MILS-Related Information Flow Control in the Avionic Domain

A View on Security-Enhancing Software Architectures

Kevin Mueller*, ***Michael Paulitsch****, Sergey Tverdyschev**, Holger Blasum**

* EADS Innovation Works
** SYSGO

25 June 2012

Sponsored by German Ministry of Research and Education

Aircraft Architectures Are Changing

YESTERDAY

Non-integrated aircraft

- Systems are simple, obscure, proprietary and isolated – clear ATA responsibilities
- easy integration, low complexity

TODAY

Integrated aircraft

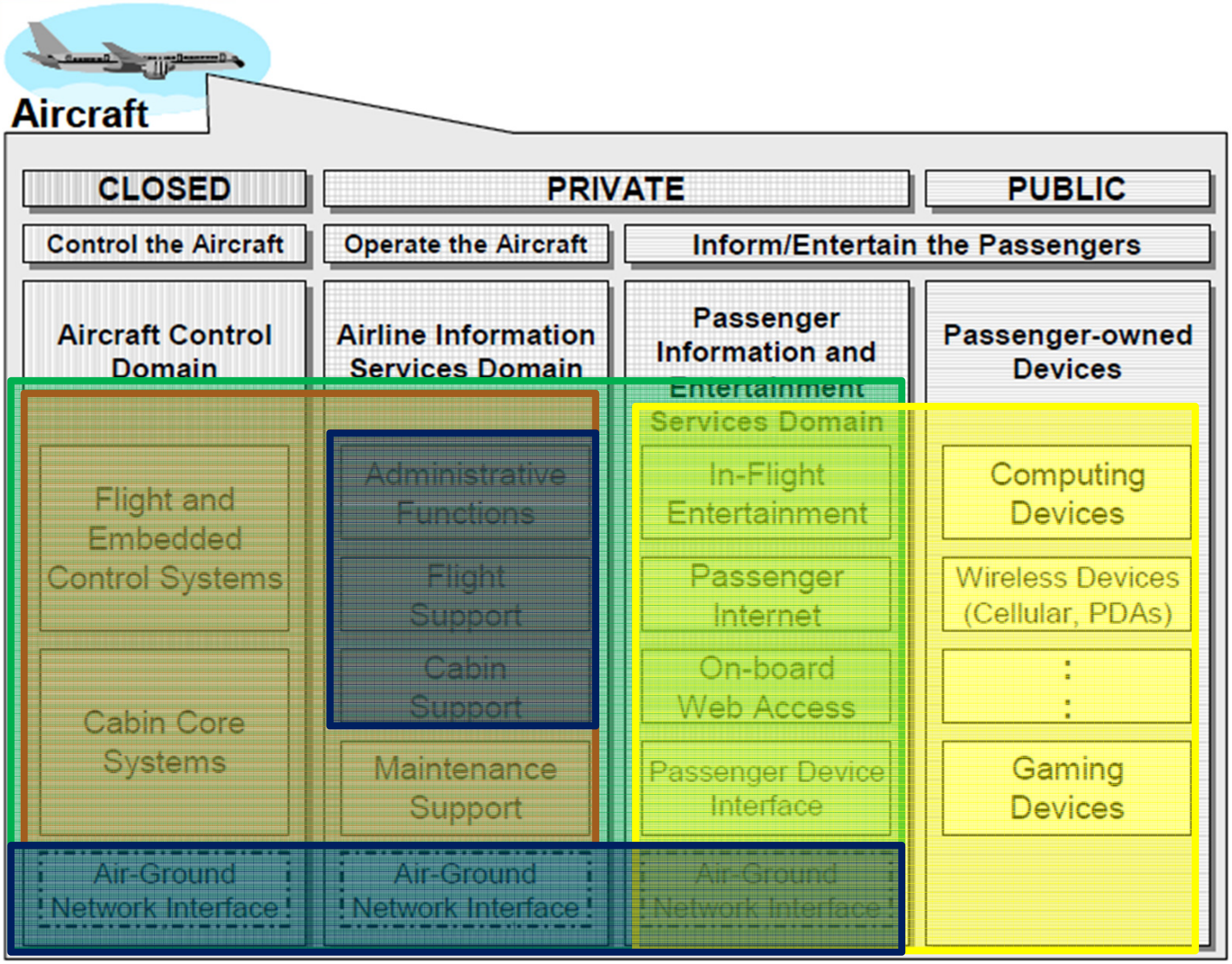
- Systems share platforms (Blade Server, A653)
- Communication networks (Ethernet, AFDX)
- More complexity, more integration efforts

