Dr. Rainer Gerlich

BSSE System and Software Engineering

EaSySim II

Early System Validation:

With Executable Models through the Life Cycle

Dr. Rainer Gerlich

BSSE System and Software Engineering

Early System Validation with EaSySim II©[1]: With Executable Models through the Life Cycle

Introduction

Systems are becoming more and more complex and they include an always increasing amount of hardware and software. Until now the traditional "paper" approach is mostly used at the beginning of a system's development life cycle: specification and design are expressed by documents, reviews are held to conclude on the correctness of the documents and the intended way to implement the system. Rather late in the development cycle the system is becoming "alive" by execution of the software on the hardware.

Usually there is a gap between the conclusions on the documents and the final product because the interaction of system components is so complex that it cannot exactly predicted from paper work what the system will do later on. The later such deviations are identified the higher are the costs, especially if hardware has to be manufactured in parallel to software development.

The idea of the EaSySim II system development approach is to use executable models instead of "paper models" and to allow for continuous checks whether the engineers are doing it right. When executing such models they give the required feedback to the engineers which is needed to tune and to correct specification and design. Such models are established at the beginning of the life cycle and continuously refined towards the final version. The target environment in which they are executed is adapted accordingly.

To take full benefit of the time and cost saving potential of such an approach the right development procedures and tool support need to be provided. What is (known to be) needed has been identified during ESA projects and is now provided by EaSySim II.

Although the EaSySim approach was initiated to improve development of space systems it is a quite general approach which can be and has already been well applied to other application areas such as air traffic control, telecommunication or avionics.

ESA placed the contracts HRDMS, OMBSIM and DDV to establish and evaluate this new approach and supported BSSE to develop EaSySim II.

History

First experience towards a new approach for system validation was collected during the HRDMS project ("Highly Reliable Data Management System and Simulation). Then EaSyVaDe (Early System Validation of Design) was defined in the course of the ESA/ESTEC project OMBSIM (On-Board Management System Behavioural Validation). To allow for practical work the tool environment EaSySim (EaSyVaDe simulation environment) was established. The outcome of OMBSIM was reused for the DDV project (Data Managment System Design Validation). These first exercises already convinced the involved parties (Dornier and Matra Marconi Space) on the benefit of the method and tool. However, some weakness was also detected which motivated BSSE to implement the new version EaSySim II to make the approach and the related tool environment sufficiently mature for industrial use. ESA funded the development of EaSySim II in part.

[1] © The EaSySim II approach is protected by international copyright and treaty provisions. All rights reserved by BSSE. This protection applies to the Δ-approach, the communication and the configuration mechanisms, the mechanisms for access of resources and external components, the means to prevent state explosion and the provided software and guidelines.

The EaSyVaDe Development and Modelling Approach

The EaSyVaDe approach divides the "conventional" life cycle consisting of the activities "specification, design, coding & testing, integration, acceptance" into multiple smaller phases each one comprising specification, design, code generation and validation (Fig. 1). This procedure reflects the hierarchical decomposition of a system and the iterative dependency between specification and design: on each decomposition level a design is an answer to a specification and it imposes requirements on the next lower level. To reduce the risks validation is done for each specification at each level and its refinements to a design. At each such stage code can be generated for execution on the development and the target platform. This allows to coherently approach the final system by continuous refinement over the life cycle as shown by Fig. 2.

