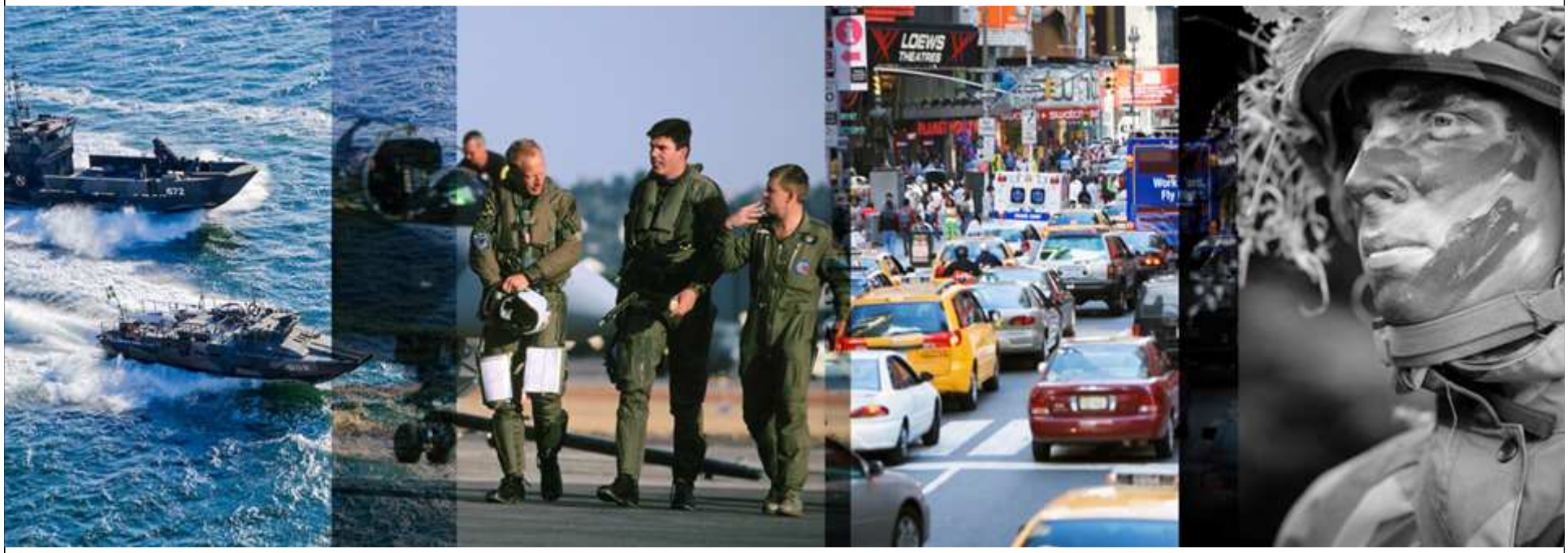
Avionic Architectures

Trends and challenges



Mats Ekman

101104

KTH, INCOSE

Saab Aeronautics

- More than 4000 aircraft manufactured
- Among them 500 airliners
- 15 different types of aircraft

Architecture paradigms

- Federated Architectures
- Swedish approach, Integrated Federated
- IMA, Integrated Modular Avionics
- DIMA, Distributed IMA

Design Process

- Requirements
- Design Constraints
- Design Flow

Federated Architectures

- Each system has its own computers performing its own functions
- Analog PtP, digital PtP, digital buses
- Few dependencies between LRUs
- Reliability and availability determined by LRUs
- New/Added system functionality often causes major system redesign, integration test and verification work
- High cost for spare parts and maintenance

Swedish approach, Integrated Federated

- Centralized Integrator computers with federated systems around
- Increased degree of computerization in Swedish military aircraft systems
  - 37 Viggen Attack, reconnaissance and trainer versions developed during the 60´s, mainly one computer
  - 37 Viggen Fighter version developed during the 70´s with approx 5 computers
  - and 39 Gripen during the 80´s and 90´s --- with approx 30 computers