TOMORROW

eEnabled aircraft

- More and more COTS will be used
- Merging of ground and aircraft systems
- High integration complexity
- ATA-isolated responsibilities will decrease

On-Board Security Domains



CLOSED	PRIVATE		PUBLIC
Control the Aircraft	Operate the Aircraft	Inform/Entertain the Passengers	
Aircraft Control Domain	Airline Information Services Domain	Passenger Information and Entertainment Services Domain	Passenger-owned Devices
Flight and Embedded Control Systems	Administrative Functions	In-Flight Entertainment	Computing Devices
	Flight Support	Passenger Internet	Wireless Devices (Cellular, PDAs)
Cabin Core Systems	Cabin Support	On-board Web Access	: :
	Maintenance Support	Passenger Device Interface	Gaming Devices
Air-Ground Network Interface	Air-Ground Network Interface	Air-Ground Network Interface	

Perspective “User”
(not 100% accurate)

🟫 Crew

🟨 Passenger

🟩 Maintenance (all types)

🟦 Others (Air Traffic Contr Airline Services, Ground)

© ARINC811

How Can You Design a Secure Architecture ...

… that fulfills stringent secure requirements

… that is adaptable for deployment of 20+ years of service

… that should not weigh “much”

… that builds on 20 years legacy (safety aspect does likely allow abrupt change)

… in a conservative incident-driven safety culture

→ **One needs strong base upon which to build upon.**

- MILS architecture could be one approach building the basis → the foundation
- “Software on top”, white-based filtering rules for information flow, and security policies address changing requirements

So what is MILS?

MILS – Multiple Independent Levels of Security

- Architecture for a (software) system processing data of different security domains concurrently
  - Combines trusted and non-trusted apps within the same system
- In layman's terms: MILS is the best name for IMA (Integrated Modular Avionics) when concerned about security
- High-assurance security architecture based on the concepts of **separation and controlled information flow**
  - Separation builds 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
- Two level platform design approach: System policy level and enforcement level
- Small analyzable components; composability targeted
- Certifiable MILS system is built out of key components (separation kernel, trusted hardware, guards, …)
  - Have to be **N**on-bypassable, **E**valuatable, **A**lways invoked, and **T**amperproof (NEAT).
- Components should be single level security systems (SLS)
- Multi-level security (MLS) components are hardly avoidable, but should be used with care (limited number, convincing in view of system-level architecture)

