



AUTOMOTIVE

INFOCOM

**TRANSPORT &
ENVIRONMENT**

AERONAUTICS

SPACE

**DEFENCE &
SECURITY**

3rd IAASS Conference

Safety-critical Software in Modern Integrated Avionics Systems

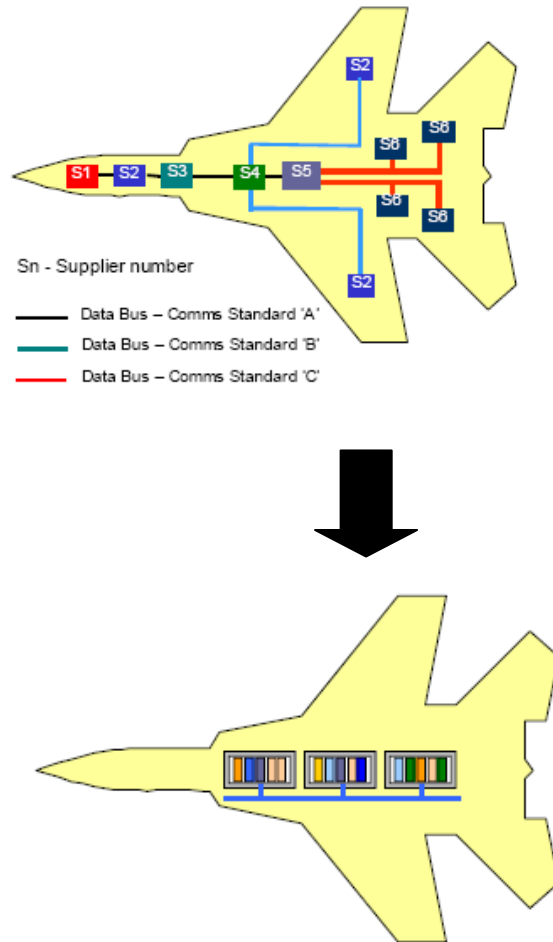
Michael Klicker

21-23 October, Rome

Overview

- Introduction IMA systems
- ASAAC
- Safety Issues
- Example: System reconfiguration
- IMA in space ?

