AVT-357 Research Workshop on “Technologies for future distributed engine control systems (DECS)”

Challenges and Chances of Multi-Core processors within future Control- and Monitoring FADEC

K. Stastny, AES, Germany
M. Wichmann, AES, Germany
L. Rietschel, MTU AeroEngines, Germany

aes AEROSPACE EMBEDDED SOLUTIONS

MTU Aero Engines

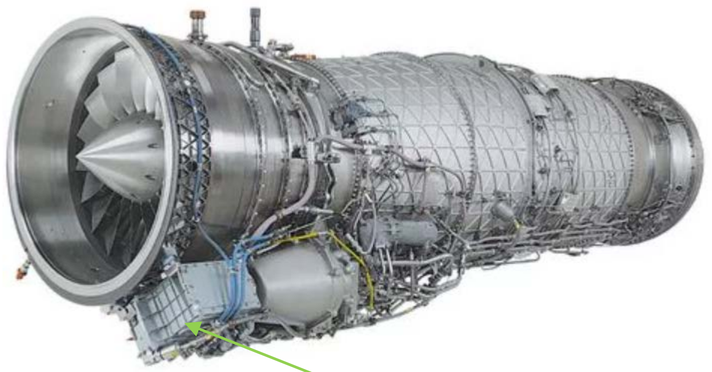
Agenda

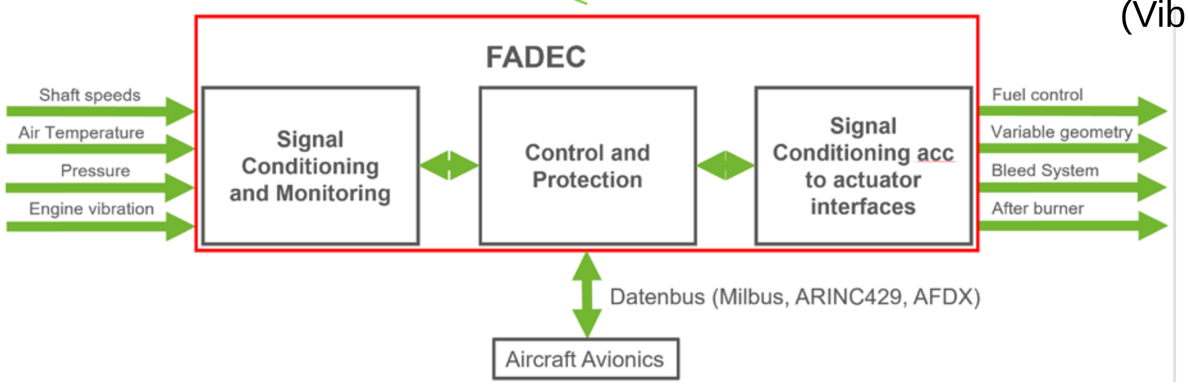
- **Todays FADEC Objectives**
- **Future Trends on Military Engines**
- **Requirements for Future FADEC**
- **Usage of Multi-Core Processors**
- **Current Opportunities and Risks**

Todays fighter engine configuration / FADEC

Todays fighter engine configuration / FADEC

- Control
  - Thrust core engine
  - Afterburner
  - Thrust vectoring
- Monitoring
  - Sensor plausibility
  - Actuator plausibility
  - Storage of engine mission data (Life Usage Monitoring)
  - Engine health status (Vibration monitoring)





