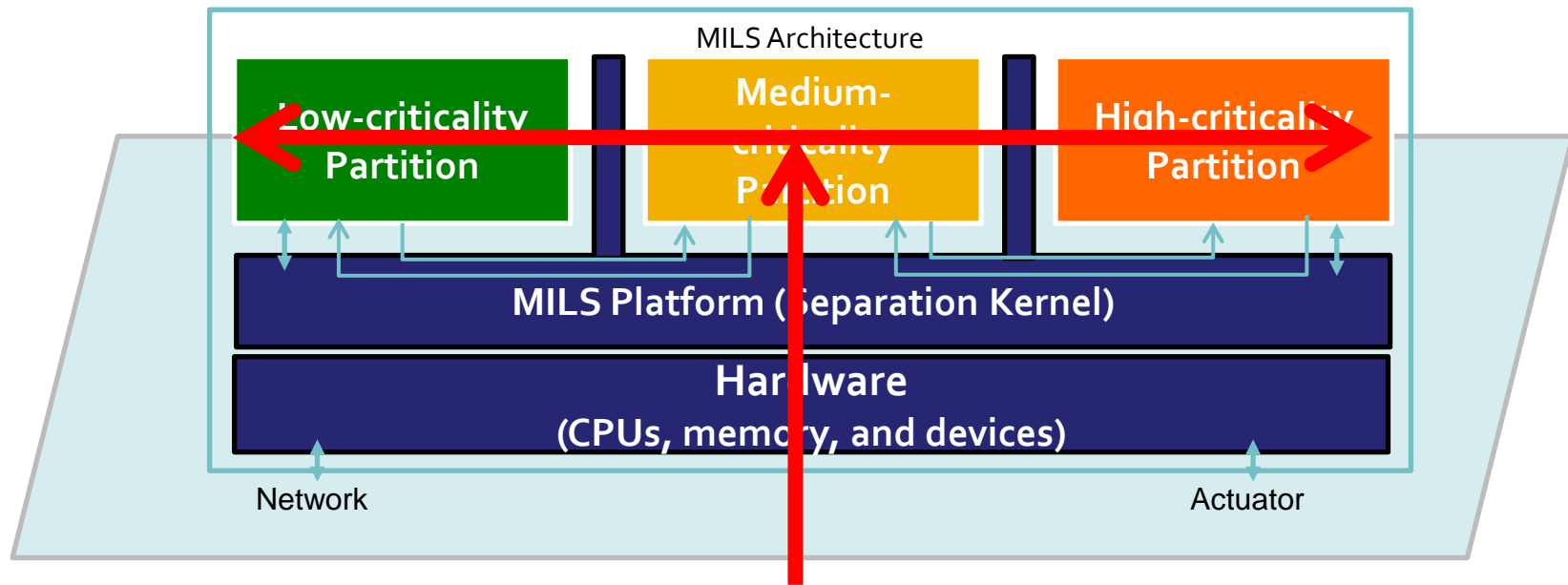
FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **A subject with the attribute “role” set to “user application” is allowed to treat the object of asset AS.COMMUN_OBJ_CONT, if and only if the attributes “subject identity” and “object identity” have values for which the SSP allows treating this object by this subject.**

COMPOSITIONAL EVALUATION

Compositional Certification: Scenario-T

- MILS architecture is the enabler for high-assurance compositional certification
- The core is Separation Kernel
- Components under certified composition
 - Hardware, Separation kernel, Applications