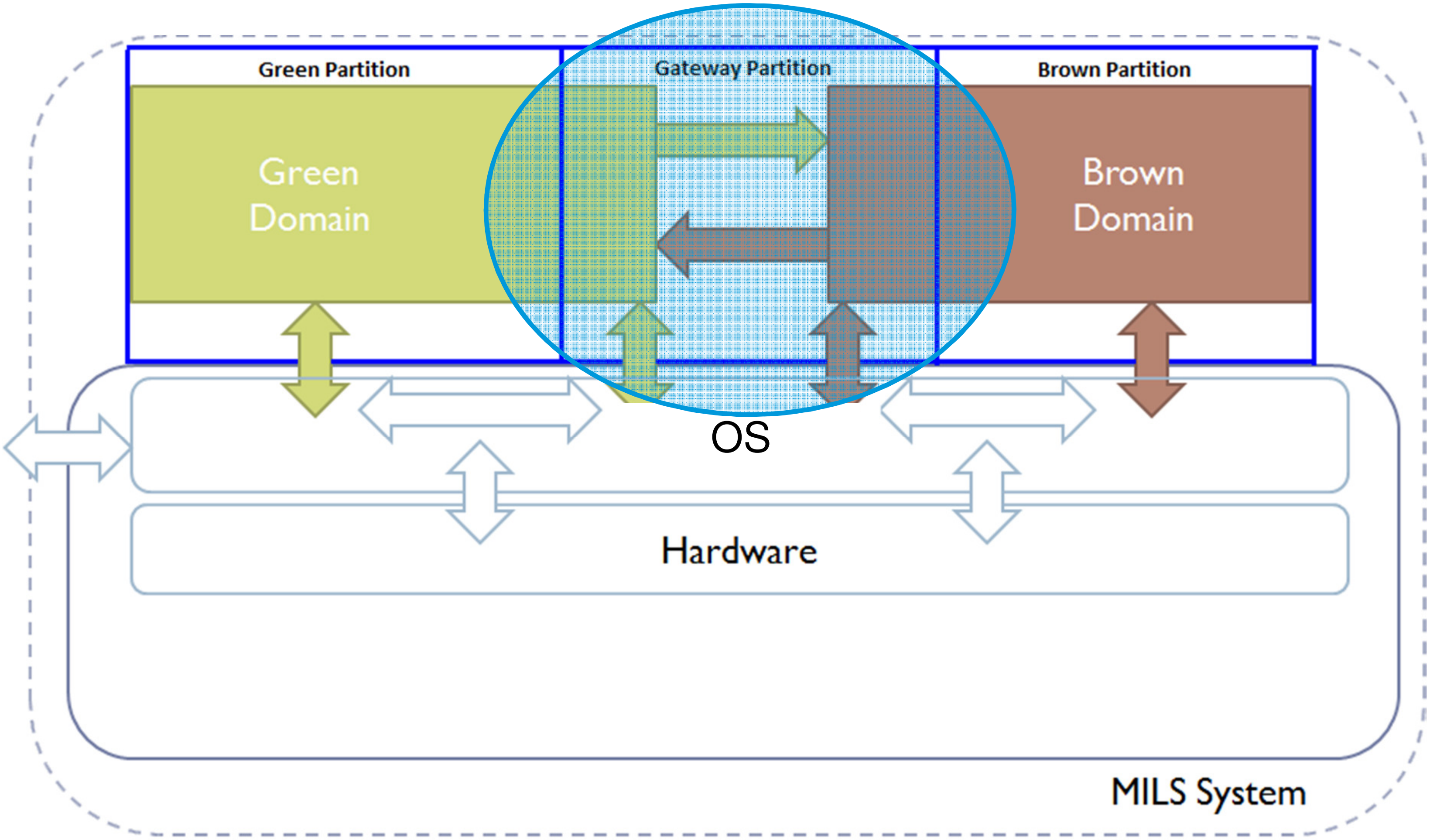
MILS and Avionics

MILS architecture implementations (can be) close to existing IMA (Integrated Modular Avionics) solutions (especially with respect to separation)

