SESP 2010

Session:	Session: Model Based Design (03)
Type:	Plenary Session
Date:	Tuesday, September 28, 2010
Time:	10:00 - 11:00
Room:	Newton
Chair:	
Co-chair:	
Remarks:	

Seq	Time	Title	Abs No
1	10:00	Evolving Standardization Supporting Model Based Systems Engineering	

de Koning, HP[1]; Eisenmann, H.[2]; Bandecchi, M.[1]
[1]European Space Agency, NETHERLANDS;
[2]EADS/Astrium Satellites, GERMANY

In this presentation an overview will be given of the standardization that supports the trend towards model based concurrent and collaborative engineering of space systems. Over the last 3 years there have been two complementary initiatives under ECSS (European Cooperation for Space Standardization):

- ECSS E-TM-10-25 "Engineering design model data exchange", and,
- ECSS E-TM-10-23 "Space system data repository".

Both are technical memoranda (TMs) which serve as a means to build and reach consensus within the European space community on the data to be exchanged and the main process aspects to be applied in order to achieve efficient and effective concurrent and collaborative engineering of space systems. They are intended to evolve into a "real standard" in the future.

E-TM-10-25 focusses on the (short term) needs to exchange and share data between concurrent design studies in Phase 0 and Phase A, like in the ESTEC CDF and similar concurrent design centres. The OCDS (Open Concurrent Design Server) environment is the first implementation of this TM. The scope of this TM comprises the definition of the disciplines, (conceptual) architectural decomposition of the system and parameters that define properties / aspects / characteristics of the system under development.

The scope of E-TM-10-23 is mainly to provide a general conceptual data model for the whole space system life cycle. This provide shared semantic At its centre is the systems engineering data (requirements, functional decomposition, architectural / topological decomposition and interfaces, operational modes, etc.) that are common to all disciplines involved in a space project. This TM is being validated and demonstrated in the Virtual Spacecraft Design (VSD) project.

In addition there are related international standards, of which OMG SysML (Systems Modeling Language) is one of the most important. The presentation will show how the standardization efforts are related, what is available today in both document form and as schemas and reference data on the web, as well as as how these assets are intended to be used in the near future to further improve methods, tools and their interoperability.

2 10:30 A Model-Based Approach for Safety Assessment Processes

Bunus, Peter
Linköping University, SWEDEN

With increased system complexity in recent years, almost every system under deployment is exposed to component failures or is under the risk of suffering a major breakdown under its lifetime. The necessity of guarantee the safety of engineering system and the growing importance of lowering the maintenance and repair cost demands for a closer integration of safety assessment tasks in the entire design process and reuse of product related information through all the product development cycle. Existing safety assessment standards offer general guidelines for integration of the safety life cycle into the product life cycle. The safety assessment will generally go through several main stages as functional hazard analyses (FHA), preliminary fault tree analysis (Prelim FTA), common cause analysis (CCA) or failure mode and effect analysis (FMEA) to derive safety requirements before the engineering process takes over to realize the system. While different software tools are used to address these aspects, none of the tools available on the market addresses the whole safety assessment cycle nor can provide a mode-based technology for supporting the assessment process in the avionics and aerospace industry. Moreover there is a lack of integration of software testing and verification techniques into the safety assessment process. Software modules are often tested separately from the hardware modules or at the end of the development cycle when it is extremely hard to change the design of the system. In these modules we will address interoperability issues between various tools and methodologies in different stages of safety assessment process. Model-based engineering and validation approaches must be exploited to efficiently support the design for safety and diagnosability approach and the rigorous assessment of these properties as well as supporting the traceability during the safety assessment process.

In this paper we propose model-based approach of the SAE ARP 4754 "Certification Considerations for Highly-Integrated or Complex Aircraft Systems" in which different simulation techniques for supporting design verification are integrated from very early stage into the safety assessment process. In this context, we show how model-based diagnosis can be employed for system validation and for design of avionics/aerospace systems for improved readiness, maintainability and availability. The basic principle of model-based diagnosis consists in comparing the actual behavior of a system, as it is observed, with the predicted behavior of the system given by a corresponding model. A discrepancy between the observed behavior of the real system and the behavior predicted by the model is a clear indication that a failure is present in the system. Diagnosis is a two-stage process: in the first stage, the error should be detected and located in the model, and in the second stage, an explanation for that error needs to be provided. Diagnoses are usually performed by analyzing the deviations between the nominal (fault free) behavior of the system and the measured or observed behavior of the malfunctioning system. As a general rule, the models are built to enable the identification of failed Line Replaceable Units (LRUs). Once a model of the real system is built, simulation or prediction can be performed on the model. The predicted behavior, which is the result of the simulation, can then be compared with the observed behavior of the real system. This comparison is usually done by a reasoning that is able to detect discrepancies and also to generate and propose corrective actions that need to be performed on the real system to repair the identified fault. We illustrate the application of our approach on a satellite power generation, storage and distribution system test bed (EPS) with real hardware from NASA Ames called ADAPT (Advanced Diagnostics and Prognostics Testbed). We will also show how models developed for diagnosis purposes can be reused for other safety assessment tasks such: failure mode and effect analysis (FMEA), reliability prediction calculations and fault tree analysis.