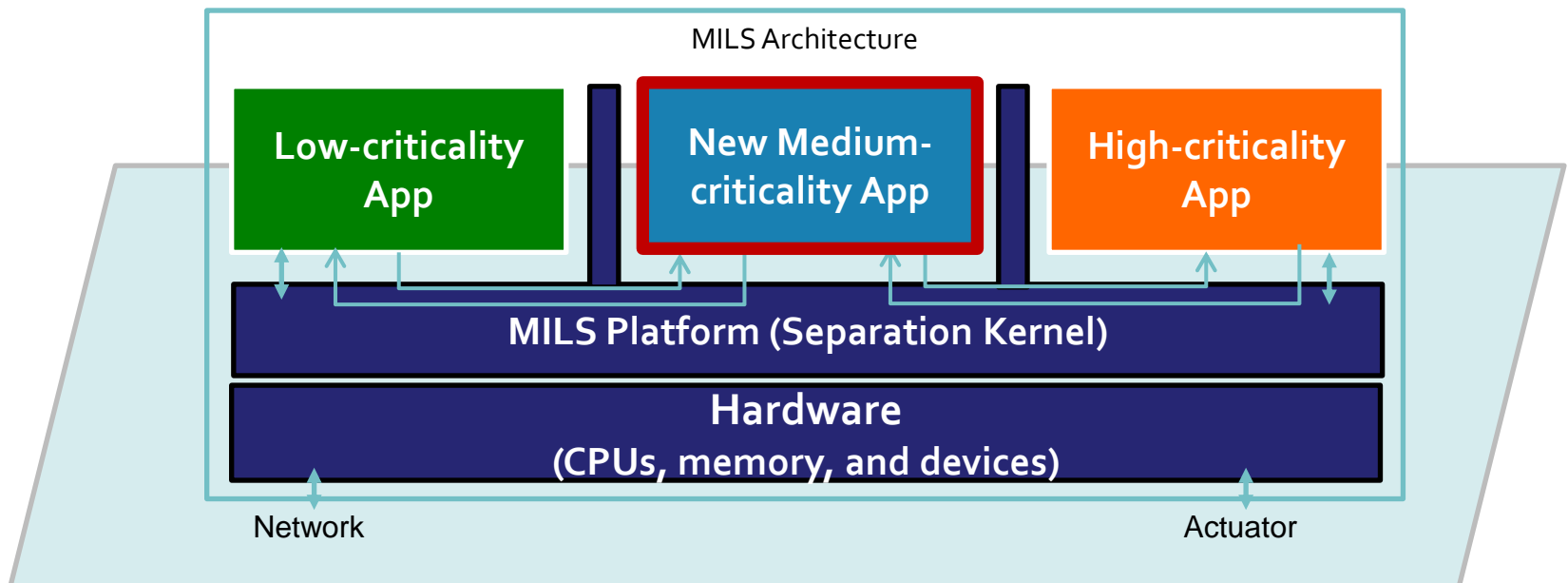
T-composition



Compositional Certification: Puzzle

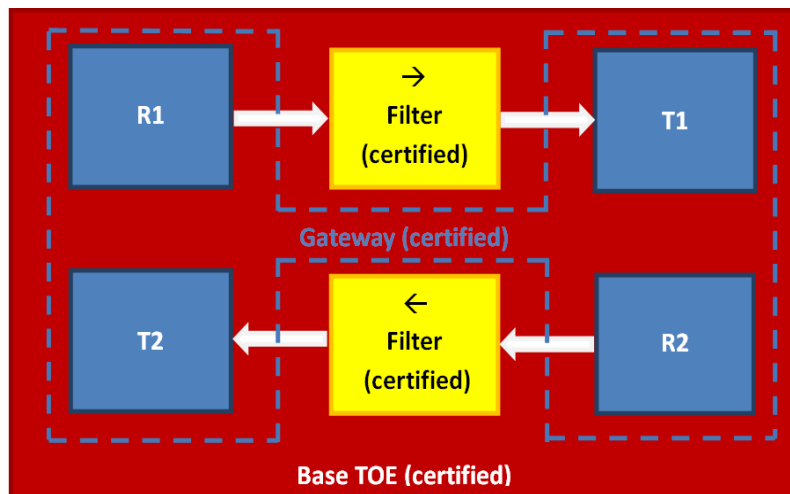
➤ Puzzle Composition

- 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



Non-Interfering Composed Evaluation

- Common Criteria does not offer a highly flexible methodology for composed evaluation regarding:
 - » Reusability of single components
 - » Independent evaluation of components
 - » Compositional assurance of products from different vendors
- New methodology solves issues and transfers efforts for vulnerability assessment to component evaluations
 - avoid duplication of effort during the compositional step when performing re-evaluations
 - however initial certification efforts likely similar to CCDB composite methodology
- Evaluation effort for Non-Interfering Composed TOE can significantly be reduced due to the non-interfering property/evidence of Component TOEs
- So far only theoretically evolved; practical application remains as future work



Non-Interfering Composed Evaluation – Benefits & Results

Objective: certifications of high-assurance systems demanding updates during the life-cycle

- Conformance claim to each **EAL** package is possible
- Enables a verdict for the Composed TOE resistance to attacks by an attacker with even **high** attack potential



Component TOE can be replaced with less effort

Non-Interfering Composed Evaluation
AVAILABLE ON
<http://euromils.eu>

The new evaluation methodology for non-interfering Composed TOE enables a **higher business flexibility** for the vendors and operators of Composed TOEs

- Methodology is disseminated on multiple events:
 - White paper on “*Non-interference Composed Evaluation*”
 - ICCC 2015, MILS Workshop 2016

➤ CEM for MILS

- Suggest CEM extension for high-assurance security assurance level
- Proposed interpretations for ADV_FSP.6, ADV_TDS.6, ATE_COV.3, AVA_VAN.5, ADV_SPM.1