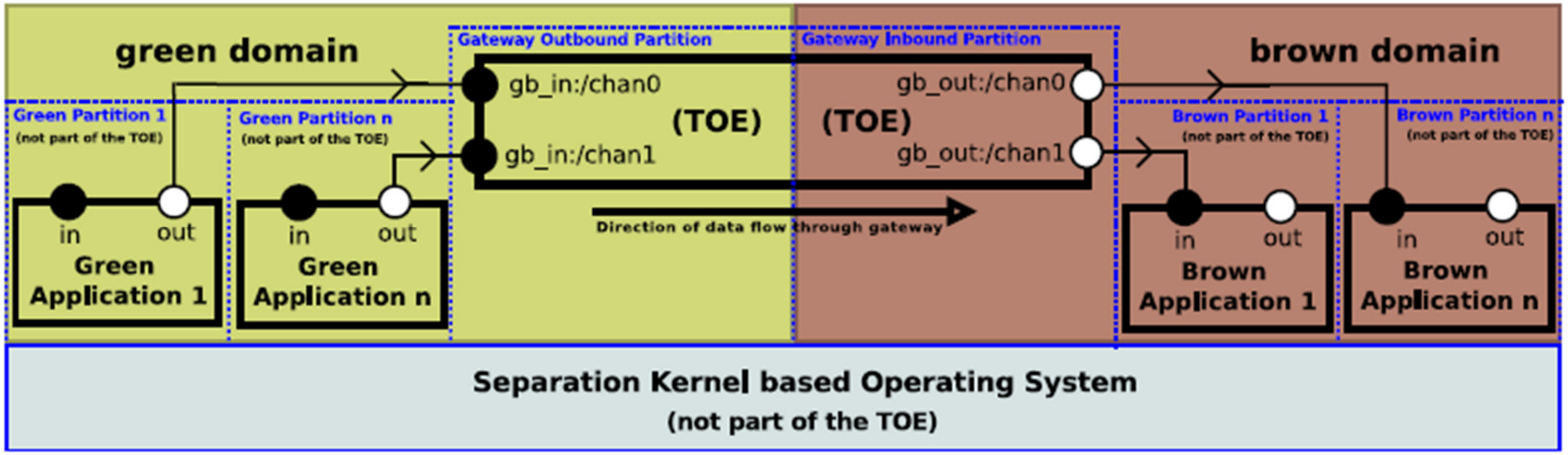
Information flow to be assessed for given design blocks (design under constraints addressing legacy; ARINC 653)

Substantial part of required security policies does not have to be information technology based (e.g. aircraft zone access strictly enforced due to safety concerns)