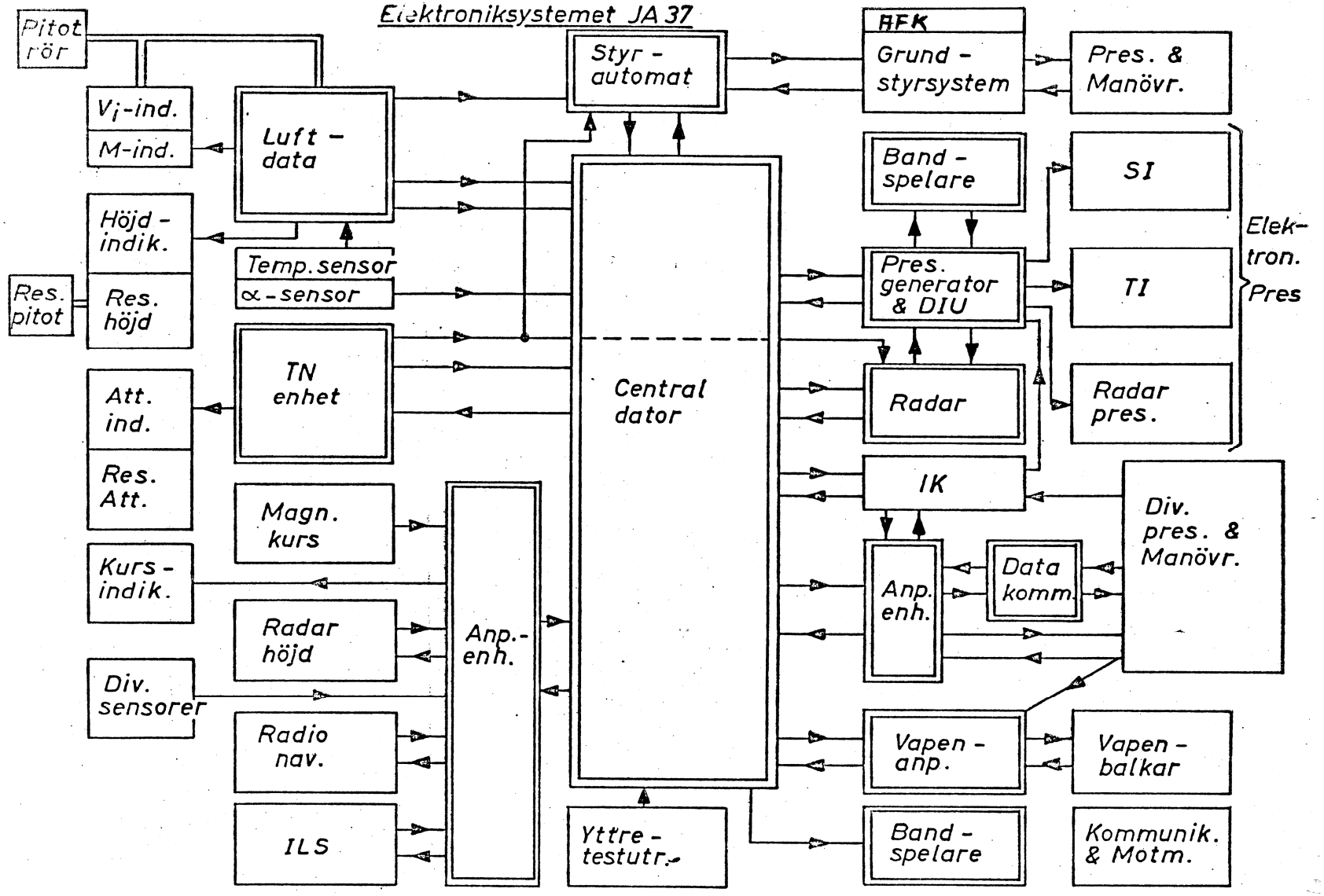
Saab 37 Viggen

Saab 37 Viggen
Sweden
Multi-role

Span:	10.6 m
Length:	16.3 m
Engine:	P&W JT8D-22
	SFA RM8A / 6700kp/
	11800 w Afterburner
Max speed:	Mach 2.0+
Max alt:	18000 m
Armament	2 x 30 mm guns, missiles
	or 16 x 120 kg bombs
Number:	287 (all versions)
In service:	1971–

RETURN

JA 37 Elektroniksystem

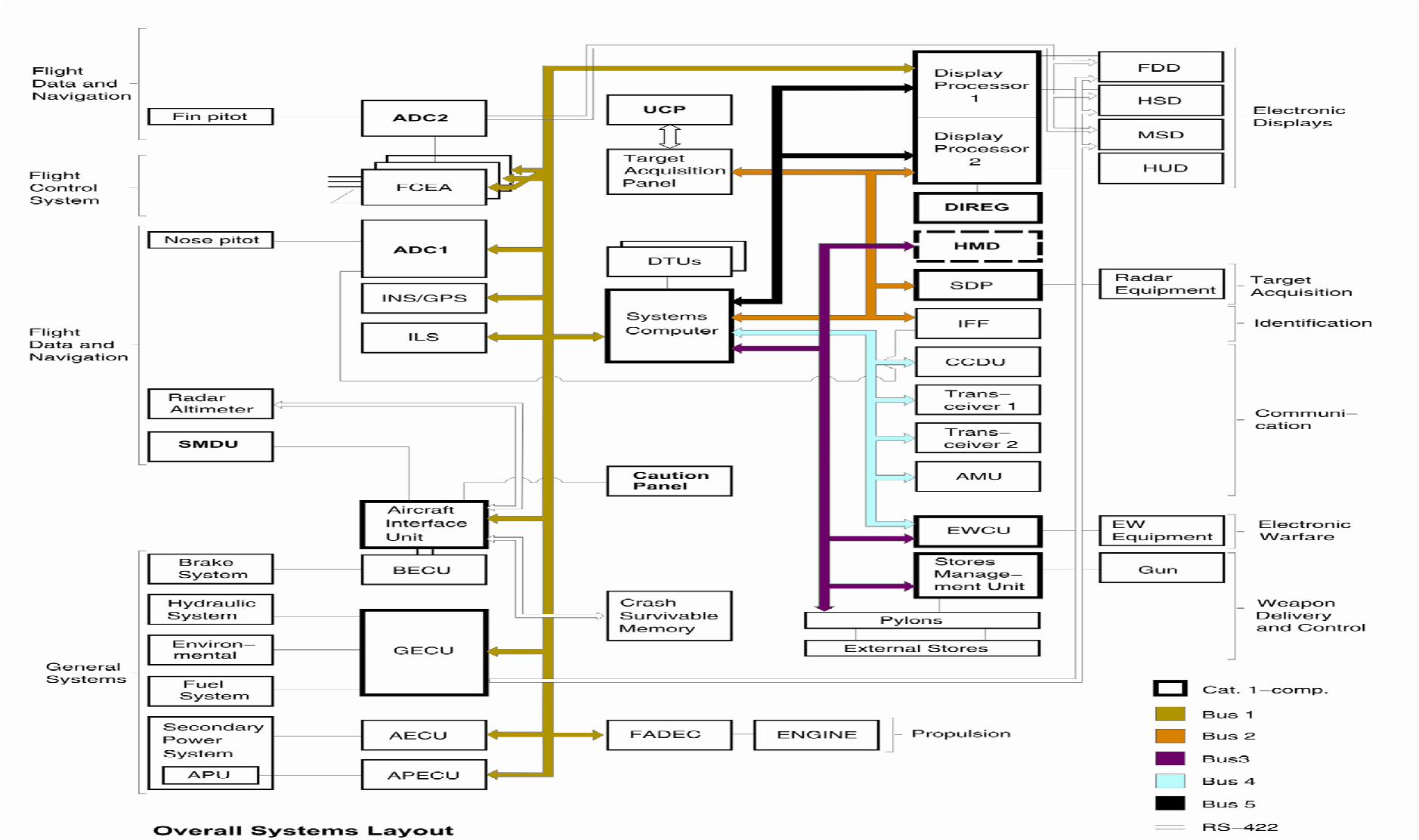


Saab 39 Gripen

Saab 39 Gripen
Sweden
Multi-role supersonic combat aircraft

Span:	8.4 m
Length:	14.1 m
Engine:	Volvo Aero Corporation RM12
Max speed:	Supersonic at all altitudes
Range:	800 km
Number:	200+
In service:	1997–