➤ Attack Potential



“Addendum to CEM”
AVAILABLE ON
<http://euromils.eu>

➤ Attack Methods

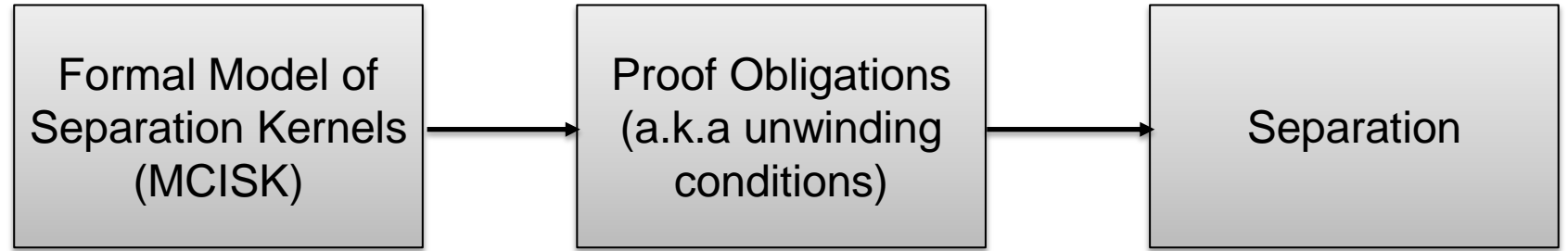
- Describe typical attacks on MILS system, MILS components, MILS platform
- Applied JIL SOGIS approach used in SmartCard

High-Assurance

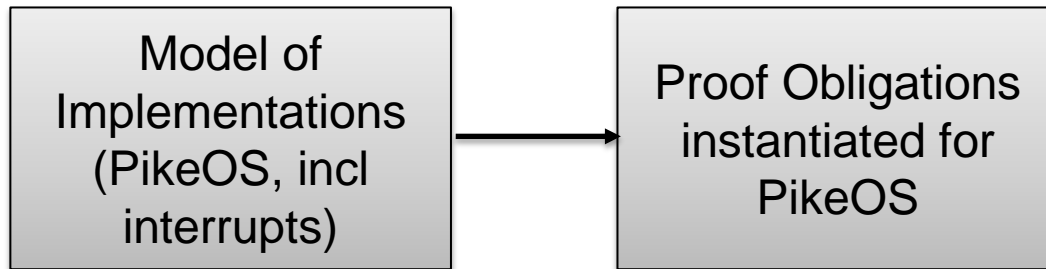
FORMAL METHODS

Formal Modelling: Separation Kernel

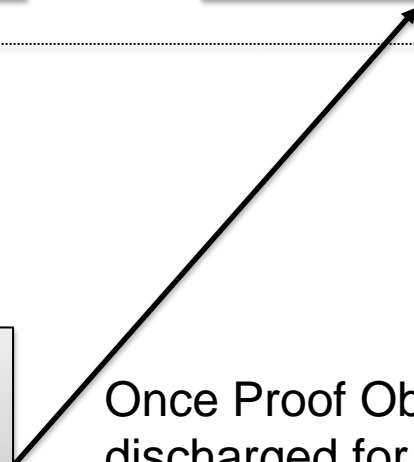
Complex generic model - prove *once and for all* that Proof Obligations imply separation



Formal Model induces modelling methodology



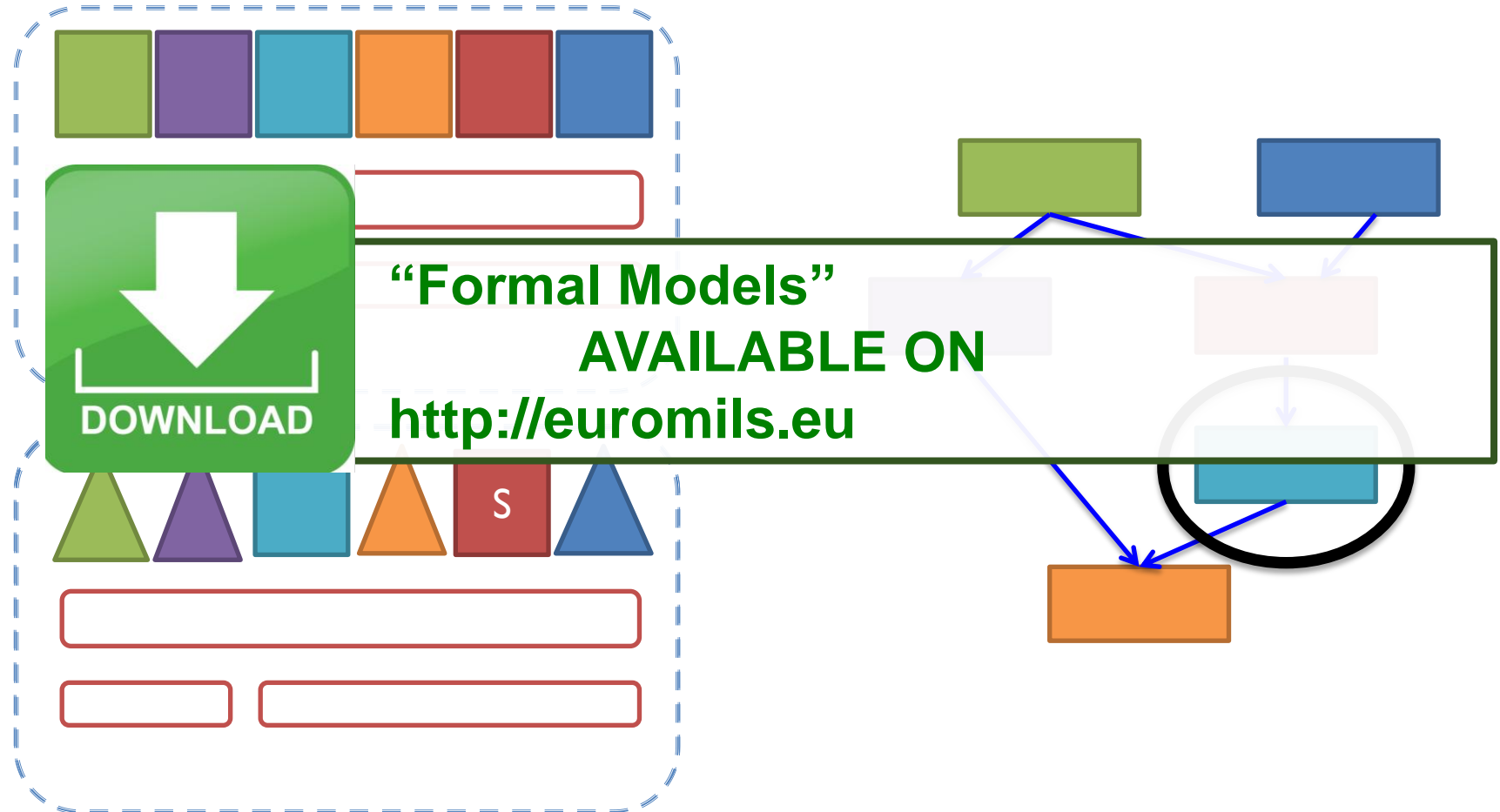
Once Proof Obligations discharged for PikeOS, Intransitive Noninterference immediately follows