FADEC

Shaft speeds

Air Temperature

Pressure

Engine vibration

Signal Conditioning and Monitoring

Control and Protection

Signal Conditioning acc to actuator interfaces

Fuel control

Variable geometry

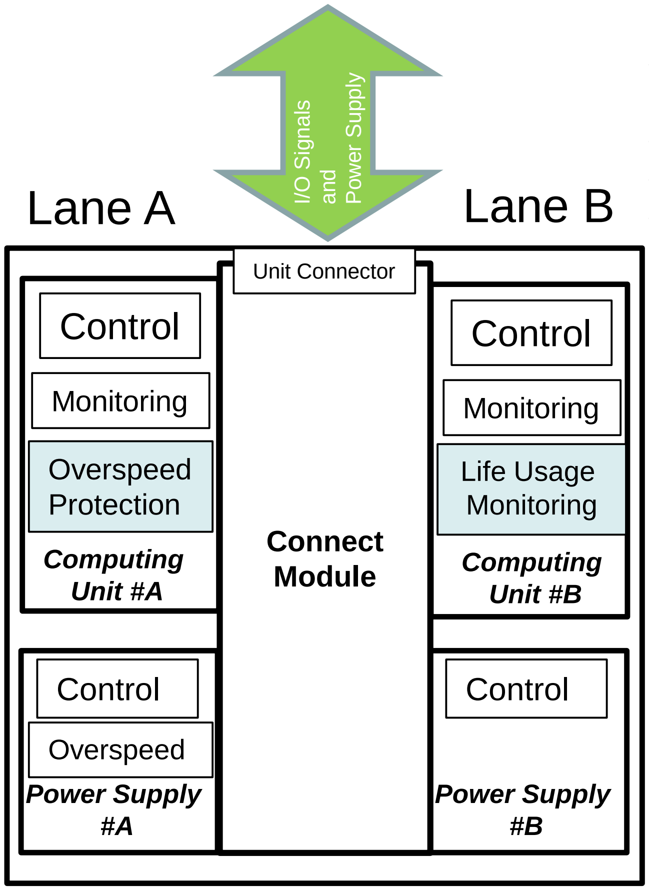
Bleed System

After burner

Datenbus (Milbus, ARINC429, AFDX)

Aircraft Avionics

Principle of todays FADEC



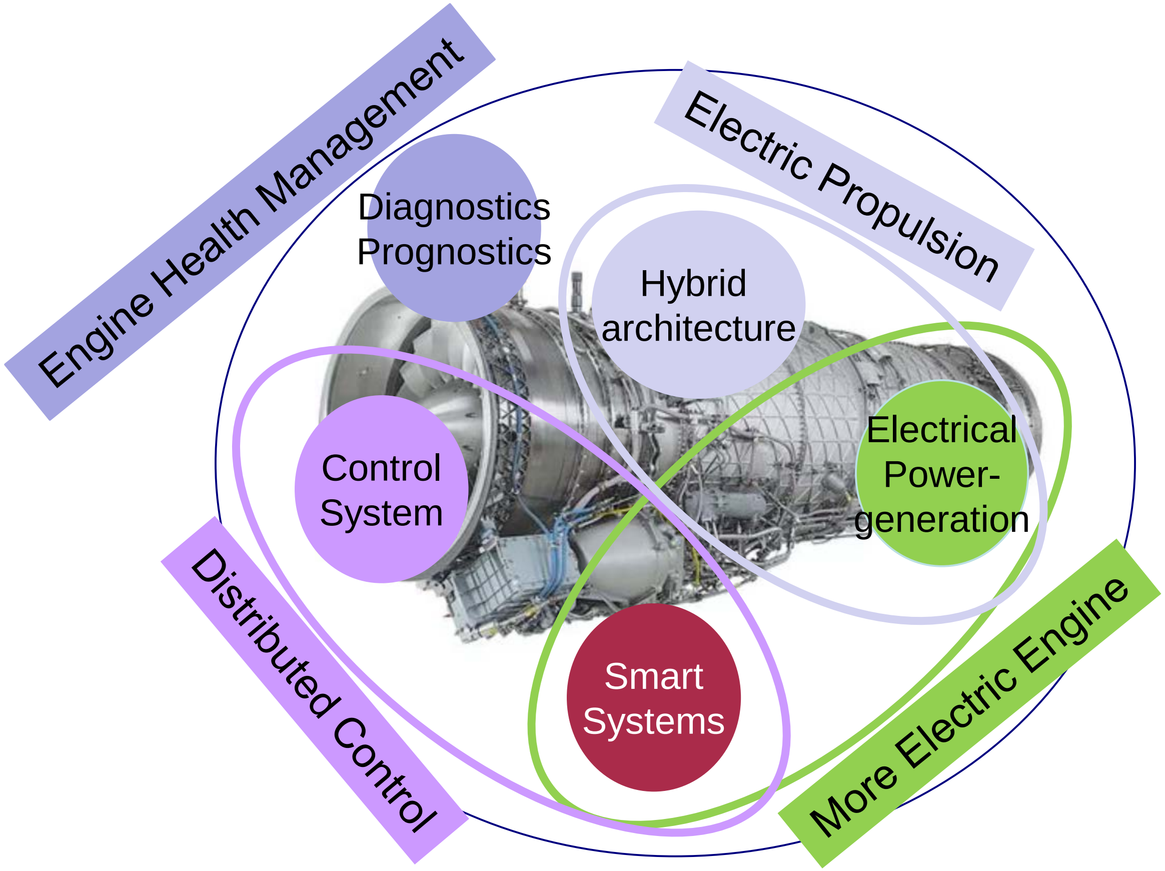
- 2 similar Engine Control Monitoring Processing Units in Active / Active configuration
- Both channels are time synchronized
- Dedicated channel change logic guarantees “independent” channel change
- Usage of dedicated Micro Controllers and FPGAs for each functionality