RETURN



Overall Systems Layout

ACS execution strategy

The main application function characteristics of the Aircraft Computer System are:

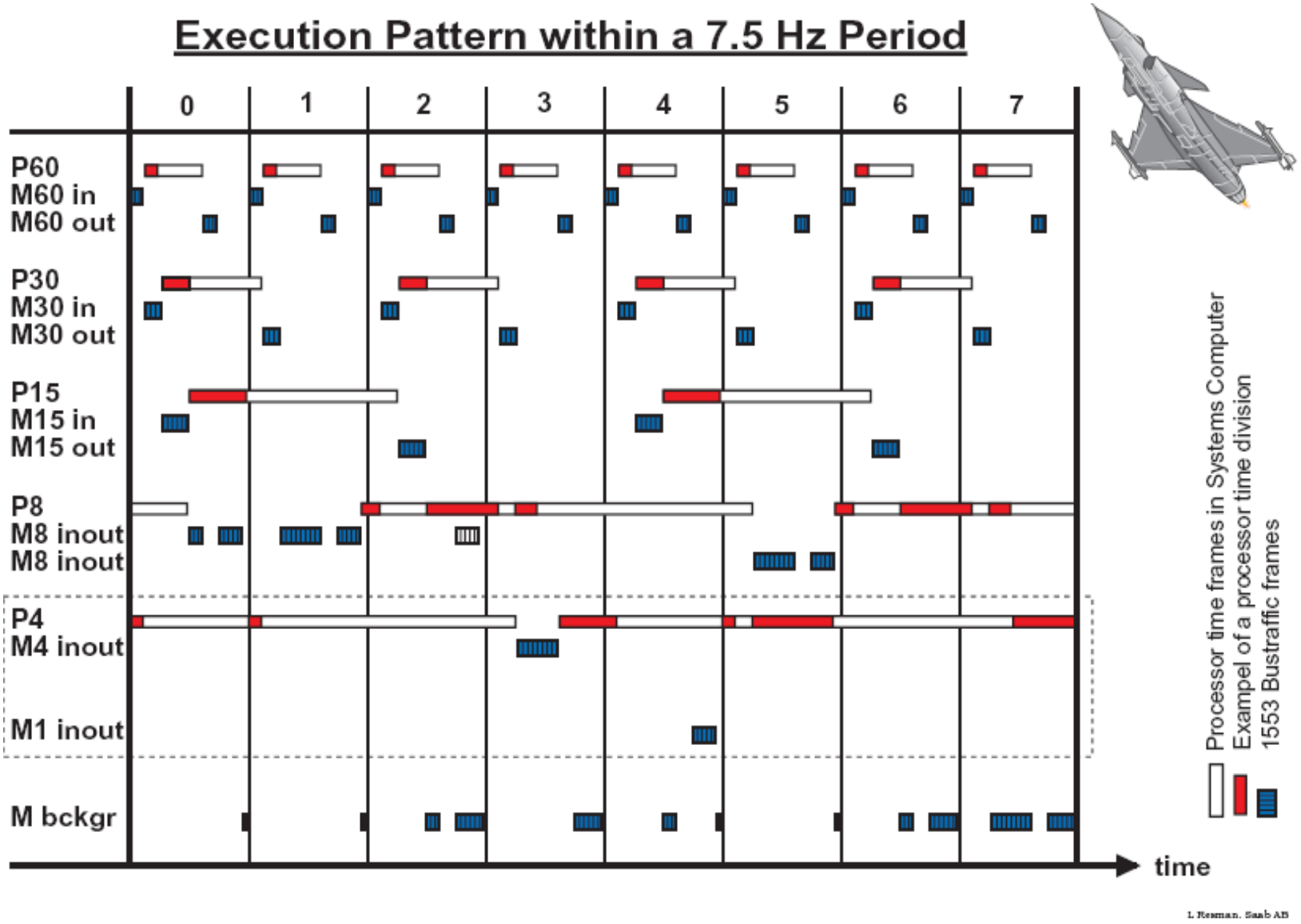
- Control, monitoring and display of continuously running processes, where the movement of your own and other aircraft are typical example.
- Reactions on mode changes and discrete events in the cockpit, the avionics, the real environment as well as in the computer execution.

The first case is the most demanding as to computer resource and has thus set the total execution strategy, periodic sampling. Periodic sampling is required with a complete spectrum of sampling frequencies (bandwidths) from 60 Hz to background execution.

Key strategies:

- Periodic execution with consecutively halved (harmonic) process frequencies (60, 30, 15 … Hz) and a low priority background process.
- Process priorities (monotonically) rising with frequency (Harmonic Rate Monotonic Scheduling).
- For each sub function the lowest sufficient execution frequency is selected.
- Data bus traffic and data processing are arranged non-overlapping for corresponding frequency.