Specification: Non-Interference

System Components

Security Policy



- Usage of Isabelle/HOL in CC Security certification Process
 - Using Isabelle/HOL in Certification Processes: A System Description and Mandatory Recommendations
 - Style Guide
- Target both evaluators and developers



of the recommendations and style guides on the models

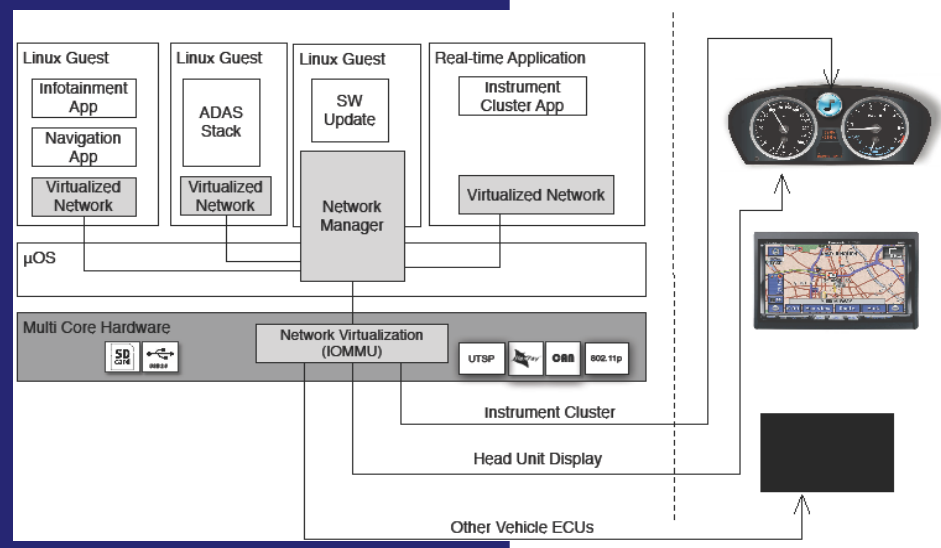
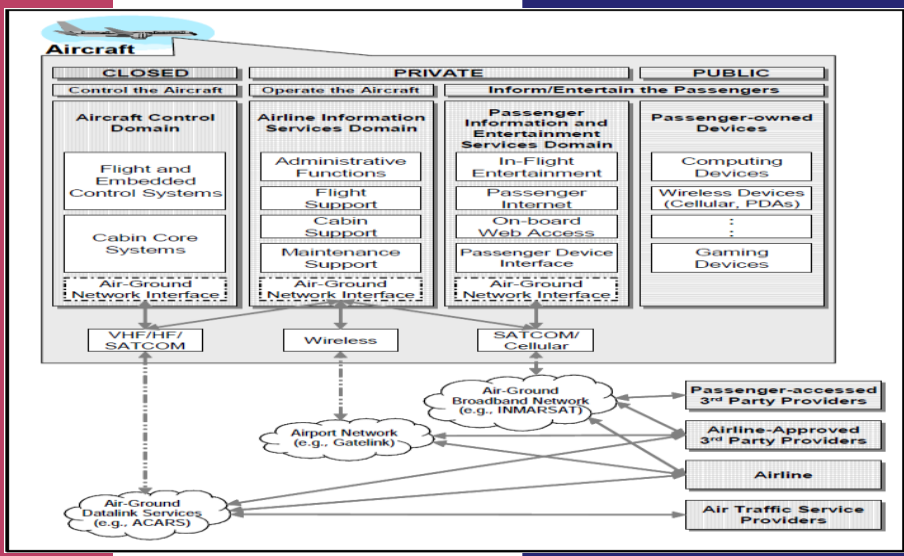
**“Used Formal Methods”
AVAILABLE ON
<http://euromils.eu>**