Future Engine Configuration – Key FADEC Objectives

Future Engine Control System challenges

Improvements in:

- Performance
- Efficiency
- Energy Sources
- Reliability
- Availability
- Maintainability



Distributed Control technology Objectives

- **(D1) Replace existing engine accessories by smart actuators / sensors.**

- **(D2) Optimize accessories performance based on engine mission (no fixed link to engine shaft speed [gear box]).**

- **(D3) Implementation of distributed control architecture where engine control function can be configured to different controllers ("Integrated Modular Avionics" approach).**

- **(D4) Share calculation power between different controllers (adaptive CPU power) according to current mission needs (e.g. diagnostics / prognostics) – one common propulsion system (2 engines / 1 FADEC).**

- **(D5) Introduction of advanced control laws (e.g. adaptive control) including new actuators.**

More Electric Engine

- **(M1) Implementation of additional electrical power generators (e.g. LPT – Gen, HP generators).**
- **(M2) High voltage power network (> +/- 270 V DC).**
- **(M3) Merge electrical / pneumatic and hydraulic power into optimized one energy system (electrical power).**
- **(M4) Implementation of electrically-driven actuators (e.g. Smart Fuel System).**
- **(M5) Implementation of electrical batteries to manage short peak loads.**
- **(M6) Carbon fiber aircraft structure.**

Electric Propulsion

- **(E1) Electrical boost of gas turbine engine during take-off and in emergency situations.**
- **(E2) Energy regeneration during descent.**
- **(E3) Hybrid architecture for propulsion.**

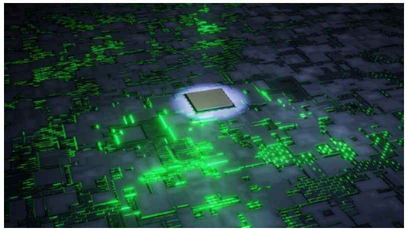
Engine Health Management Objectives

- **(H1) Real Time (on board) diagnostics and prognostics.**
- **(H2) Real Time (on board) life usage prediction.**
- **(H3) Onboard engine characterization and sensor modelling.**
- **(H4) Real Time diagnostics interaction with pilot and maintenance crew.**

Additional FADEC needs

Technology needs – FADEC Multi-Core Processor

- **Reconfigurable and Distributed Controls**
  - Definition and adaptation of “IMA technology” for smart engine control system
  - High performance CPU architecture (Multi-Core, System On Chip)



- **Cyber Security compliant architecture**
  - Threat data base development
  - Secure Hardware key components and SW development methods
  - Definition of encryption technologies
  - Secure Ground station architecture

- **Big Data Management**
  - Data Storage Technologies
  - Data Management Technologies

Technology needs - Software

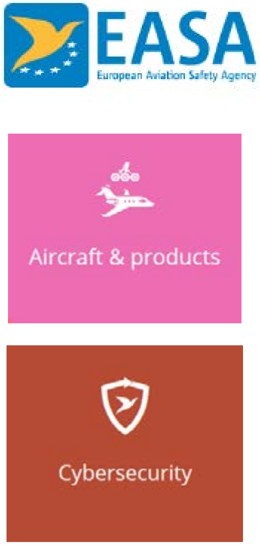
- **High Performance / Multi Core Operating System**
  - ITAR / EAR free operating system
  - Secure and Multi Core capable OS
  - Reconfigurable SW strategies