Introduction to IMA systems

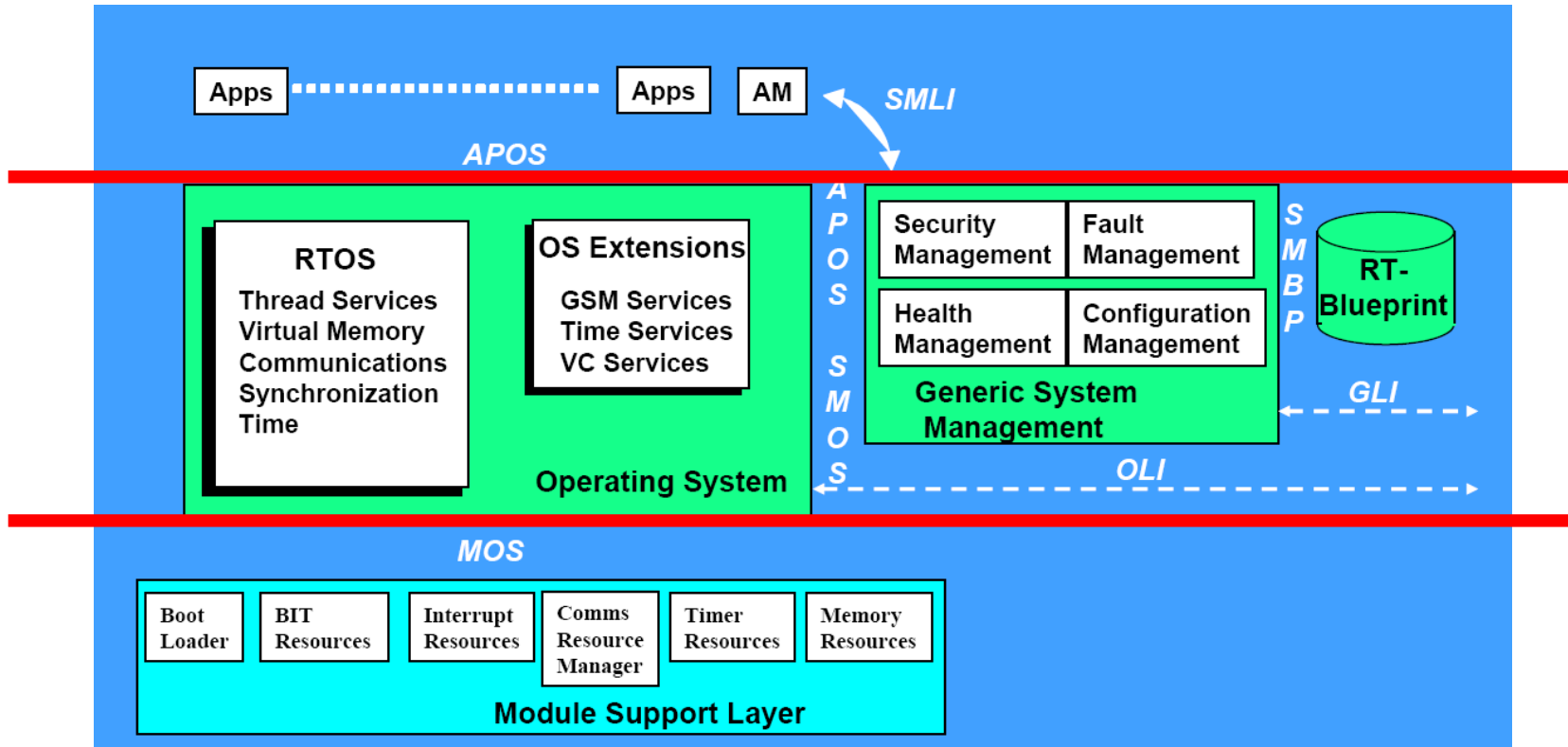


- **IMA: Integrated Modular Avionics**
 - **Modular: Small number of line-replaceable entities (general purpose computers)**
 - **Integrated by Generic System Management**
- **Reduced weight, volume, and power consumption**
- **Fault-containment units**
- **Improve technological obsolescence management**
- **Reuse through open architecture and standardized interfaces**
- **Drastically reduced parts numbers leading to less spares**
 - **simplified logistics support**
 - **simplified maintenance**
- **HW and SW resources generic and configurable**

Introduction to ASAAC (1)

- ASAAC stands for *Allied Standard Avionics Architecture Council*
- Outcome
 - Standard for Modular and Open Avionics Architectures (MOAA)
 - Technology Transparency
 - Companies and MoD's from UK, France and Germany participating
 - Final stage ended 2004
 - Status of formal standardization:
 - NATO: Ratification process as STANAG 4626 started
 - ASD/ISO: Submitted as draft standard
- Goals:
 - Interchangeability
 - Buildability
 - Modularity/configurability
 - Reusability
 - Growth Capability
 - Maintainability / Obsolescence Management
 - Fault Tolerance

Introduction to ASAAC (2)



- MSL: Module Support Layer
- OSL: Operating System Layer
- AL: Application Layer
- RTOS: Real Time Operating System
- APOS: Application Program Operating System Interface
- MOS: Module Operating System Interface
- GSM: Generic System Management

Safety Aspects (1)

IMA System Safety

Temporal Separation:

- OS Scheduler
- Time slots enforced
- I/O bound to time slots

Spatial Separation:

- MMU
- Dedicated memory

System Management:

