OPEN ARCHITECTURE PLATFORMS FOR AVIONICS APPLICATIONS: CHALLENGES IN SAFETY CRITICAL SYSTEMS AND POSSIBLE SOLUTIONS

D. Geiger
Certification Expert, Department Head
Computing Platforms for Defence
Platform Software Avionics Computer
Airbus Defence and Space GmbH
Woerthstrasse 85, 89077 Ulm
Germany

A. Schacht
Certification Expert, Department Head
Computing Platforms for Defence
Platform Software Avionics Computer
Airbus Defence and Space GmbH
Claude-Dornier-Strasse
88090 Immenstaad, Germany

Abstract

Open Architecture Computing Platforms are the basis for competitive avionic systems. This platforms are standardized and can be used for various applications, reducing cost and risk. An additional advantage is the ease for porting of existing applications on updated avionics computing platforms i.e. in case of obsolescence. The basis for such platforms are powerful microprocessors. The trend in the consumer market to move from classical Single-Core Processors to Multi-Core Processors (MCP) based on Systems on a Chips (SOC)s imposes various limitations to the avionics industry. To demonstrate robust time and space partitioning for Multi-Core-Processors is challenging and in some cases even impossible. Certification challenges, existing guidance, possible solutions and possible way ahead are discussed in this paper.

Introduction

In the 1980s more and more electronic functions were entering the Aircraft. At this time for each AC function a dedicated computer was installed in the AC. The underlying computer HW was individually developed adapted to the specific needs of the applications. Changes and updates of such legacy systems are very hard to achieve as HW and SW modules have various interdependences.

The increased number of electronic functions in the AC was accompanied with weight penalties and increasing demand on electrical power and cooling. This leads to the wish to integrate independent functions in one computer. This concept is called Integrated Modular Avionics (IMA) or Open Architecture Computing Platform which was for a first time implemented around 2000 (example A380). This concept imposes various requirements to the computing platform. A computing platform consists of groups of Modules, including core SW, that manages HW resources in a manner sufficient to support at least one application [1].

Integrated Modular Avionics (IMA)

As a guidance for the development of IMA systems RTCA/DO297 [1] was written, covering system development process, system resource allocation, safety, development assurance, partitioning and resource management, health monitoring and fault management and others. Key aspects are partitioning and resource management to be performed to ensure incremental acceptance of the modules, platform and application.

The partitioning analysis should demonstrate that no application or sub-function in one partition could affect the behavior of a sub-function or application in any other partition. All propagation paths between partitions should be identified.

An important aspect of certification IMA systems is to obtain incremental acceptance of and certification credit for IMA platforms, modules and/or hosted applications, cumulating in IMA system installation approval in on an aircraft product.

Experience showed that the way to obtain incremental certification is very extensive and costy compared to a "classical" certification approach of the complete computing platform with all application functions. This extra cost may be justified if the applications are done by different, sometimes, competing companies or if various configurations of the IMA systems are planned for certification.

Open Architecture Computing Platform

The benefit of robust partitioning between independent functions but without incremental certification is obtained by an "Open Architecture Computing Platforms" as shown in Fig.1. It decouples the Application SW from the underlying HW- and SW- modules by a well-defined application interface. The robust partition should also ease obsolescence removals which are a main concern on current HW platforms, as modern Microelectronics are available for only a limited time.

With a classical single core processor one of the approved solutions is the implementation of SW layer based on an ARINC653 operating system which should ensure segregation in the time and space domain.

The Sferion Product Family from Airbus Defence and Space as shown in Fig.2 is based on such an open Architecture Computing Platform. It consists of one Processor which provides the computing resources for various applications and dedicated I/O resources which are shared between the applications under the control of the processor. The Platform SW (based on an ARINC653 operating system) ensures the segregation between the different partitions (SW applications) running on the processor.

Challenges for "Open Architecture Computing Platforms"

Open Architecture Computing Platforms implementations have a huge demand on processing power of the underlying HW. This is in fact the limiting factor in current implementations. For further integration more powerful Microprocessors are required. Driven by the consumer market the silicon industry is continuously improving the performance of Microprocessors according to Moores Law (Fig.3).

In the last years the high performance processors are all MultiCore Processors (MCP) which implement several processing cores in one Silicon chip.

The Avionics industry is following the evolution of the Silicon Chips with some years delay. In Fig.4 the evolution from federated Architectures to Open Architecture and to Multi Core based Open Architectures is illustrated.