- of real test-sequences from formal models
- Testgen tool for Isabelle/HOL
- Method and tools available online

DEMONSTRATORS

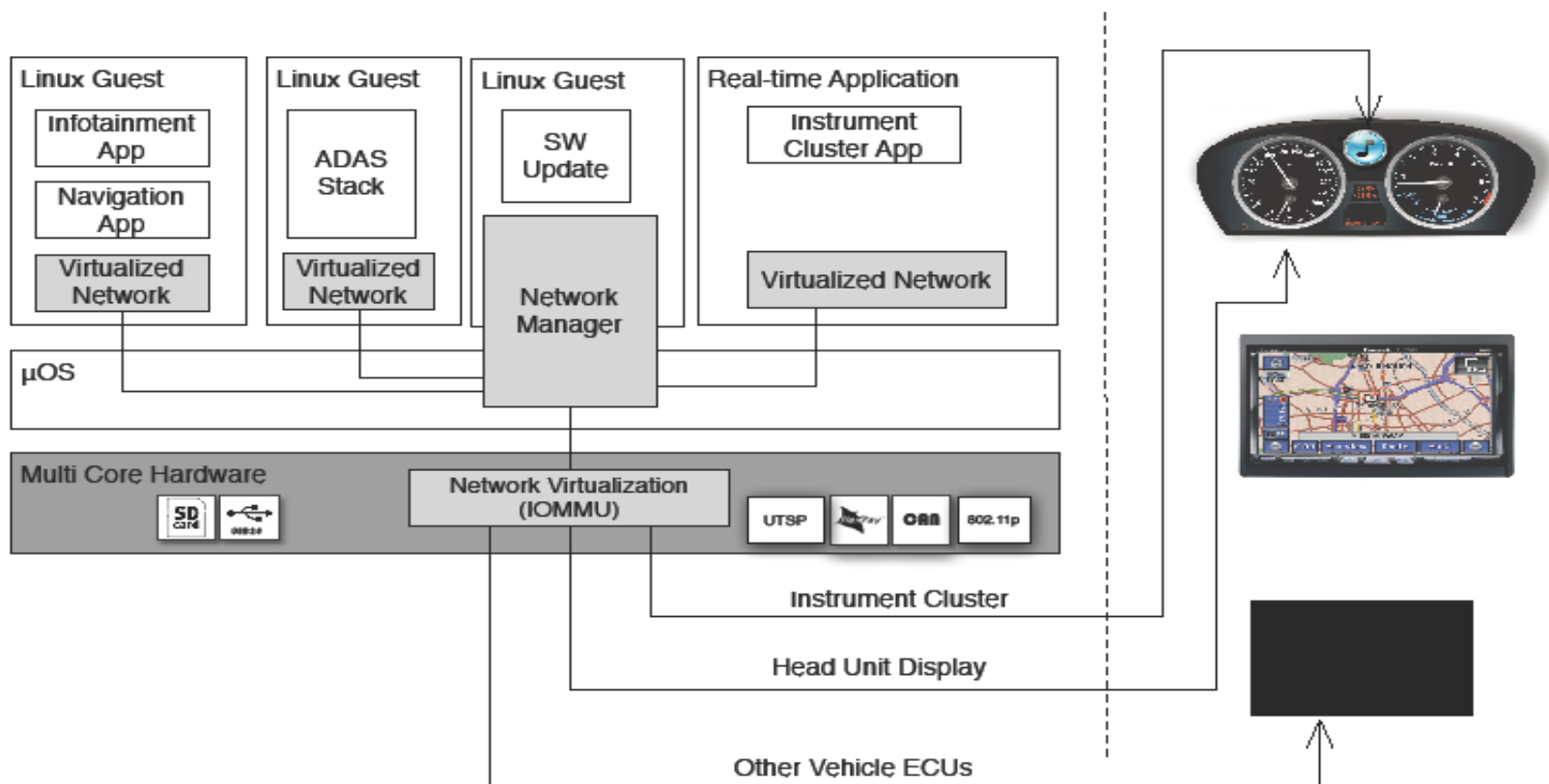
Avionics

Automotive



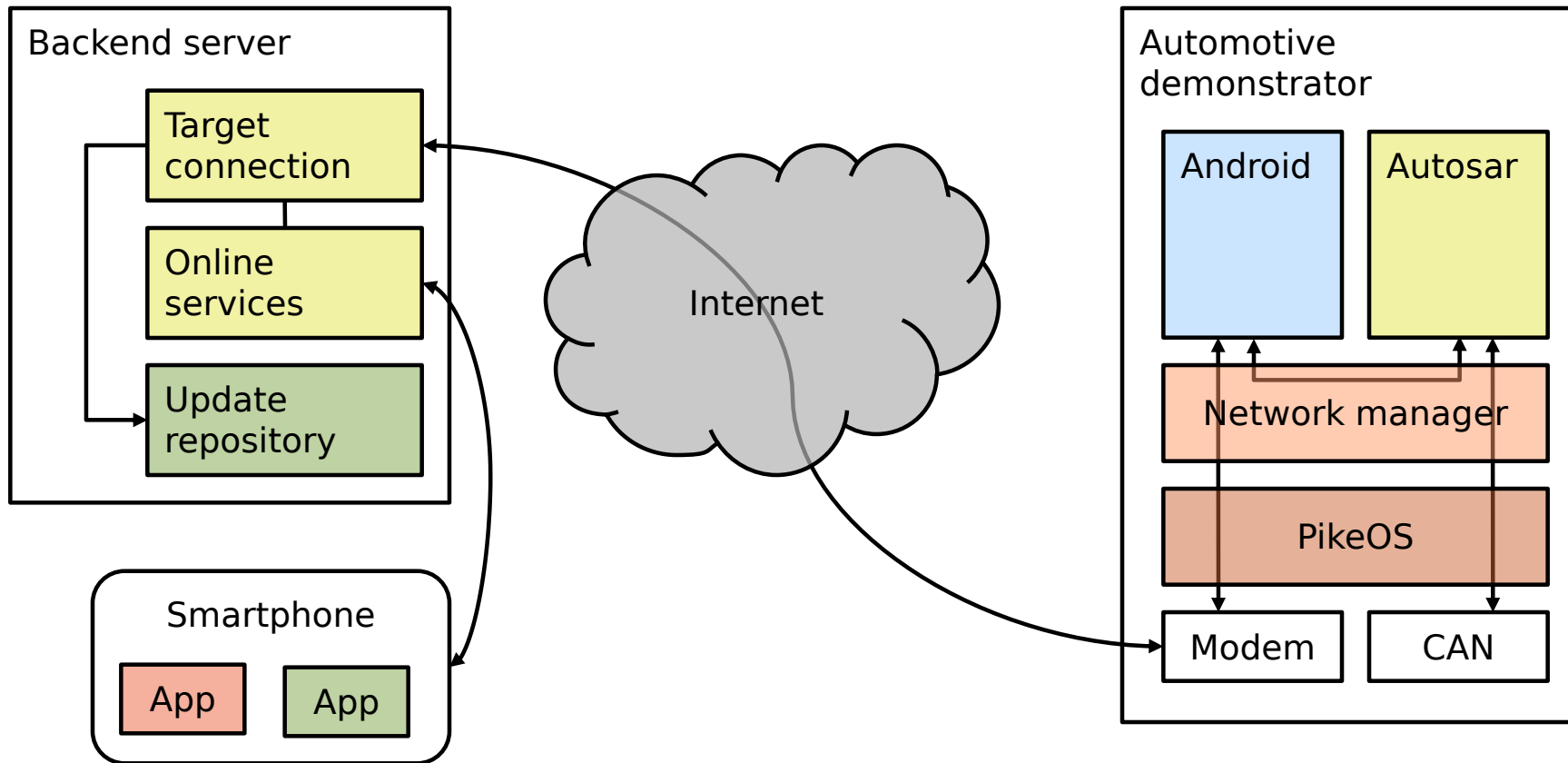
Trustworthy ICT
for networked
high-criticality systems