MILS System Architecture for Controlled Information Flow

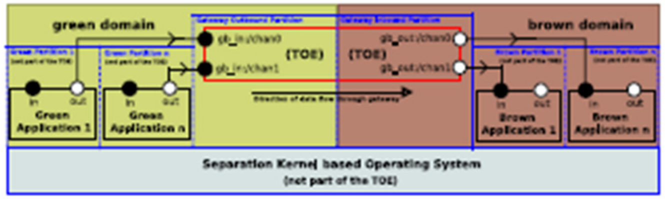


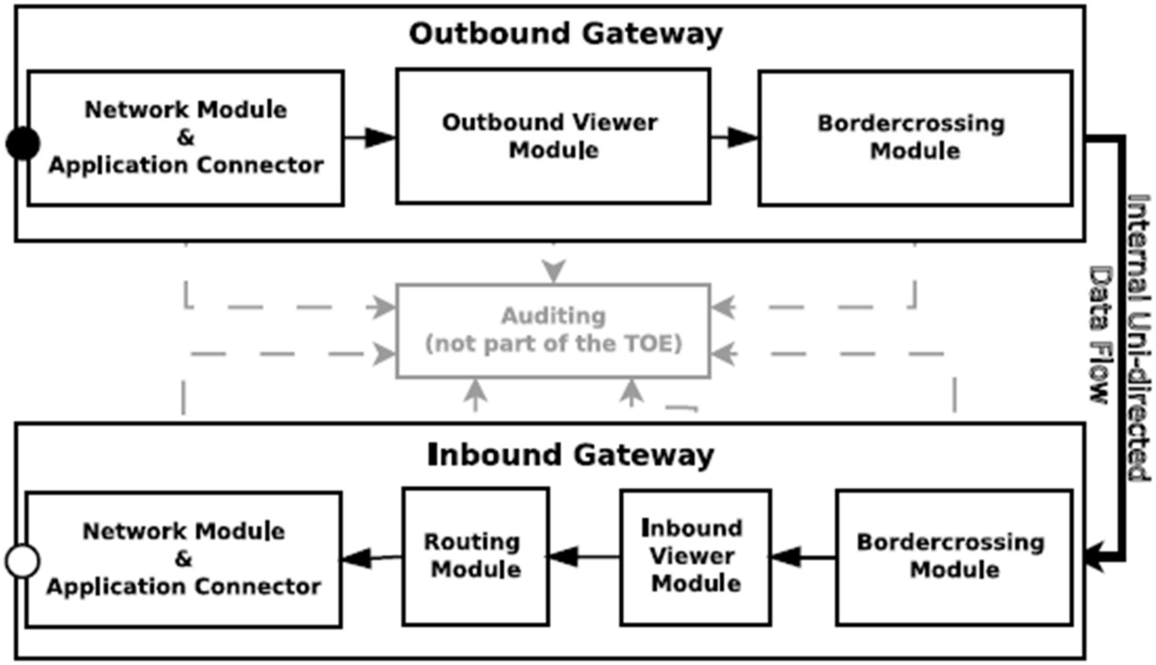
Gateway – Architecture: Network View



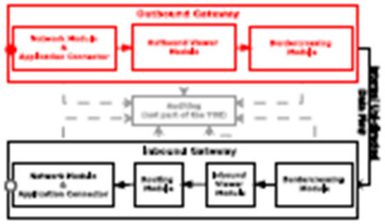
- Depicted version shows unidirectional data flow between domains
- Bidirectional flow can be achieved leveraging two contra-directed gateway instances