- Reconfigurability
- Fault Management
- Separation monitoring
- GSM Hierarchy

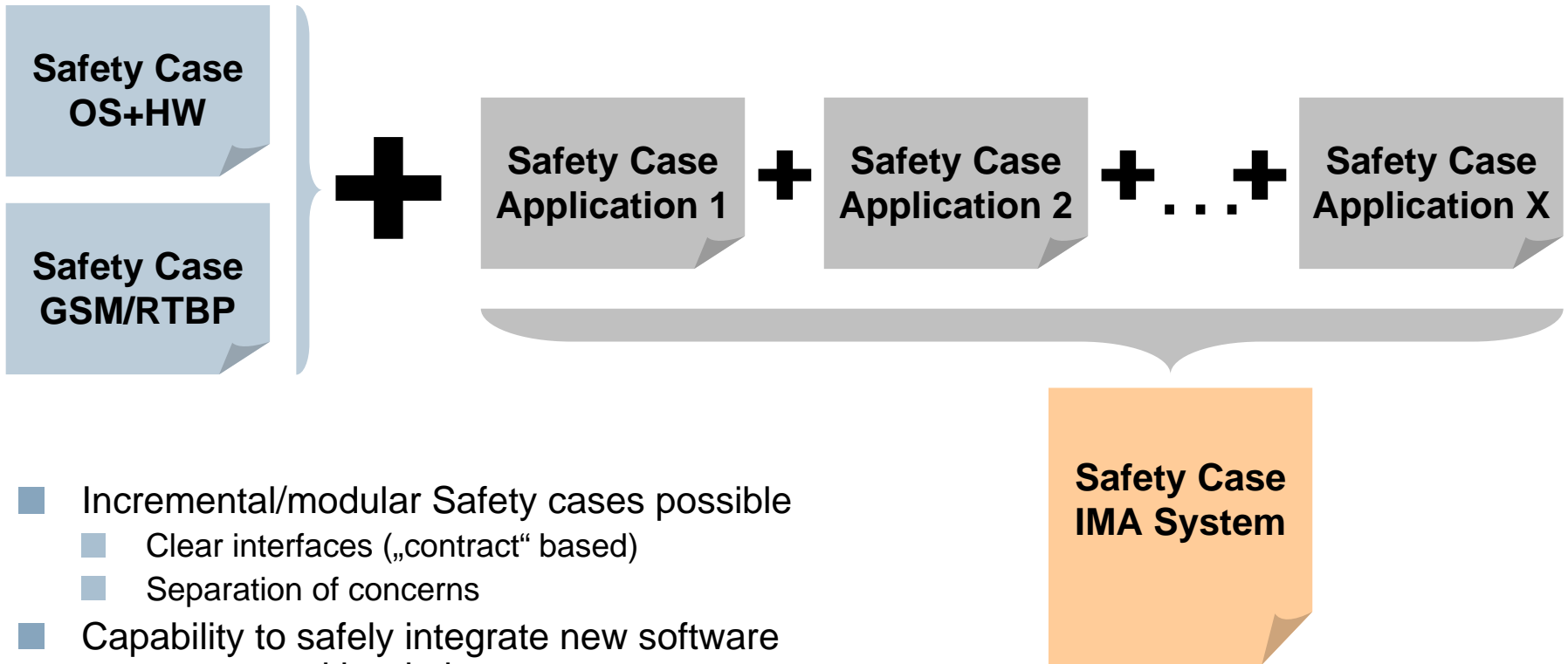
Operating System:

- Level A certifiable
- Virtualisation of I/O
- HW Abstraction

Enables:

Pieces of Application Software of different safety and/or security criticality run concurrently !

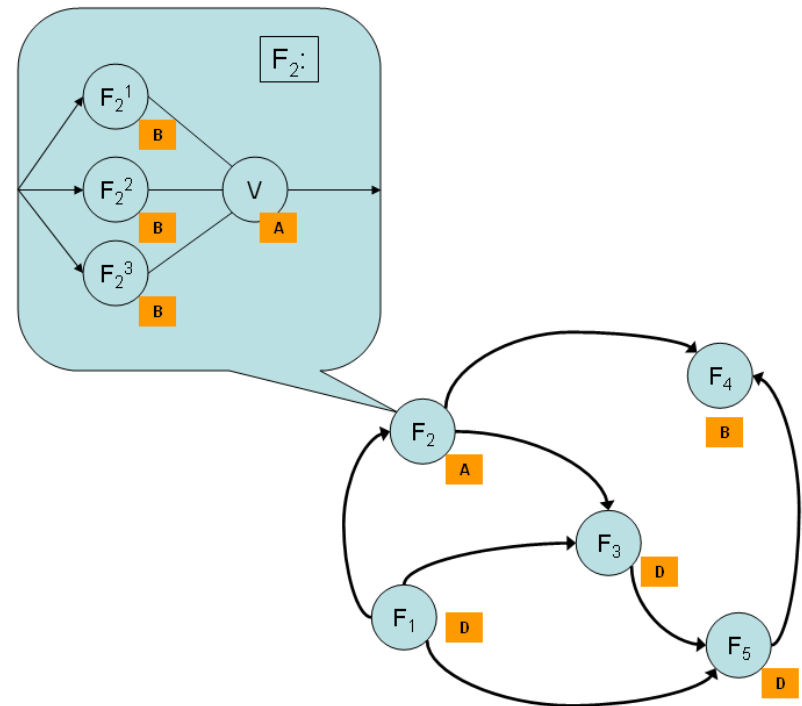
Safety Aspects (2)