Example: Automotive Security Domains

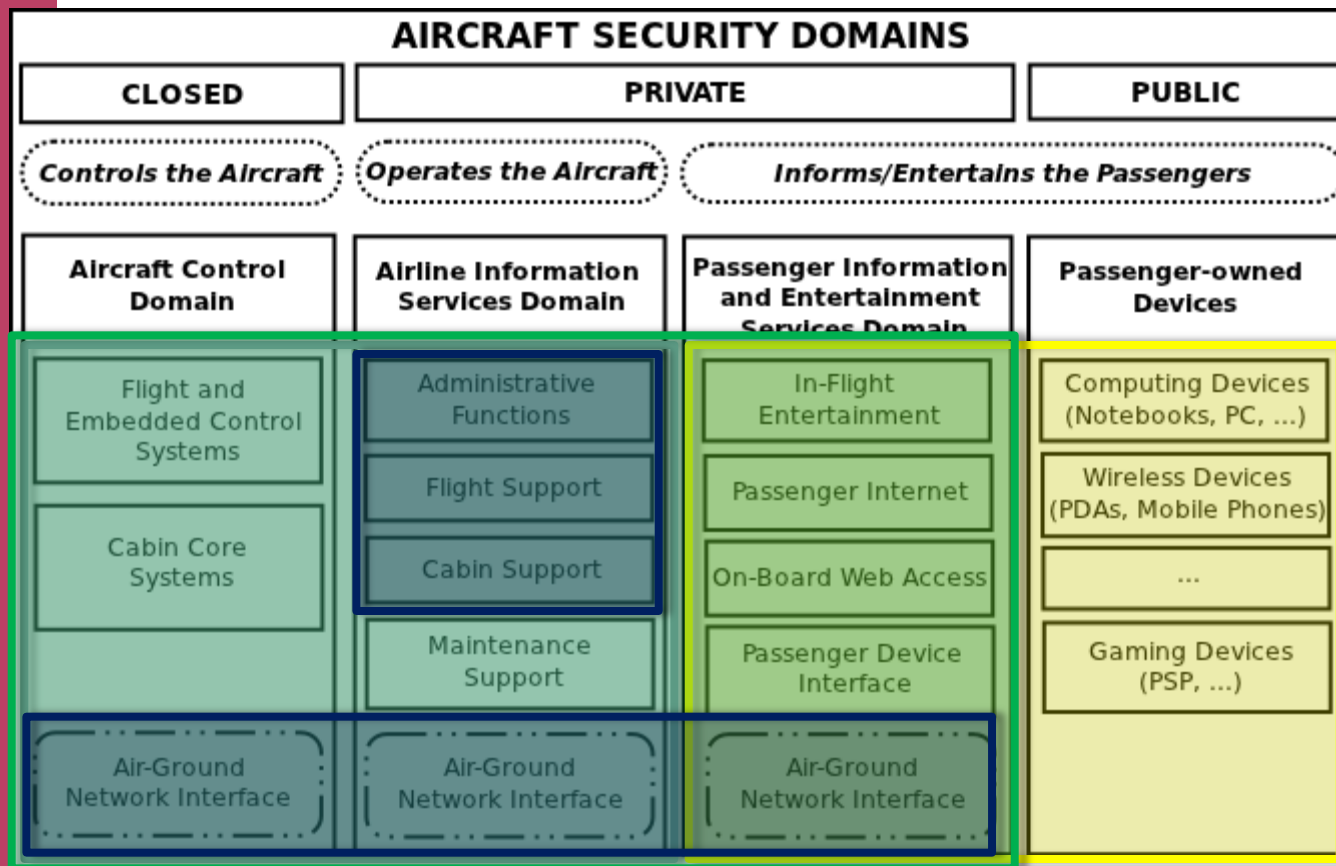


- Target of automotive security measures is the protection of instrument cluster and head unit display control, as well as the underlying virtualisation platform. Under no circumstances, these units may be compromised or disturbed in their normal operation.





Automotive Telematics Environment



Example: Aircraft Security Domains



Perspective "User"
(not 100% accurate)

-  Crew
-  Passenger
-  Maintenance (all types)
-  Others (Air Traffic Control, Airline Services, Ground)

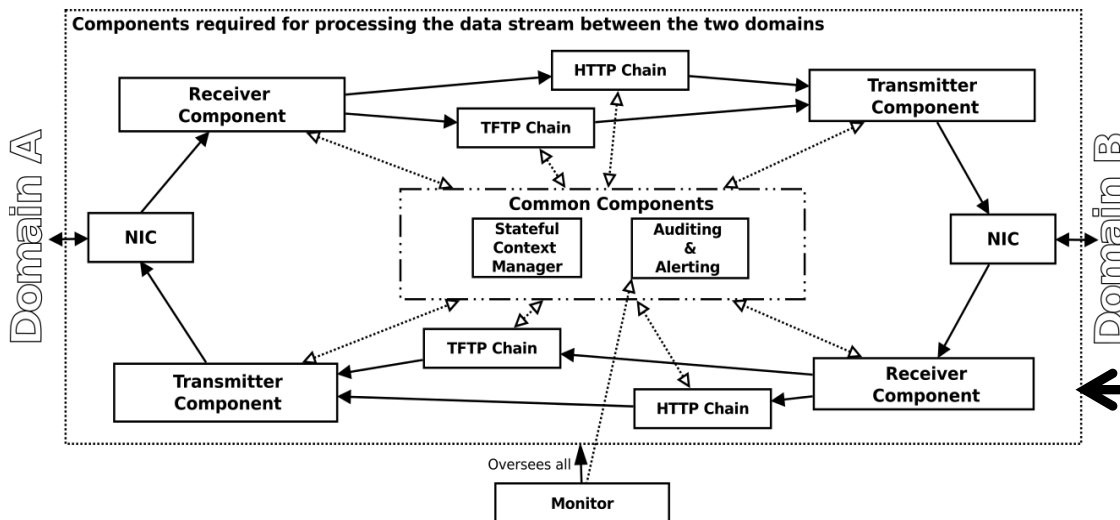
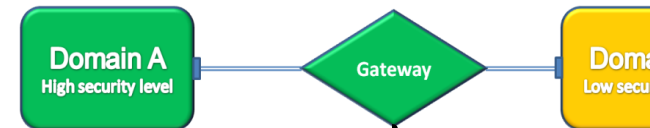
- Picture adapted from ARINC 811.
- Domains are defined In ARINC 664 Part 5.