With respect to Open Architectures the avionics industry is actually facing with two challenges:

- Higher levels of integration as well as the increasing complexity of the individual applications leads to higher demand on computing power.
- Classical Microprocessors with "only" one computing core in the chip are no longer on the roadmaps of the major silicon vendors.

The driver for innovation in the silicon industry is the consumer market, i.e. the demand for communication and connection via mobile devices. The avionics and defence industry are representing only a small portion of the revenues in the silicon industry thus limited or no influence on the characteristic of future silicon devices exists.

Thus no classical (powerful) single core processors will be available for future avionics developments. The Avionics industry has to base the systems on processors which are developed for another market i.e. on Multi Core Processors (MCPs). In principal the implementation of an Open Architecture Computing Platform based on a Multi Core processor looks the same as on a single core processor (Fig.5). From the top level it is even assumed that there is more segregation on the MCP as applications can be split between the two cores.

An implementation of an Open Architecture Computing Platform is only possible if the segregation objectives from system level are broken down to the HW (i.e. the processor). This issue is solved for Single Core Platforms using a dedicated SW layer between HW and application SW which is based on an ARINC653 operating system. This SW layer ensures segregation in the space and time domain. Unfortunately this cannot be easily adapted to Multi-Core Processors, as SW tasks are running in parallel on the different cores, and may access or block shared resources at the same time.

Moreover the MCPs implement additional features to improve performance of the overall MCP system (i.e. coherency fabrics which ensures that cache contend is exchanged between different cores). These acceleration

functions could cause interference between the applications executing simultaneously on the separate cores of an MCP. This interference has actually been observed during testing [2], as shown in Fig.6.

Taken into account, "Microprocessors and systems-on-a-chip (SoC) have become extremely complex, highly integrated, nondeterministic, and densely packaged. As a result, deterministic performance is difficult or impossible to predict in some cases. These devices require additional evaluation methods beyond that identified in current regulatory requirements".

Many of the features implemented in MCPs introduce interference channels between cores. In addition these features have not been designed or verified for compliance with the current airborne software or hardware guidance material. It may therefore be difficult or even impossible to fully characterize and verify all the possible effects of these features. So it is a big risk that such features cause unintended and unexpected behavior. E.g. variations in data access times, denial of access to data or to peripherals This leads to concerns that these features could cause a loss of integrity, a loss of availability or an non-deterministic behavior of hosted applications[4]. If safety-critical applications are hosted on MCPs, the allowable data latency of each input parameter to an application must be analyzed to guarantee that the applications can cope with the worst case variations in data access times. The overall execution times of applications may have to include allowances for such variations.

Current Solutions and Limitations

Certification authorities got aware of this issue and workshops were established between EASA, FAA and Industry (represented by the MultiCore for Avionics Working Group MCFA). As a results of this workshops authorities established guidance material in the form of a generic CRI (EASA) and CAST-32 (Certification Authorities Software Team) paper (FAA). The contend of both is identical. This guidance is addressing topics for Multi-Core Processors with two active cores and software for a single airborne system executing on the MCP.

For such a MCP implementation 16 objectives have to be fulfilled for determinism including configuration setting, errata data, hypervisors, interference channels, shared memory/cache, shared resources and coherency mechanisms. Six objectives are defined for Software including SW plans, Verification plan, applicability of RTCA/DO178C, data and control coupling and robustness testing. Two objectives are defined for error monitoring and handling including safety net and availability.

This guidance will allow Dual Core processors to enter ACs. However, the guidance imposes a lot of limitations to the Avionics industry. First of all the guidance is limited for SW from one AC application only. So IMA architectures are not permitted. The limitation is driven by the fear that the interferences between applications running on different cores could never be entirely mitigated. Thus the functional independence of AC functions cannot be achieved.

Certification authorities in particular have concerns with respect to interference between several applications executing simultaneously on individual cores and non-deterministic behavior caused by shared resources such as coherency fabrics / coherency modules / interconnects that control the data transfers between the MCP cores, memory and the peripheral devices. Therefore the deployment of a safety net is mandatory introducing a means to mitigate unforeseen or undesirable MCP operation by detecting and recovering from anomalous behavior. The safety net approach assumes that a microprocessor will misbehave. An external monitor is an example for a safety net.

This described approach is in line with DOT/FAA/AR-11/5 - Microprocessor Evaluations for Safety-Critical, Real-Time Applications: "Microprocessors and systems-on-a-chip (SoC) have become extremely complex, highly integrated, nondeterministic, and densely packaged. As a result, deterministic performance is difficult or impossible to predict in some cases. These devices require additional evaluation methods beyond that identified in current regulatory requirements".

