August 2004

Serge GOIFFON
Pierre GAUFILLET
AIRBUS France

Linux
A multi-purpose executive support for civil avionics applications ?

Civil avionics software context

- **Main characteristics**
  - Required dependability
  - More and more software intensive : From 23Kb to 100Mb and more
  - Synchronous and asynchronous architectures
  - Very long lifetime compared to hardware components
  - Integrated Modular Avionics concepts as new paradigm

- **Development process based on DO-178B/ED-12B**
  - Guidance for satisfying airworthiness requirements
  - Accepted by industrials
  - Define processes and processes data
  - Level of assurance and completion criteria depend on software criticality level

Highly critical avionics systems

are not considered here !

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

The Operating System : a key component

- **O/S main objective**
  - Offers execution model and standard API to avionics applications
  - H/W access through drivers and generic services : no impact on applications if hardware changes
  - Portability, interoperability and reuse-ability of applications

- **Linux as a multi-purpose O/S candidate**
  - Open source based on common adopted standards -> portability, interoperability
  - Follows cooperative development model -> distributed knowledge, innovation
  - Adaptable, reliable, scalable, fits to a wide range of hardware components
  - Widely used and today mature for embedded market

- **3 steps for appropriation in avionics**
  - **Embedding Linux on avionics specific hardware platform**
  - **Host multi-level critical software : partitioning properties**
  - **Make Linux ready for DO-178B certification**

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Some features comparison ...

POSIX	ARINC 653
Event driven execution model	Cyclic based execution model
Multi-processing, multi-threading execution model	Same as POSIX but terminology used is partition for process, and process for threads
Priority preemptive scheduling for processes and threads	Within partition time slice : priority preemptive scheduling of A653 processes with deadline management
No temporal partitioning	Temporal partitioning : fixed allocation of time slices to partitions in a repetitive time frame pattern
I/O interrupt driven	I/O polling and I/O partitioning
Memory segregation	Same as POSIX but terminology is spatial partitioning
Socket	Sampling and queuing ports on I/O
Inter Process Communication	Sampling and queuing ports on RAM
Mutex and condition variables	Buffer, blackboard, semaphore, event
Timers	No timers like POSIX but API service to wait for timeout
Signal management	Health monitoring

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Linux for embedded and real-time systems

- Several OSS solutions based on Linux have been developed :

RTAI	KURT	QLinux
RTLinux	ADEOS	...
Linux/RK	RedLinux	

- The 2.6 kernel features low latency and preemptible kernel, and is now ready *out of the box* for soft real time systems.

- Today, some projects aiming to bring Linux to the required maturity for embedded uses are in progress :
  - Carrier grade Linux (telecoms) – high availability, hot swappability, kernel and driver robustness
  - FlightLinux (NASA) – Linux in Space systems
  - SELinux (NSA) – security enhanced Linux

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Embedding Linux on an avionics platform

- **Research project**
  - Replace existing POSIX RTOS by Linux, in avionics platform, without changing existing applications
- **Targets**
  - Acquire kernel internals knowledge (drivers, memory management, file systems, scheduling, synchronization, time management, ...)
  - Verify the Linux API conformance to the replaced O/S (limit the effort of porting existing applications to the new Linux platform)
- **Results**
  - Linux integrated on a i486 avionics platform with network capabilities
  - Reduced kernel footprint (memory, drivers, file system, ...)
  - Reduced common Unix tools footprint (using Busybox)
  - Adapted avionics I/O drivers and FLASH PROM file system with eXecute In Place capability
  - Re-use of an existing Ethernet driver (fast prototyping)
  - Avionics applications successfully migrated to this new environment