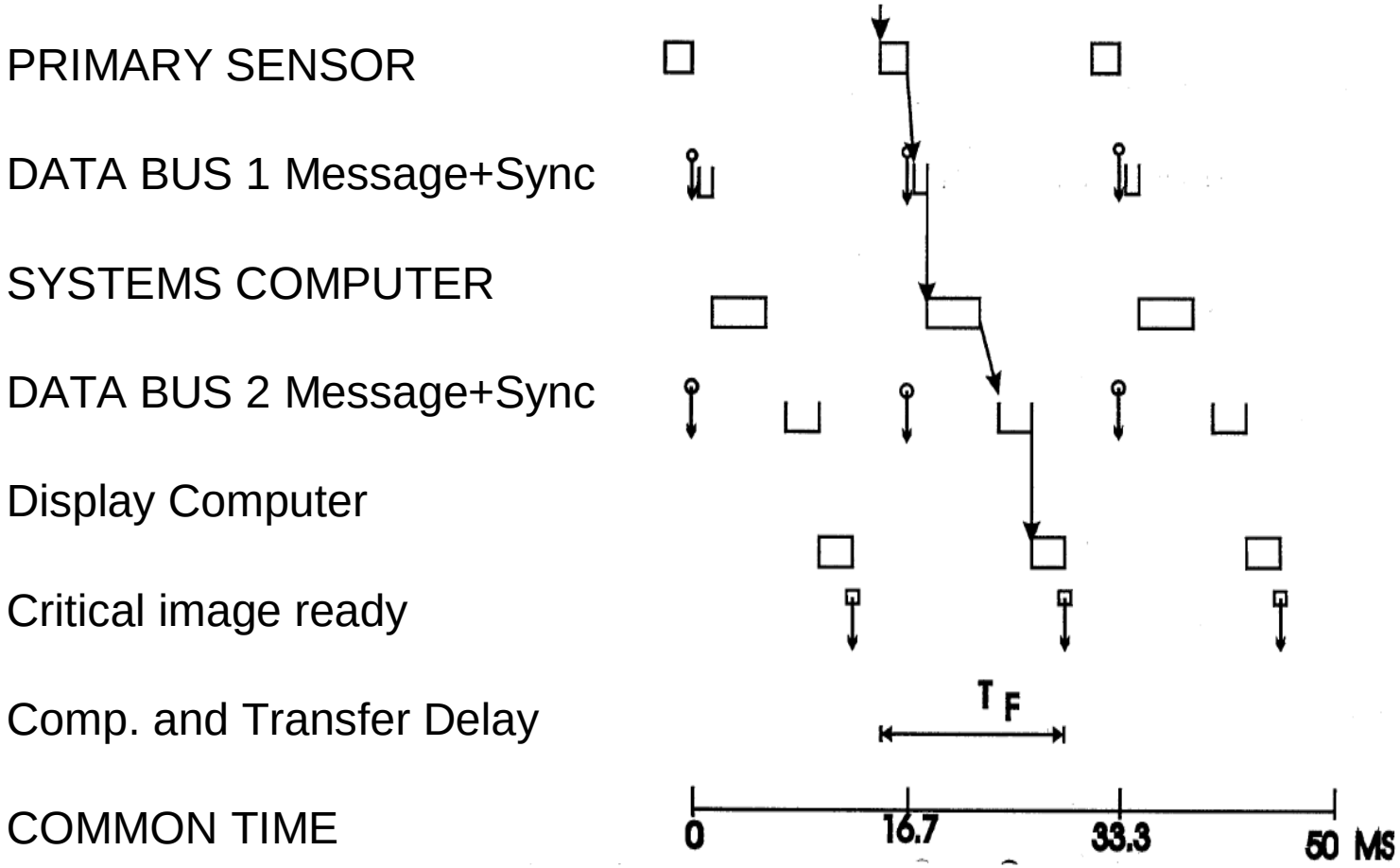
Execution Pattern within a 7.5 Hz Period



L Rosman, Saab AB

Execution architecture GRIPEN

Synchronization between subsystems. Data Delay.



Swedish approach, Integrated Federated

- Synchronized system
- Simplified information sharing and data fusion
- High resource utilization of computing resources
- Small and deterministic delays
- Data integrity requires attention
- Sensitive to singel faults
- Changes are not contained
- One level of criticality
- Special purpose h/w and s/w
- Long development cycles

IMA Goals
(Defined by University of York)

- Technology Transparency
  - The underlying hardware should not have any impact on an application either during development nor execution
- Scheduled Maintenance
  - The system should have in built capability to operate in the presence of failures so that Maintenance Free Operating Periods (MFOPS) can be achieved
- Incremental update
  - The system should be designed such that applications can be inserted/altered with minimum impact on other applications and on the supporting safety case

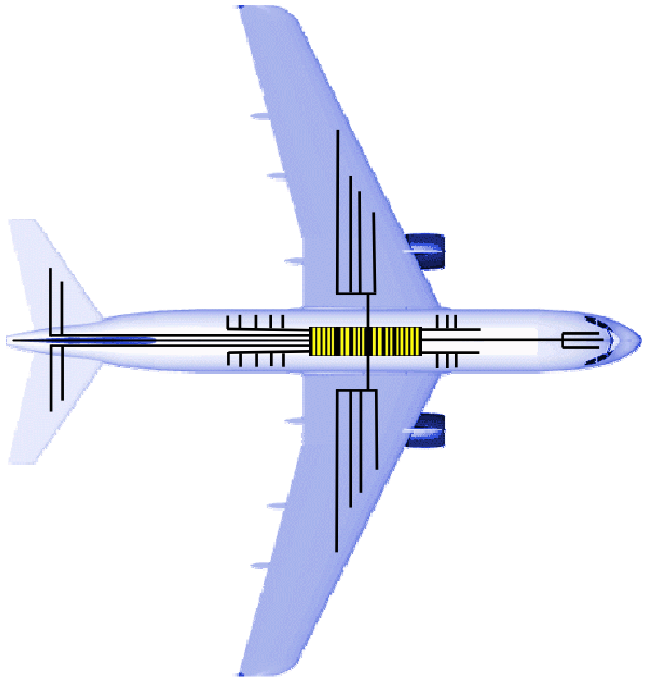
Features of IMA (Defined by University of York)

- Layered architecture
- Reconfiguration of applications on the module
- Protection mechanisms (Partitioning)
- Flexible scheduling to meet the deadlines of all the applications, for each viable configuration and when system is upgraded
- Code reuse and portability
- An operating system to manage the applications
- Physical integration of networks, modules and I/O devices
- Designed for growth and change

