Hot Topic 2: Development and Industrialisation

Presenters:

Michel Riffiod, Future Technologies and Innovation Director, MBDA, France,
Paul Caspi, Directeur de recherche CNRS, Verimag,
Christophe Piala and Jean-Luc Voirin, Avionics Certification, Thales Avionics, France

This second technical session illustrates the methodological dimensions of technology transfer. It elaborates on some methodologies deployed in critical steps of the whole embedded systems development process, particularly to specify safety critical embedded systems, to manage obsolescence of components and to certify the airworthiness of the final solutions.

Paper 1: Management of technologies obsolescence and supplier dependence

Since 30 years, the performances of Aerospace & Defence systems have been dramatically increased using new technologies more and more driven by the civil market which is demanding on large quantities compared to the Aerospace & Defence market size. The very fast evolution in the technologies has been one opportunity to offer to the Aerospace & Defence customer new systems to face also the rapid changes of customers needs.

There are major trends in these systems:

- Systems complexity increases with extended performances & services demands and various technologies have been used to answer these demands
- Customers requires the systems to be more upgradeable rather than to get full new systems, Mid Life Update of the systems are more frequent than full new systems.
- Miniaturization of technologies still offers more performances in smaller volume
- Civil market largely drives the technologies and the Aerospace & Defence industry must use civil technologies with the risk of accelerated obsolescence of technologies
- Defence and Civil Industry have been concentrated due to the worldwide market with high level of competition reducing the number of technologies suppliers.

As a consequence, the obsolescence of technologies as well as the supplier dependence have been increased dramatically during the last past years and they are today two key issues in Aerospace and Defence domain. Automotive, PC and Telecommunication industry has made great efforts to manage supplier dependence and new technologies insertion in their products.

In this context, the question is “How to deal with obsolescence and suppliers dependence in the Aerospace & Defence business?” Technologies obsolescence and suppliers dependence must be continuously managed at each system and sub-system level. The presentation highlights the importance to start the management of obsolescence and supplier dependence at the earlier stage of the development and industrialisation phase.

There are basically two kinds of tasks management to deal with these issues:

- Preventive actions tasks
- Correctives actions tasks

Preventive actions tasks starts early in the selection of new technologies which will be inserted in the future systems and sub-systems. The technologies selection must take into account that life cycle and cost of technologies are depending at first on the market size, secondly on the level of competition between technologies suppliers and thirdly on the technologies roadmap which define the technologies evolution. These non-technical data must be known by the systems designers to operate the selection of new technologies for systems application.

Corrective actions require a continuous assessment of the technologies suppliers’ base by the procurement chain of the systems and sub-systems companies. This survey provides advanced warning on the obsolescence

978-3-9810801-2-4/DATE07 © 2007 EDAA

occurrence and also on the risks of increasing cost due to higher supplier dependence. Actions such as technologies stock or re-design can then take place minimising the cost and time impact on systems deliveries.

Often the systems and sub-systems designers are not enough focused on the issues of obsolescence and suppliers dependence because there are not technical issues. One key recommendation is to inform the designers which have to select new technologies for the systems. For this purpose, there are guidelines to help systems and sub-systems designers as well as technologies buyers for minimizing the issues of obsolescence and suppliers dependence (ie GIFAS "Guide de Management des Obsolescences de Composants Electroniques, Electriques et Electromécaniques").

A second key recommendation is that technologies market survey must be set-up to provide to the designers as well to the procurement chain, all data required to properly manage both issues.

Additionally, a more efficient way to deal with obsolescence and supplier dependence issues is to design systems with open architecture using well-established standard and modular products. The presentation high lights the benefits to select such approach using civil technologies selected by Automotive, Telecom and PC industry.

Paper 2: Model-based Development of Embedded Control Systems

This presentation provides an overview of model-based development for safety-critical embedded systems, mostly from the viewpoint of avionics and space applications.

First, an historical perspective is proposed: safety-critical computing systems appeared in the early eighties, for instance with the "fly-by-wire" system of Airbus A320. Note that "fly-by-wire" is actually a misleading name and that "fly-by-computer" and "fly-by-software" would be better denominations stressing the safety issues raised by these new technologies. It is in this context that Airbus made a decisive and pioneering move toward model-based development by designing the SAO tool (SAO stands for "Computer Aided Specification"): the idea was to consider the models provided by the control departments as formal software specifications and to automatically generate the code out of these specifications. The application of the tool to the A320 fly-by-wire software showed important benefits: earlier and easier debugging, easier modification and maintenance, better communication between control engineers, test pilots, computer engineers, providers and certification authorities.

The present landscape is now that of an improved and well-disseminated technology: the in-house tool SAO has been replaced by the of-the-shelf tool SCADE marketed by Esterel-Technologies. SCADE (Safety-Critical Applications Development Environment) is now used in several safety-critical control industries including avionics and space but also in the control of railways, automobiles, nuclear plants etc. Many benefits were gained by moving from an in-house tool to a commercial one. It has been extended toward the control-modelling field by translators from Simulink and Stateflow (which are de facto standards in control). It comes equipped with formal verification and simulation tools and with enriched code generation capabilities addressing new execution platforms such as multi-threaded and distributed synchronous ones. Moreover the SCADE compiler is qualified for the most severe assurance levels, Do178B level A and IEC 61508 SIL 4. As a result of all these developments, the landscape is now that of a truly industrial approach replacing the "handicraft" one which has long prevailed in the software field. It is not unfair to say that, in that aspect, embedded control is by now one of the most advanced fields of computer engineering and one of the few where such an industrial viewpoint has emerged.

Finally, a look at the future is proposed, with the need for addressing more modelling frameworks (such as UML) and more execution platforms. This raises the question of heterogeneity both in models and in execution, a topic which is becoming a key issue in modern model-based development and which should be the object of significant research efforts.

Paper 3: Assessment Process of Safety-Critical Software for Certification Purpose

The growth of new technologies and high tech products offers new opportunities for the design of highly integrated systems where electronics and software becoming more preponderant, even up to replace conventional solutions. The customer oriented demand, for highly performing and configurable products, constraint safety critical designers to manage with enhanced development methods, open and secure product architecture which is resulting in revision of certification processes, in a aeronautics and civil aviation domain where the context of usage requires the use of rules and constraining standards for system and software engineering.

The presentation focuses on the qualification and certification of software/hardware product in order to help the audience of high tech academics and industrial community to better project their own solutions towards onboard electronics parts for civil aviation.

The presentation starts with the origin of the certification in aeronautics domain and the actual organization put in place to govern an acceptable level of safety all over the airspace. Then, after a description of organizational and operational constraints for an industrial manufacturer, it focuses on the current practices well experienced on software and hardware development, with a description of means of compliance, standardized processes, specific life cycle data and some typical issues to cope with safety critical designs (i.e. reuse of software, highly configurable systems, COTS, ..) .

The main subjects addressed in the lecture are

- Aviation Safety and Certification matter
- International Regulation basis
- Designing Software with DO178B
- Continued Airworthiness and Changes on Certified parts.