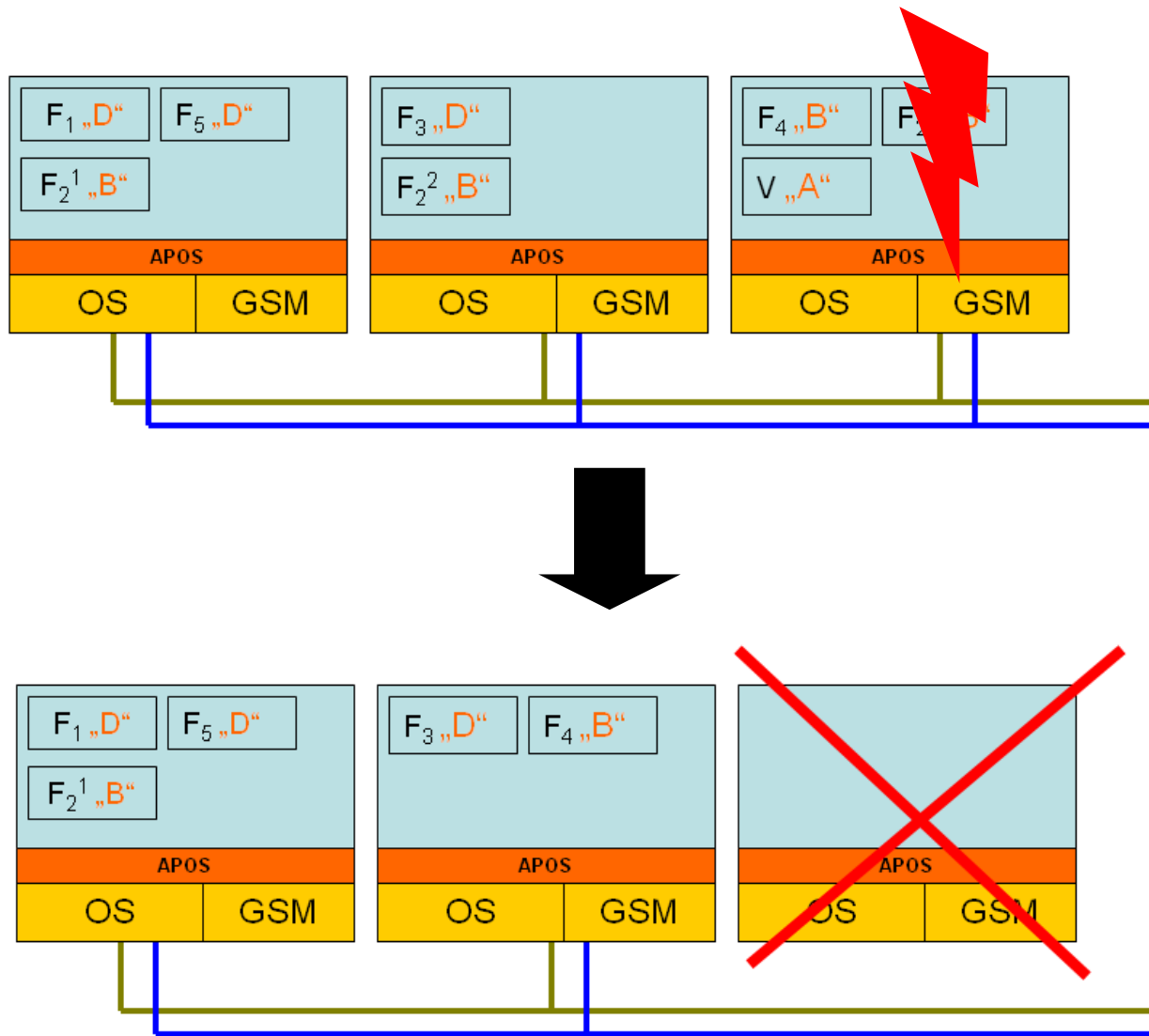
- Incremental/modular Safety cases possible
 - Clear interfaces („contract“ based)
 - Separation of concerns
- Capability to safely integrate new software components with relative ease
- But:
 - Extremely complex architecture
 - Complex interfaces
 - Verification challenging
 - Heavy frontloading of development

Example: System Reconfiguration (1)

- Suppose a system composed of 5 avionics functions, where one (F_2) is itself composed of 3 redundant subfunctions linked by a voter V.
- The arrows symbolize communication links
- This would be a (very simplified) design time blueprint
- Next Slide: Implementation of this functional „sketch“ and illustration of a possible reconfiguration



Example: System Recofiguration (2)



IMA in Space ?

- Key attributes of IMA systems relevant for space application
 - Reconfigurability in case of a hardware failure (e.g. SEU)
 - Increased commonality in different satellites/space systems
 - Weight savings
 - For human exploration:
 - Safety considerations (increased fault tolerance for example)
 - Limited number of spare parts (e.g. Moon/Mars expeditions) → Repairability!
 - For Satellites:
 - Security considerations: Multiple Independent Layers of Security (MILS) possible



© ESA

Contact

I A B G

Industrieanlagen
Betriebsgesellschaft mbH

Einsteinstr. 20
D-85521 Ottobrunn
Germany

www.iabg.de

■ Michael Klicker, VG43
klicker@iabg.de
+49-89-6088-3248