Integrated Modular Avionics, IMA

- Central rack system with communication backplane holding an array of cards, each card is an LRU
- Sharing of resources
- Industry standard LRUs fit to common backplane
- **However**
  - Backplane must be separated for safety
  - Complexity and throughput – split to “integration areas”
  - LRUs I/O via central rack

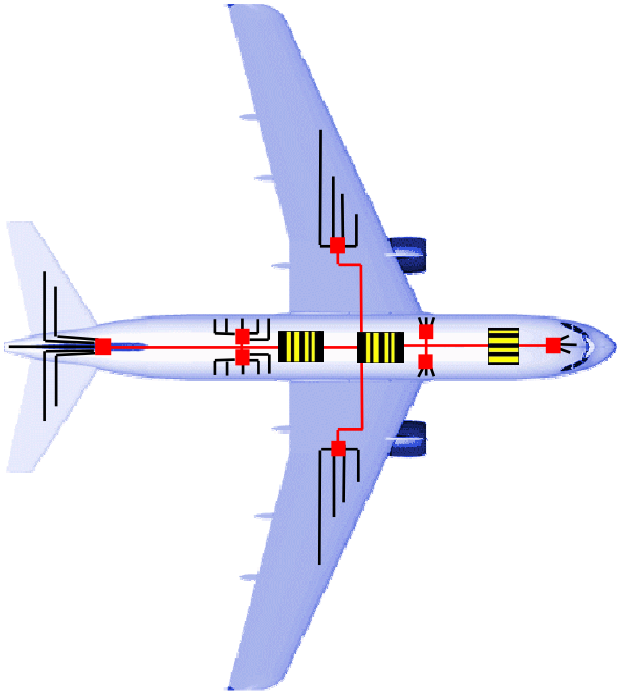
IMA System



Distributed Integrated Modular Avionics, DIMA

- As IMA but distributed intelligence
- I/O close to actuators and sensors
- Computation close to actuators and sensors
- COTS computers and I/O units as Modules
- Separation into integration areas (e.g. Cockpit, Cabin, Flight Control, Engines, Fuel)
- **Requires**
  - High bandwidth communication

Distributed IMA System



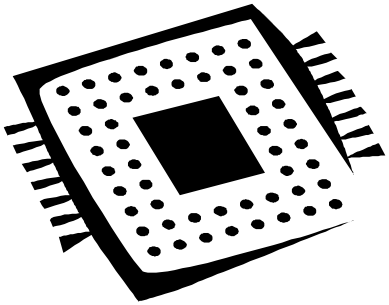
DRIVERS

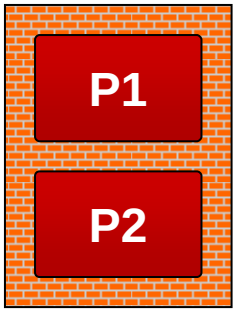
- Save Weight, Volume, Power, Cooling air
- Reduce number of spares
- Flexibility, Simplify functional growth
- Scalability, move functions to other plattforms
- Simplify obsolesence handling
- Incremental certification

- Civil aviation:
- Several partions (functions) in same CPU, mixed criticallity

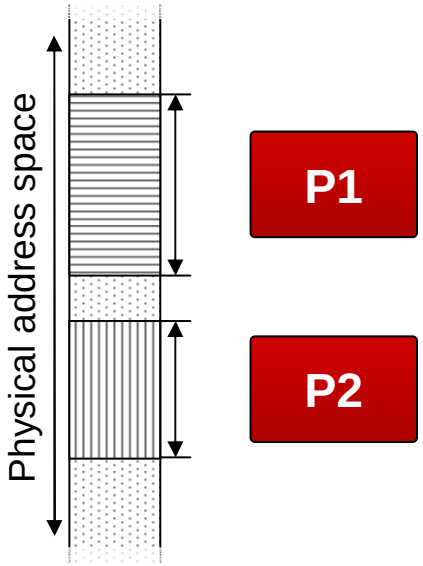
- Military : Separate functions from each other in several partitions in same CPU, mixed criticallity