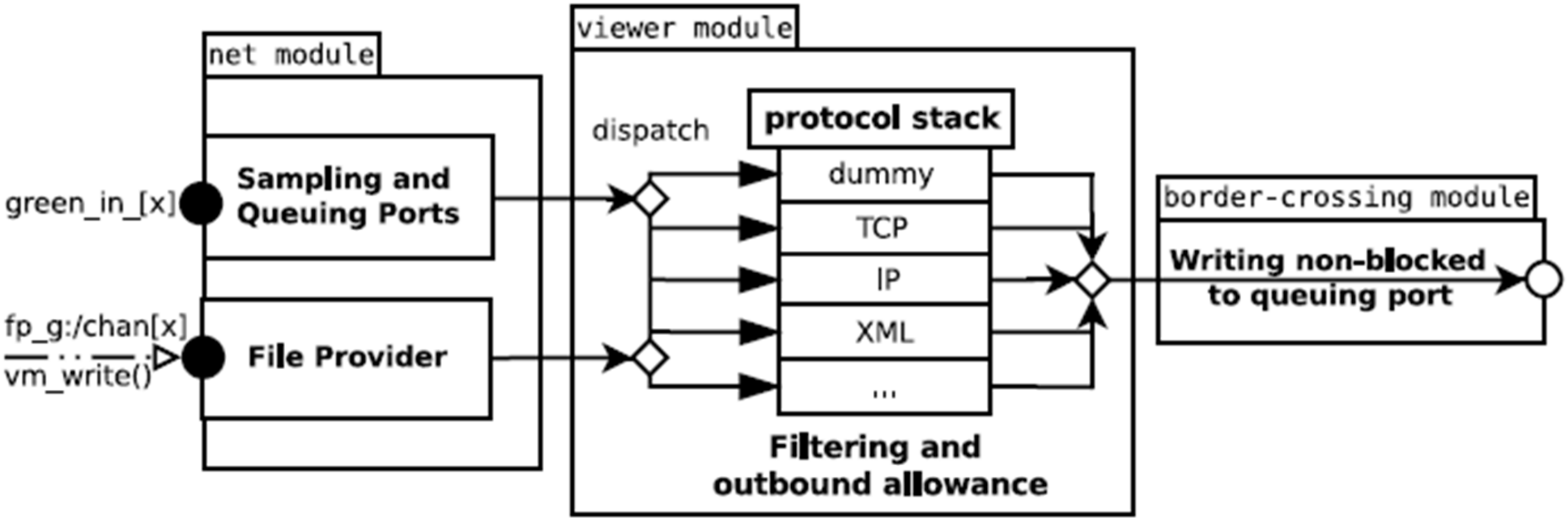
Gateway – Architecture: Component View





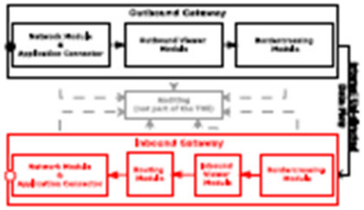
Gateway – Architecture: Data Flow

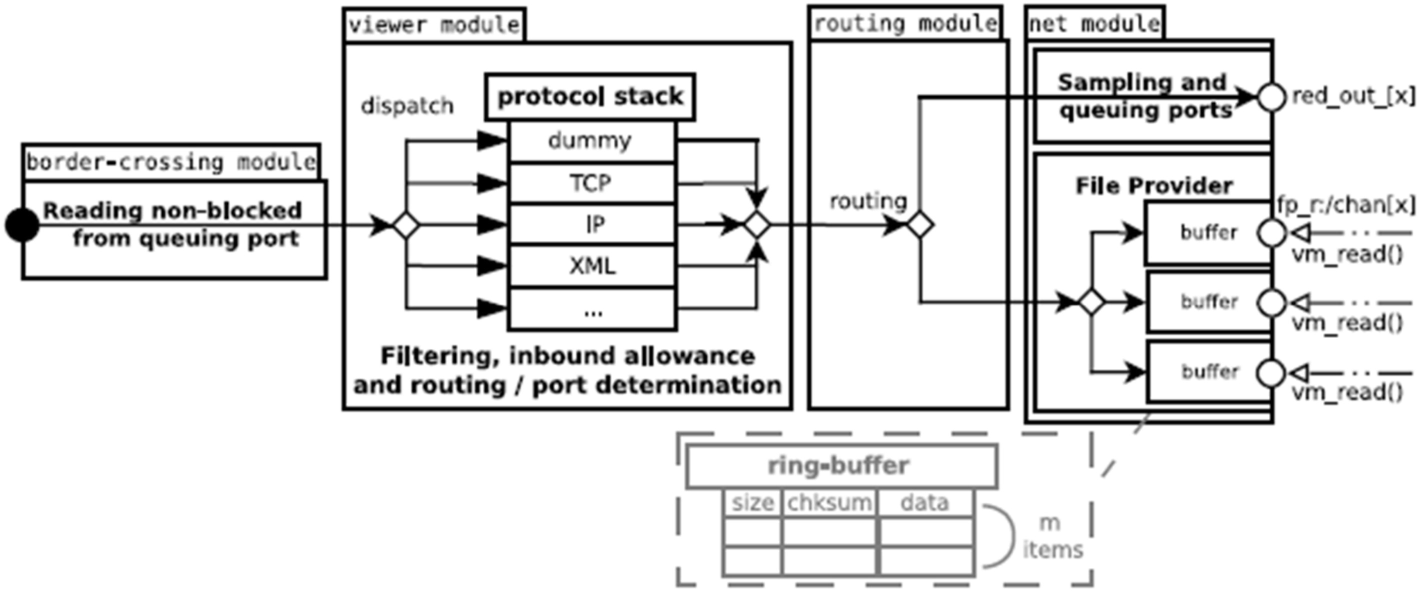




SYSGO EMBEDDING INNOVATIONS EADS

Gateway – Architecture: Data Flow





Summary, Conclusions, and Outlook

Presented context for future security architectures in aircraft

- Strong foundation need in certification context.

Presented some details on the essential security component → gateway approach for data flow management; have multiple implementation variants of the gateway running

Separation property of OS and hardware essential and to be addressed in future work

We believe a strong architectural basis is required for “open” /adaptable resilient CPS

Discussion points for workshop:

- What architectural foundation is required and essential for open adaptable secure architectures?
- Is the architectural approach a necessary restriction for evolution or possible limitation in adaptability for future modules (filter rules, software approach, policies, …)
- Where does integration of architectural blocks come into play (compositional certification)?
- How does design, production, and maintenance relate to each other?