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

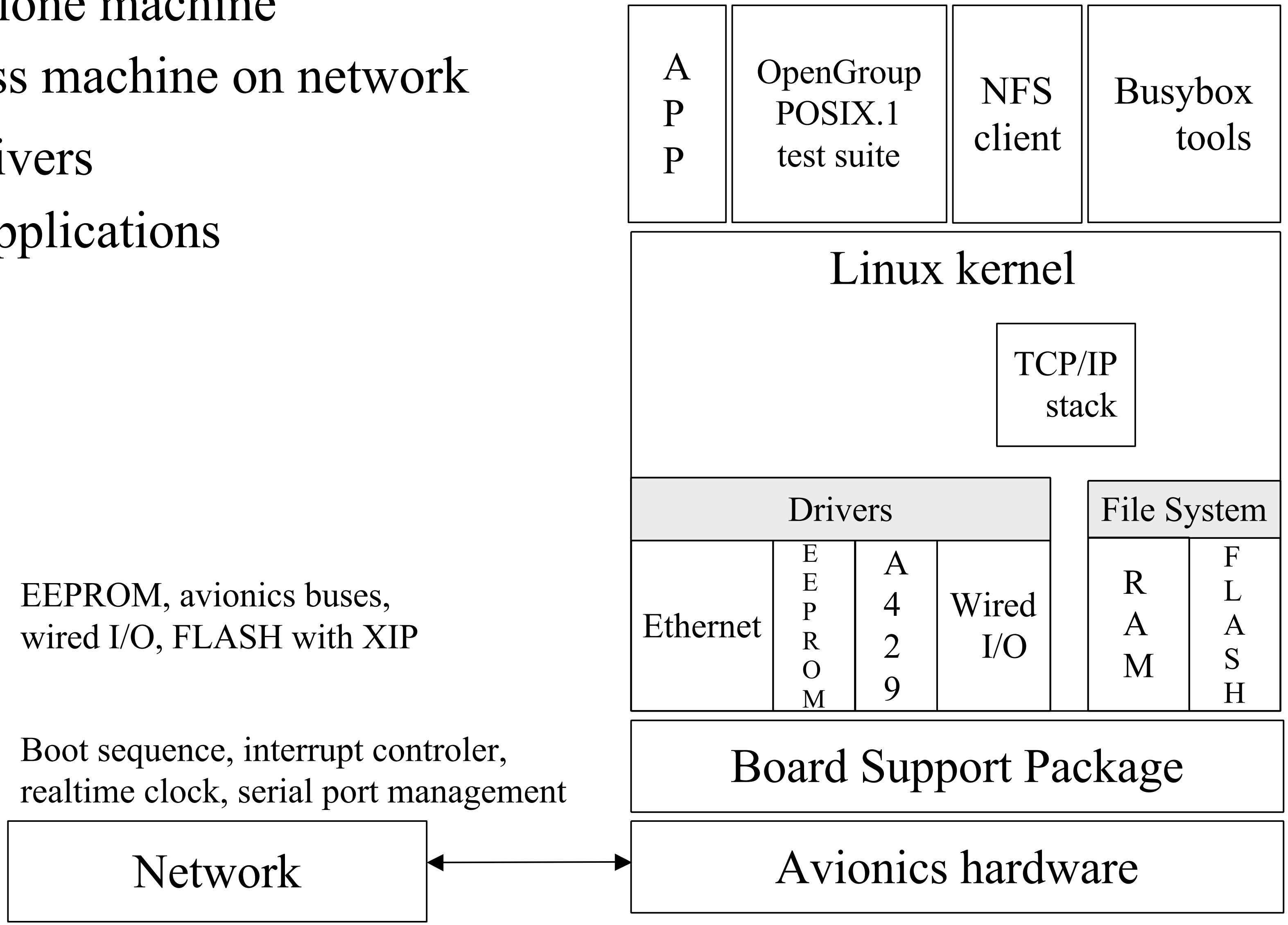
Embedded Linux diagram

1 – standalone machine

2 – diskless machine on network

3 – full drivers

4 – with applications



AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Host multi-level critical software

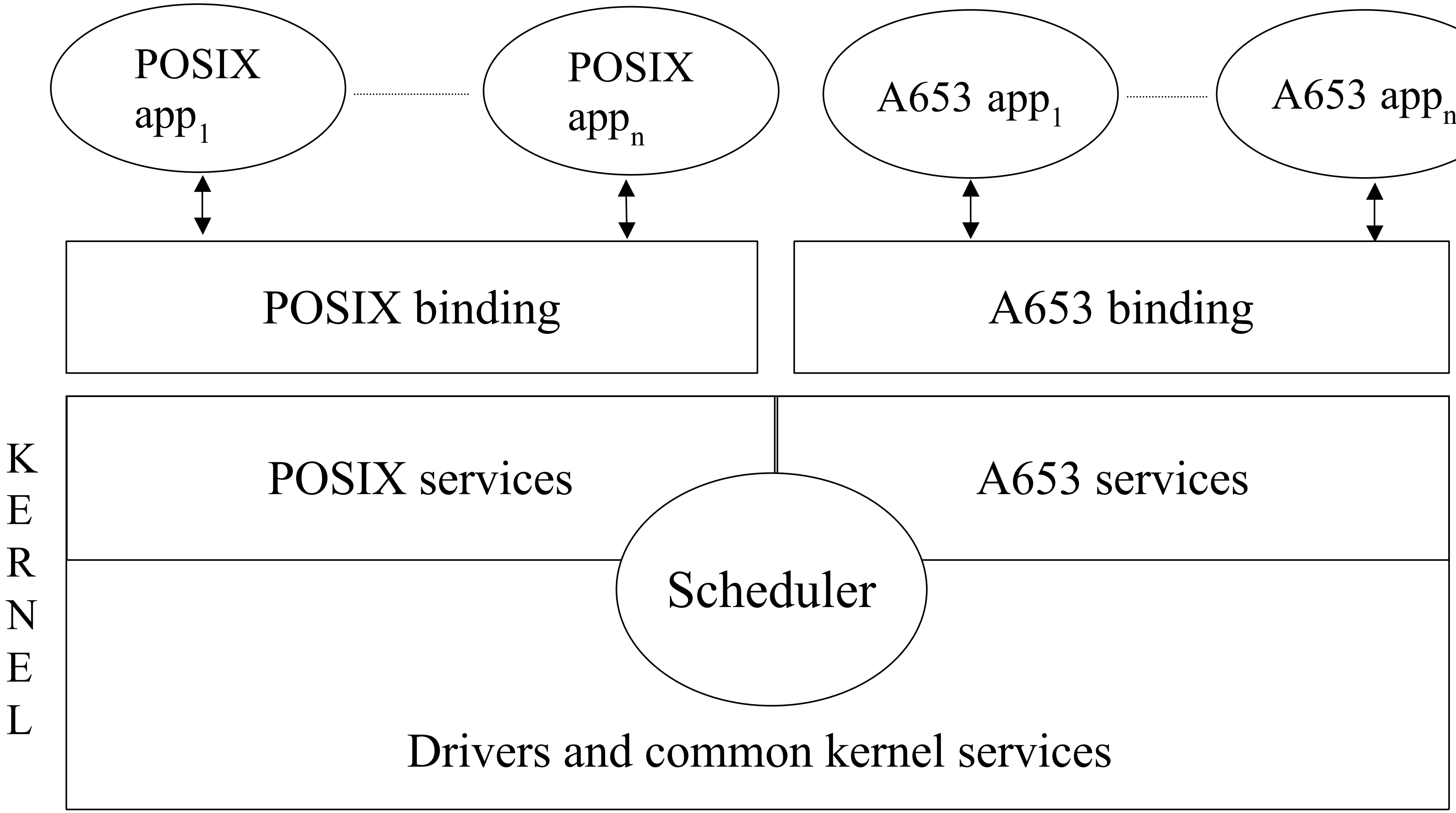
- **Research project**
  - Host avionics applications, based on Integrated Modular Avionics concepts and ARINC 653 standard, on Linux platform