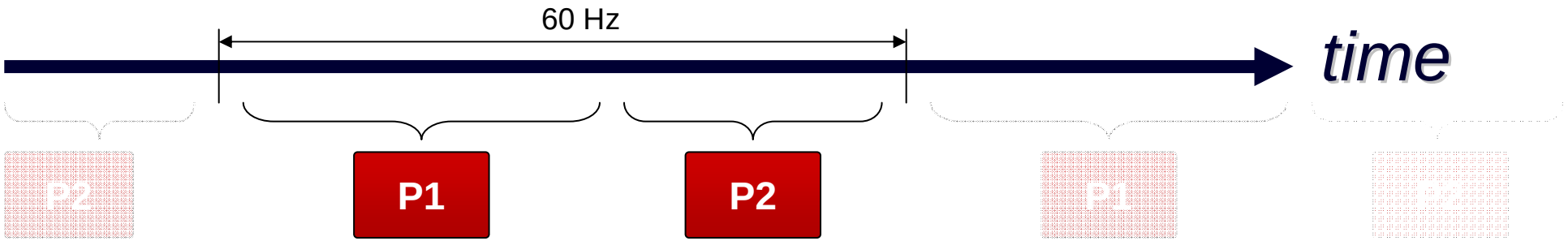
ARINC-653

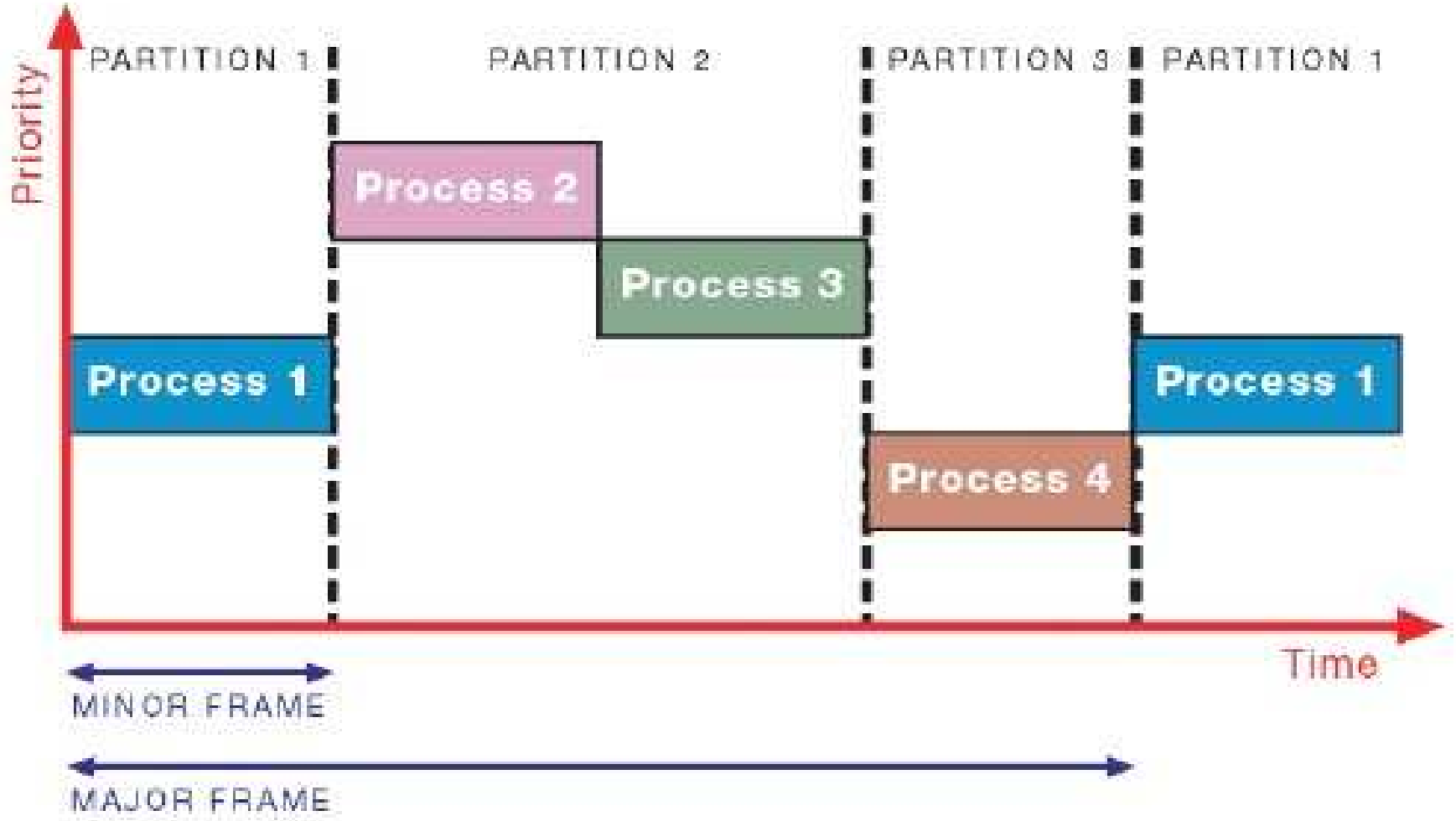




- Time separation
- Memory separation



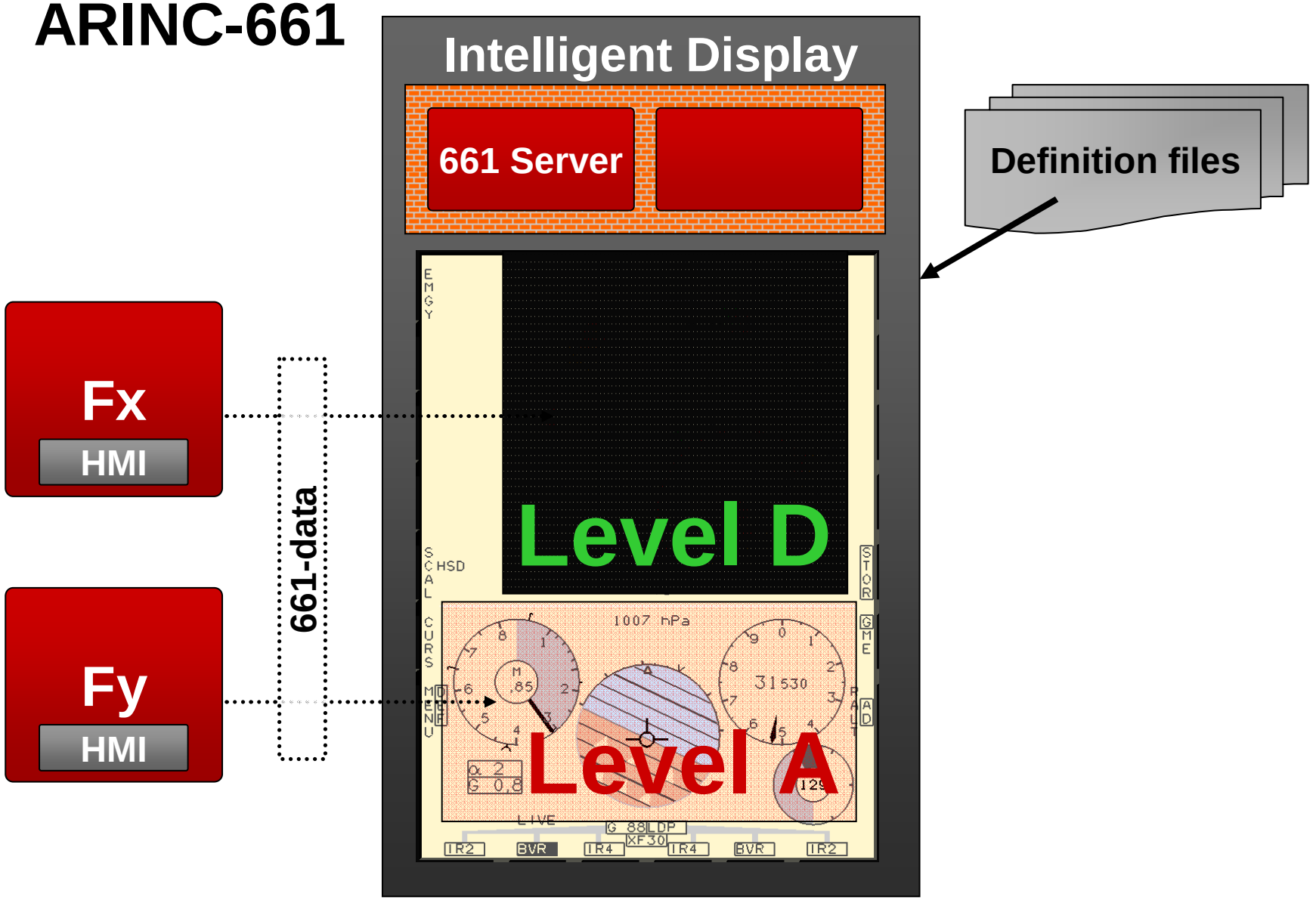



PARTITION 1
PARTITION 2
PARTITION 3
PARTITION 1
Priority
Process 2
Process 3
Process 1
Process 1
Process 4
Time
MINOR FRAME
MAJOR FRAME

ARINC 653