The authorities' conservative approach caused by the observation that the rapidly changing and emerging COTS market does not take into account requirements from safety critical industries i.e. the avionics industry. The current Sferion Open Architecture Computing Platform is in line with the current guidance from the authorities for Dual Core Processors.

Way Ahead

To overcome the limitations Airbus Defence and Space is involved in research initiatives with respect to novel technical solutions and is actively working with authorities on the evolution of guidance material. An

alternative certification approach has to be developed and the effectiveness needs to be demonstrated in robustness scenarios. To obtain approval, a certification liaison process needs to be established which ensures communication and understanding between the certification authority and the applicant.

Summary

Open Architectures are available from Airbus Defence and Space taking into account current guidance from authorities on the use of Dual Core Processors. The Sferion Product Family is based on such platforms.

For future evolution of Open Architecture Computing Platforms it is key to master Multi Core technology for safety critical applications. Acceptance of Authorities is mandatory to allow the participation of the Avionics industry on the technology push in the field of Microprocessors driven by the consumer market.

References

1. DO297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations.

2. Nowotsch, J. and Paulitsch, M., "Leveraging Multi-Core Computing Architectures in Avionics", 9th European Dependable Computing Conference (EDCC), pp.132-143, 2012, doi:10.1109/EDCC.2012.27.

3. DOT/FAA/AR-11/5 - Microprocessor Evaluations for Safety-Critical, Real-Time Applications.

4. Certification Authorities Software Team (CAST), Position Paper, CAST-32-Multi-core Processors.

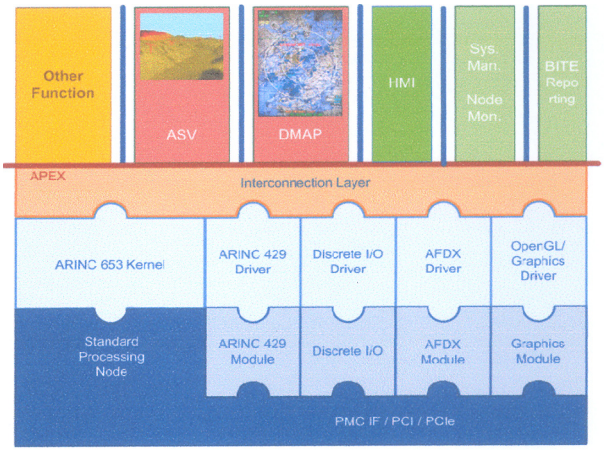

Fig.1 Open Architecture Computing Platform

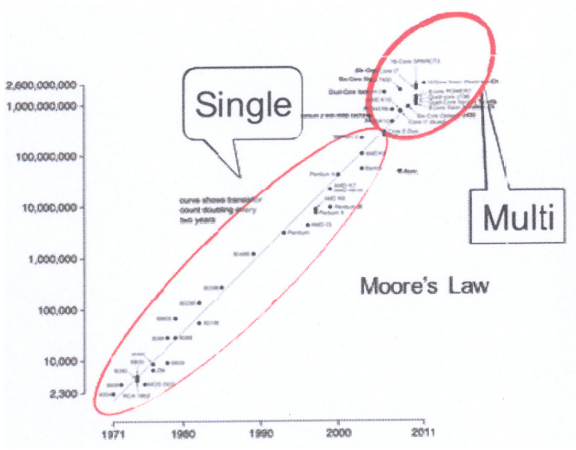

Fig.3 Moore's Law for Silicon Devices (Transistors Over Year)