- **Targets**
  - Implement ARINC 653 cyclic scheduler and temporal partitioning
  - Implement a standalone ARINC 653 API (not relying on POSIX services)

- **Results**
  - ***Scheduler adapted to run both ARINC 653 and POSIX applications***
  - ***Sampling and Queuing ports attached to RAM, Unix sockets or AFDX (Avionics Full DupleX Ethernet) ports***
  - ***Static allocation of A653 system resources and dynamic control of their use***
  - ***Management of process deadlines***
  - ***Linux Trace Tool adapted to view ARINC 653 events (context switches of A653 processes, API calls, partition switch, ...)***

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Host multi-level critical software diagram



AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Why Linux is not ready for DO-178B ?

- **From the DO-178B viewpoint**
  - No development and verification plans
  - Heterogeneous and complex development environment (distributed over Internet, multi-platform, etc.)
  - No universal requirement, design and code standards
  - No design document

- **But, from the product viewpoint**
  - OpenGroup testing environment provides test suites for POSIX conformance
  - Reliable software, modular architecture
  - Co-operative and hierarchically structured development model with centralised version management
  - Product reviewed and tested by peers

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

How to make Linux ready for DO-178B ?

- **Produce missing certification material using reverse engineering**
  - **Develop tools to extract semantic from code and produce kernel static and dynamic design**
  - **Focus on descriptions of the main kernel internal mechanisms**
- **Validation**
  - **Compliance to standard, robustness, kernel profiling and performance characterization**
- **Properties analysis**
  - Worst Case Execution Time, stack consumption, proof of properties in complex algorithms
- **Development**
  - Take part in the kernel development process to provide simple and deterministic algorithms in strategic parts of the software (memory management, scheduling, file system management)
  - Provide static allocation and dynamic control of system resources
  - Provide robust spatial and temporal partitioning

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Conclusion

- **Studies show using Linux in an avionics environment is possible.**

- **The main problem for certification is the predominant part of the process objectives of the DO-178B compared to a product objective approach...**

- **Linux gives low cost access to reliable and adaptable technology but appropriation cost for dependable systems is not negligible.**

- **Industrials need to work in partnership with labs and Linux experts to share the cost of reverse engineering activities.**

- **Those certification activities should be processed in an Open Source project.**

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.

Ce document et son contenu sont la propriété d'AIRBUS FRANCE S.A.S. Aucun droit de propriété intellectuelle n'est accordé par la communication du présent document et de son contenu. Ce document ne doit pas être reproduit ou communiqué à un tiers sans l'autorisation expresse et écrite d'AIRBUS FRANCE S.A.S. Ce document et son contenu ne doivent pas être utilisés à d'autres fins que celles qui sont autorisées.

Les déclarations faites dans ce document ne constituent pas une offre commerciale. Elles sont basées sur les postulats indiqués et sont exprimées de bonne foi. Si les motifs de ces déclarations n'étaient pas démontrés, AIRBUS FRANCE S.A.S serait prêt à en expliquer les fondements.

AIRBUS

AN EADS JOINT COMPANY
WITH BAE SYSTEMS

AIRBUS FRANCE S.A.S. Tous droits réservés. Document confidentiel.