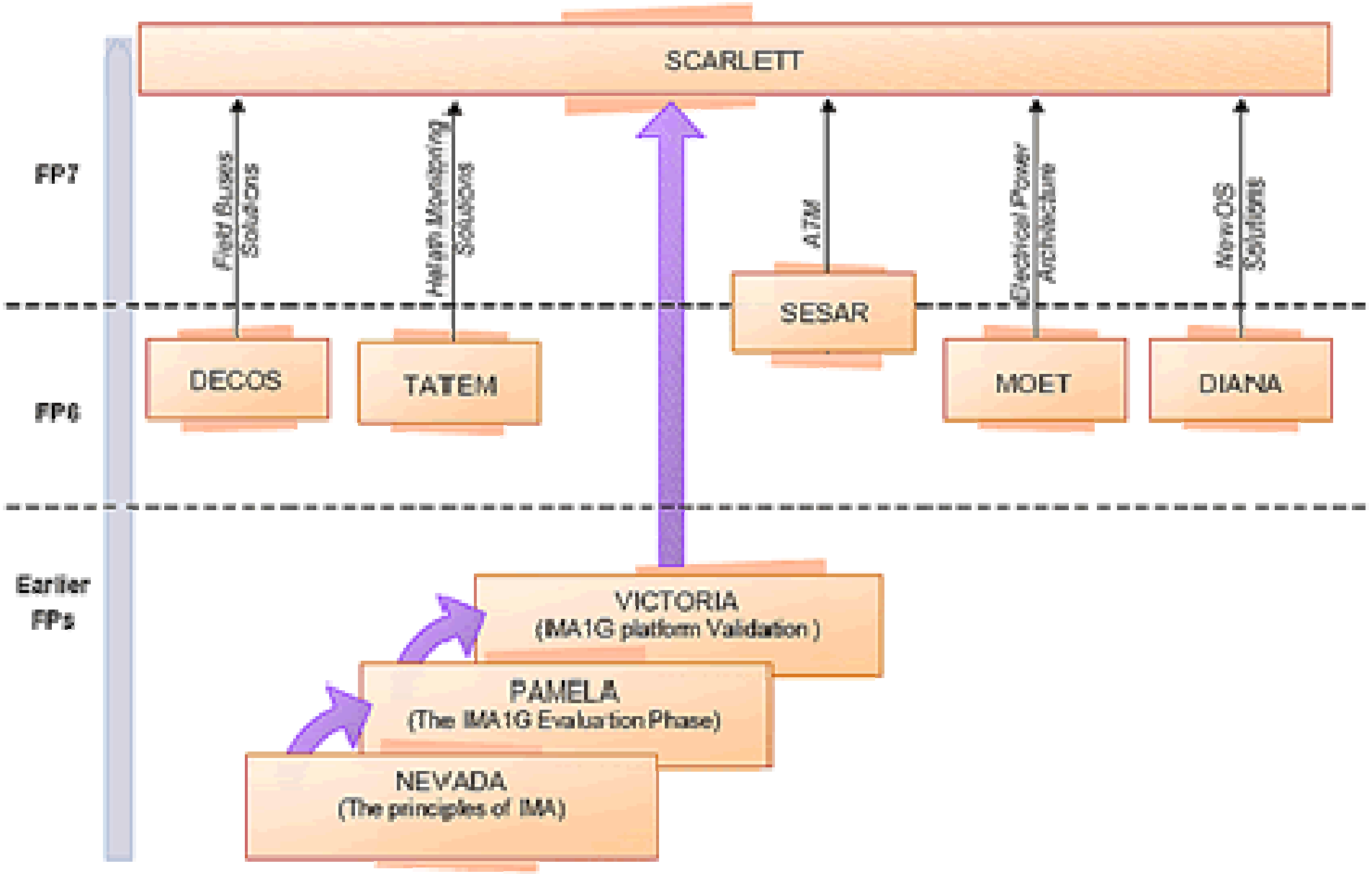
- Partition Management
- Process Management
- Time Management
- Memory Management
- Interpartition Communication
- Intrapartition Communication
- Health Monitoring

ARINC-661


Intelligent Display
661 Server
Definition files
Fx
HMI
Fy
HMI
661-data
Level D
Level A
1007 hPa
31530
LIVE
IR2
BVR
IR4
IR4
BVR
IR2

IMA ”1G”