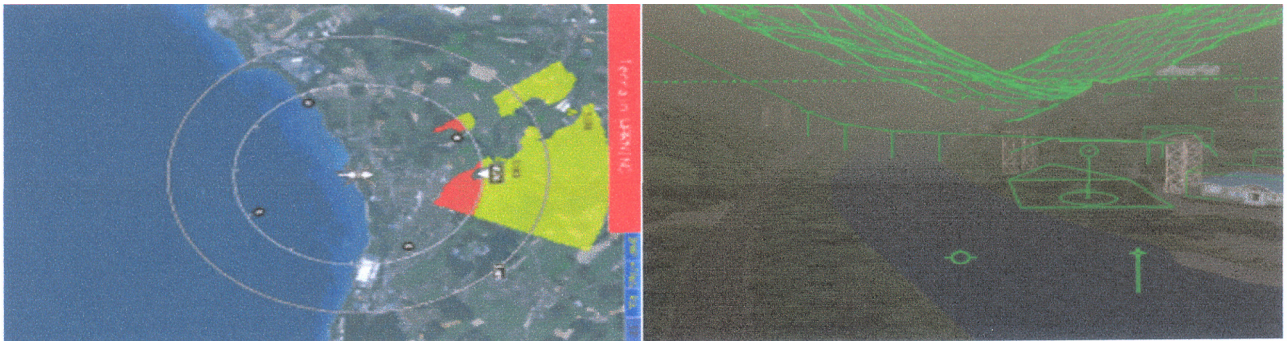

Fig.2 Sferion Product, Digital Map, Helicopter Terrain Awareness Indication and Obstacle Overlay

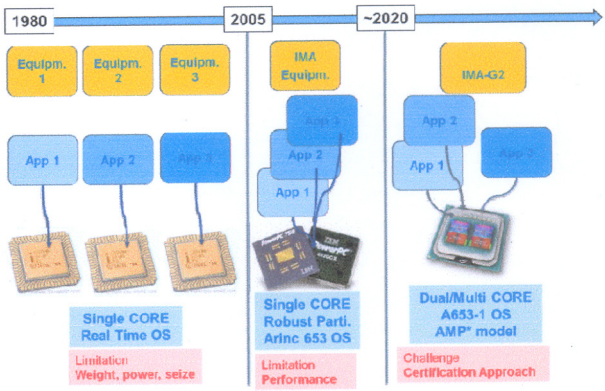

Fig.4 Evolution from Federated Architecture to IMA and Multi Core Based IMS Systems

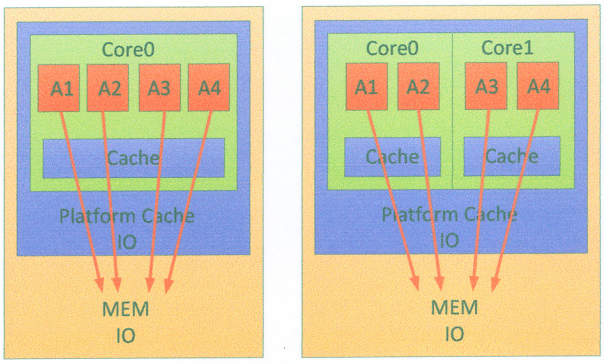

Fig.5 Implementation of AC Applications on a Single Core Platform and on a Multi Core Platform

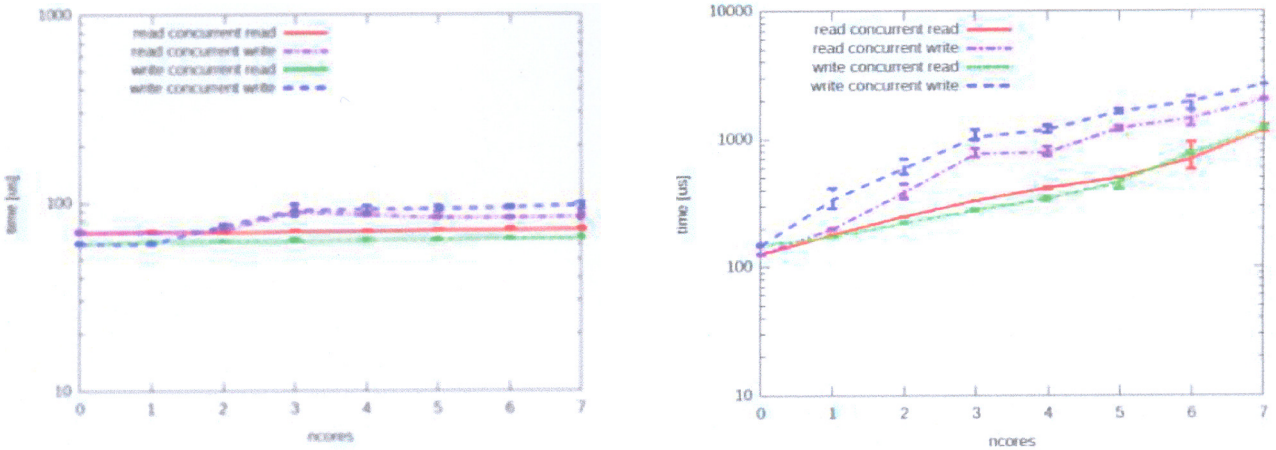

Fig.6 Dependency of Read and Write on Read and Write Accesses from Other Cores for SRAM and DDR3 Memory [Ref.2]