- **Adaptive Controller Architecture Structure**
  - Certifiable adaptive controller software methods
  - Verification strategy for adaptive controller algorithm
  - High performance computing algorithm (model of the system)

- **Secure SW methods**
  - Encryption algorithm implementation / verification methods
  - Defensive implementation methods / standards

Technology needs - Certification

- Multi Core Controller (DAL-A) verification methods
- Adaptive Controller Verification strategies
- Cyber Security certification needs (e.g. DO-326 / DO-356) and penetration-test
- Blue Print (reconfiguration of a system based on Health status) certification concept



Usage of Multi-Core Processors

Certification Objectives for MCU

- **Certification objectives of the MCP based system are essentially the same as for SCP system:**
    - System needs to be deterministic – this means that for known set of inputs the system will always produce a known set of outputs (predictable outcome).The outcome needs to be produced repeatedly (rate) within specific period of time (duration).
    - Robust Resource Partitioning shall be achieved:
        - SW partitions cannot use more resources than allocated to them
        - SW partition cannot corrupt the data / storage areas of an other partitions
        - SW or HW Failure unique to a specific SW partition cannot inadvertently affect an other partition
    - Robust Time Partitioning shall be achieved:
        - SW partitions do not consume more time that allocated to them, regardless of if they execute on a single- or multi-cores
        - SW partitions do not affect other SW partitions under all conditions (failure in execution of one SW partition shall not affect timely execution of other partitions).
    - Software that provides partition shall be of the same SW level as the highest SW level of the SW it partitions.
    - A Safety Net shall be provided – mitigation of risks associated with COTS HW through passive monitoring and active fault avoidance and system recovery functions

Multi-Core Processor Selection Requirements

The selection of a multicore processor is mainly related the following topics:

- Performance requirements (e.g. core, network and floating point performance)
- Availability of a DO-178C DAL A RTOS (e.g. *Wind River* VxWorks 653, *Greenhills* INTEGRITY-178, *Sysgo* PIKEOS, LynxOS-178, *DDC-I* Deos, *Kronosafe* Asterios)
- Independence of peripheral controllers
- Interference in the SoC interconnect fabric
- Support of all DAL levels coexisting on partitions within a single SoC
- Flexible License Business Model for different products and platforms
- Certification support package availability
- CAST-32A / AMC 20-193 compliant multicore design

Multi-Core Processor Roadmap

FADEC In Service
single core

NXP
MPC5566
(Power Arch e200 z6)

Mainly in
Avionics products

NXP
T2080
(Power Arch e6500)

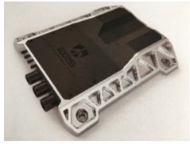
XILINX 16nm
Ultrascale+
ZYNQ
(ARM A53)

NXP
MPC5777C
(Power Arch e200 z7)

Next Generation of FADEC
(EIS ~ 2023)
dual core

XILINX 7nm
Ultrascale+
VERSAL
(ARM A72)

NXP
S32S
(ARM R52)
NXP LayerScape
(ARM A53)



Future FADEC
(EIS ~ 2030)
multi core

Multicore usage in aerospace

ARM core relevance for embedded systems

2006 2012 2016 2021

Roadmap
FADEC CPU

Operating Systems

The most difficult challenge on multi-core processors is to handle *interference* between cores via shared resources. These are typically memory controllers, cache, DDR memory, I/O and the internal fabric that connects all of these peripherals. This interference has to be managed as proposed by CAST-32A/ AMC20-193.

An operating system can effectively manage the interference based on runtime mechanisms, Memory and Peripheral Management Unit configurations, libraries and tools that address all CAST-32A/ AMC20-193 objectives.

RTOS Overview

Three RTOS candidates have been identified as preferred candidates for a FADEC

DDC-I

- *DDC-I* ***Deos***: A DAL A certifiable single and multicore platform RTOS kernel allowing space and time partitioning. Implemented today in nearly every commercial aircraft in various certified systems. Supports Power Architecture, ARM and Intel x86 targets. 30 years of experience.