Avionic Demonstrator: Gateway

Gateway uses this principal as system architecture to implement network filtering between Security Domains (ARINC 664/811) up to application layer

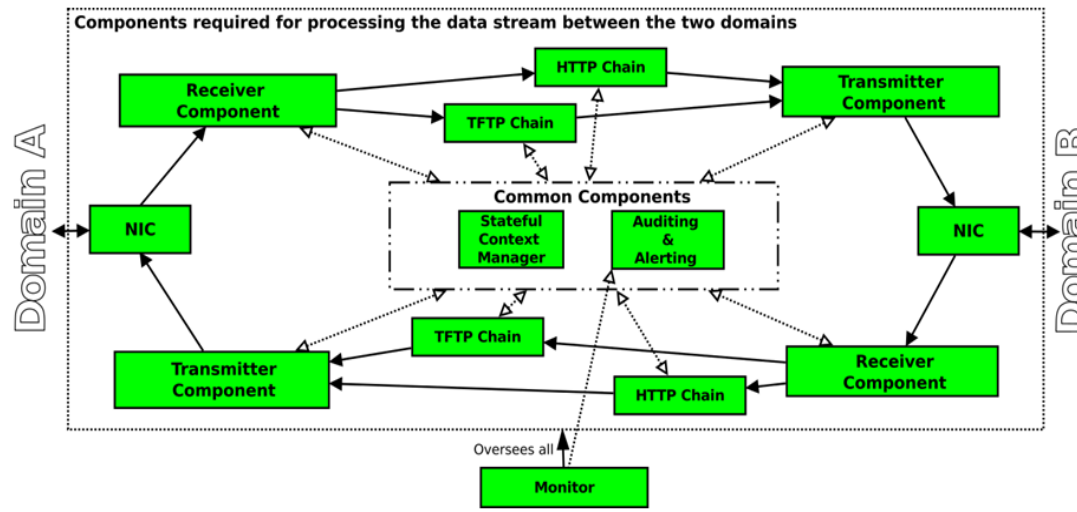
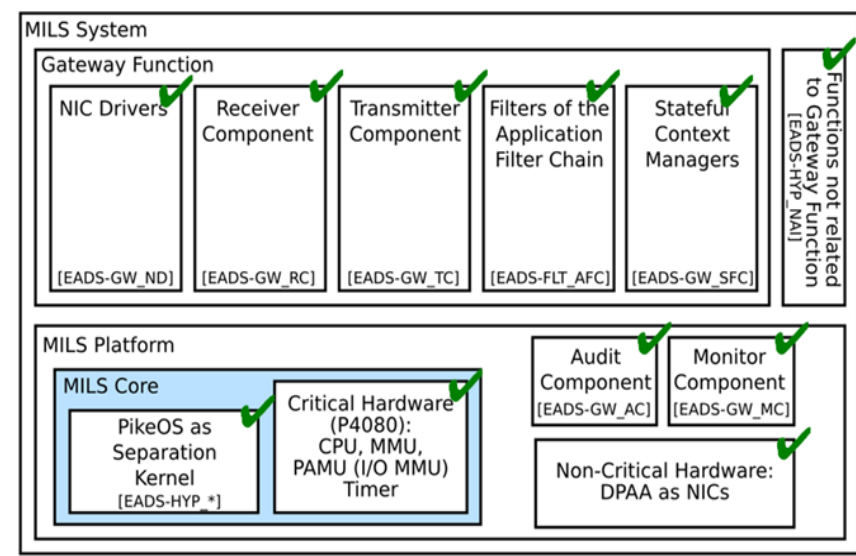


- Highly adaptable and extendable software design
- Reusability of components (e.g. Health Monitors, Audit, ...)
- Limitation of attack impact propagation
- Filter Chain Technology
- Small Gateway Components ease verification/certification (Common Criteria, Compositional Certification Methods)



Gateway Implementation and Testbed Environment

- Based on industrial requirements
- Fully implemented filtering of TFTP and HTTP traffic
- Gateway functional and security tests using the Scapy network testing environment
- Used for development of compositional evaluation methodology as use-case



as a summary

MILS COMMUNITY

- Involve all stakeholders interested in MILS topics
- First meeting **tomorrow**
 - When: 20.01.2016, 13:00 – 16:00
 - Where: Klub Lavka,
Novotného lávka 201/1,
110 00 Praha

EURO-MILS CONTRACT NO: 318353

"The EURO-MILS project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-318353."

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@euromils.eu

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.