- Civil cabinett standards
  - ARINC-…
- Civil standards
  - ARINC-653 Application Software Interface
  - ARINC-661 Display System Interface
  - ARINC-664 Data Network, AFDX (Avionics Full Duplex Switched Ethernet)
- Military alternative
  - ASAAC (Allied Standard Avionics Architecture Council)
    - Applications
    - Resources
    - Blueprints


SCARLETT
FP7
FP6
Earlier FPs
Flight Busses Solutions
Health Monitoring Solutions
AFM
Electrical Power Architecture
Non-OS Solutions
DECOS
TATEM
SESAR
MOET
DIANA
VICTORIA
(IMA1G platform Validation)
PAMELA
(The IMA1G Evaluation Phase)
NEVADA
(The principles of IMA)

EU project SCARLETT Partners

- THALES AVIONICS
- ARTTIC
- AIRBUS FRANCE
- AIRBUS DEUTSCHLAND GMBH
- AIRBUS UK
- DIEHL AEROSPACE
- GE Aviation Systems
- ACQ INDUCOM
- ALENIA AERONAUTICA S.P.A.
- ARION.FR
- BARCO N.V.
- DASSAULT AVIATION
- EADS GERMANY INNOVATION WORKS GMBH
- SELEX GALILEO S.P.A.
- FEDERAL STATE UNITARY ENTERPRISE ""STATE RESEARCH INSTITUTE OF AVIATION SYSTEMS""
- HELLENIC AEROSPACE INDUSTRY SA
- INSTITUTO DE SOLDADURA E QUALIDADE
- MESSIER BUGATTI
- NATUREN LTD.
- NATIONAL AEROSPACE LABORATORY (NLR)
- SYSGO AG
- OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES
- QINETIQ
- SAAB AB

- SAGEM DEFENSE SECURITE
- SKYSOFT PORTUGAL, SOFTWARE E TECNOLOGIAS DE INFORMAÇÃO S.A.
- SYDERAL SA
- THALES AVIONICS ELECTRICAL SYSTEMS SA
- TTTECH COMPUTERTECHNIK AG
- UNIS
- UNIVERSITY OF BREMEN (TZI)
- TECHNICAL UNIVERSITY HAMBURG-HARBURG
- RZESZOW UNIVERSITY OF TECHNOLOGY
- YAMAR ELECTRONICS LTD.
- TELETEL TELECOMMUNICATIONS & INFORMATION TECHNOLOGY SA
- UNIVERSITY OF NOTTINGHAM
- THALES RESEARCH & TECHNOLOGY
- AOA APPARATEBAU GAUTING GMBH
- UNIVERSITY OF BRISTOL, SAFETY SYSTEMS RESEARCH CENTRE
- Airbus Operations SAS

IMA ”2G”, EU project SCARLETT

- System oriented
- DME´s (Distributed Module Electronics)
  - CPM, RDC, RPC, REU…
- Advanced processes and tools for application development and application integration into system
- Common DME supporting wide range of avionic applications
- Common DME supporting wide range of aircraft types
- Fault tolerance and reconfiguration involves several DME’s
- More independece application/hardware by thicker middleware layer

High Level Requirements

The Customer High Level Requirements may consist of

- Concept of Operations
- Operational Requirements
- Functional Requirements
- Safety Requirements
- Reliability Requirements

Design Constraints

The design of the avionic system is influenced by e.g.:

- System Safety
- System Availability, fault tolerance, HW redundancy, FM, BIT
- Environmental conditions, Temperature/Vibrations/Accelerations
- Limitations in equipment, Weight/Volume/Power/Cooling/Connectors
- Number of Units to be manufactured
- Use of COTS equipment
- The length of time the system shall be operational
- Growth Potential
- Available computer capacity
- Flexibility, scalability
- Communication needs
- Time delay, end-to-end
- Allowed execution time
- Single pilot, multiple tasks (coordinate display and maneuver functions, Data fusion))

System Safety Requirements

- Rules of Military Aviation (Sw: RML – Regler för Militär Luftfart)
- Requirements and activities governed by applicable parts of:
  - MIL-STD-882C System Safety Req.
  - SAE/ARP4754/ED-79 ”Complex Systems”
  - SAE/ARP 4761 ”Safety Assessment Process”
  - RTCA/DO-160D Environmental Conditions and Test Procedures
  - RTCA/DO-178B/ED-12B ”SW Considerations..”
  - RTCA/DO-254/ED-80 Design Assurance Guidance for Airborne Electronic HW
- Note, reversed criticality definitions compared to Automotive (A=High crit, E=Low crit)
- General requirements
  - ”No” single catastrophic faults or occurrence
  - Independence between normal and back up system
  - Built In Test, maintenance
  - Robustness, safe and sound handling
  - Max accident rate

Design Criteria, (882C)

- **Eliminate** Hazards through design.
- **Minimize** the effect so they can be controlled.
- Introduce **Warning-system** to make emergency procedures possible.
- If it is impossible to eliminate or control a Hazard – risks should be avoided through **Restrictions, Special instructions** etc.

Design Flow

- Divide system into Materiel groups (or civil ATA-groups)
- Functions allocated to the MG's

- Functional break down into subfunctions and related to mission phases (mission preparation, a/c start up, take off, mission, landing, mission evaluation…)

- SysML modelling on high level => use cases for functions and subfunctions, Sequence and Activity diagrams
- Define Applications/Partitions and Communication flows
- Allocate Applications/Partitions to HW resources

Design Flow

- Further Functional modelling (SysML) if needed
- Implementation modelling
- Display modelling

New issues with IMA

- Time management
  - Strict allocation of time to partitions
- Load balancing, Late binding
- The S/W applications and their interfaces must be chosen carefully in order to reduce the system complexity, latencies and minimize data couplings.
- Co-Location of applications into Partitions, Redundancy separation
- Partition restart vs Computer restart
- Incremental Verification


SAAB
SAABGROUP.COM