KRONO-SAFE
Safe design in real-time

- *KRONO-SAFE* ***Asterios***: A DAL A certifiable multicore platform RTOS kernel allowing space and time partitioning. Wide range of supported targets (Power Architecture, ARM, XILINX Zynq). First DAL A certification for FADEC in progress. 10 years of experience.

SYSGO
EMBEDDING INNOVATIONS

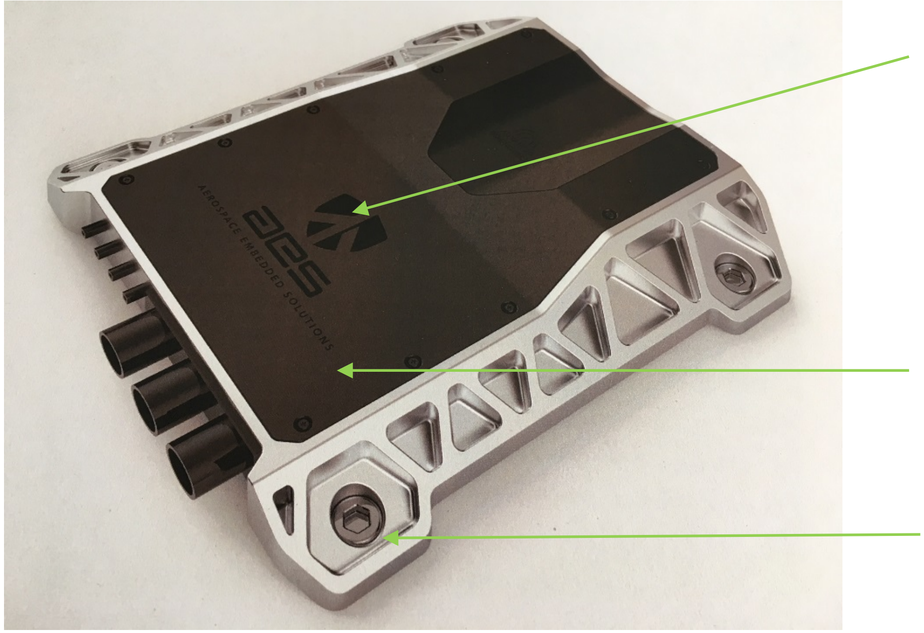
- *SYSGO* ***Pike OS***: A DAL A certifiable multi-core platform RTOS and type 1 hypervisor, allowing space and time partitioning. Supports Power Architecture, ARM and Intel x86 targets. 25 years of experience.

Opportunities and Risks

Opportunities and Risks within Multi-Core Processors

- Applications on multi-core processors require a specific scheduling architecture for data exchange between cores to eliminate interferences.
- In depth knowledge of possible target interference channels (deeper understanding of processor technology) is mandatory.
- Change from PowerPC CPU Cores into ARM based CPU Cores.
- Verification tools must be specifically tailored to address all target specific interference channels.
- Usage of a COTS OS gets more mandatory due to the complexity of the targets (additional dependence).
- Increased complexity regarding data communication (share of sources with more cores).
- Changes in SW development processes to comply with additional multi-core Certification Objectives.
- Usage of COTS RTOS instead of proprietary scheduler.
- Change of verification strategies due to higher functional integration within a multi-core Processor.

Future FADEC - Opportunities



High Performance Computer Platform allows

- Adaptive Control Laws, Onboard Engine Diagnostics and Prognostics
- Cyber security protected gateway functionality for distributed control communication
- Big Data Management of Prognostics Date
- Mission specific re-configurability of Computer Platform

- Capability to implement two channels on a common PCB (higher package density)

- Reduction of weight and size on future FADEC

Abbreviations

ARM	Advanced RISC Machines
COTS	Commercial Off The Shelf
CPU	Centralized Processing Unit
DAL	Design Assurance Level
DDR	Double Data Rate
EAR	Export Administration Regulation
FADEC	Full Authority Digital Engine Control
FPGA	Field Programmable Gate Array
HP	High Pressure
HW	Hardware
I/O	Input / Output
ITAR	International Traffic in Arms Regulation
LPT	Low Pressure Turbine
RTOS	Real Time Operating Software
SoC	System on Chip
SW	Software

THANK YOU