The EaSySim II Modelling and Validation Environment

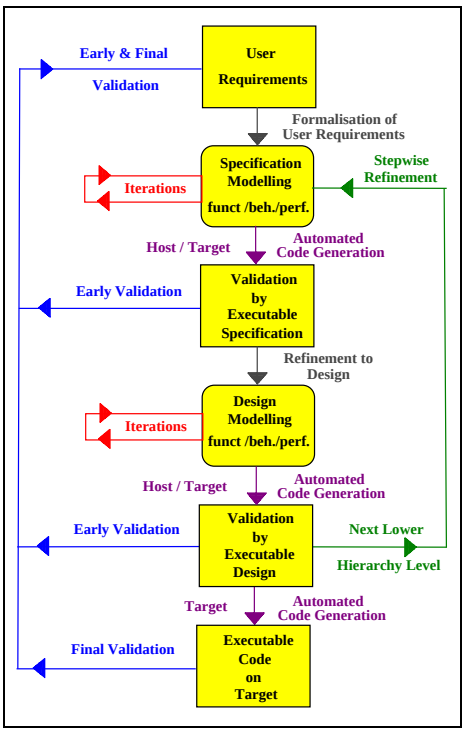


Fig. 1: The EaSyVaDe Approach

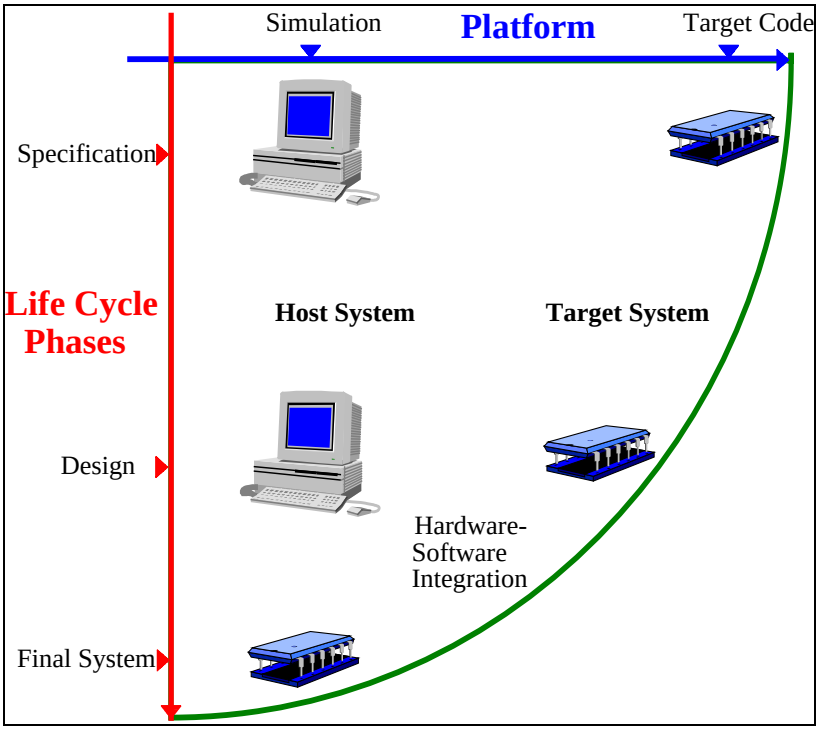


Fig. 2: The 2-Dimensional Life Cycle

The commercial SDL tool ObjectGEODE is the focal point for all modelling activities. By the EaSySim II add-on software the capabilities of ObjectGEODE are enhanced towards support of performance modelling, increased performance of simulation and interfaces to external software.

SDL is a strong typing, easy-to-learn language which introduces a formal description of behaviour by means of Finite StateMachines (FSM). This allows a formal verification of a system's behaviour by simulation techniques.

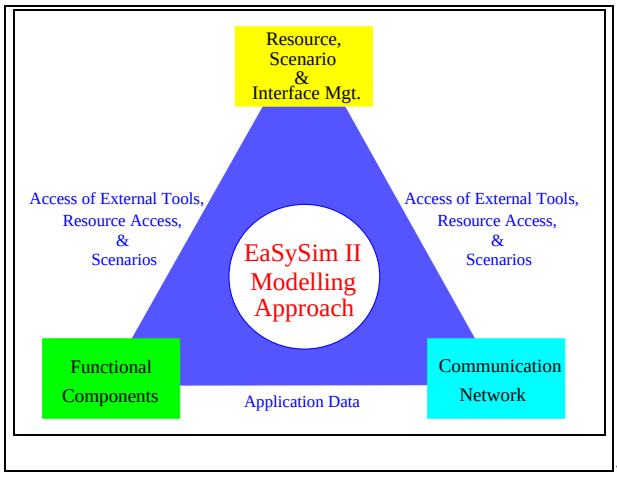


Fig. 3: The EaSySim II Δ-Approach

Support of performance modelling turned out as a major cornerstone for early system validation. Examples exist where a system which is only functionally verified will not run on the target system or vice versa, a design which will tune the final system may be rejected at an early stage due to insufficient consideration of performance.

The high flexibility of modelling is achieved by the so-called **Δ**-approach© shown by Fig. 3. This approach allows to implement access of external software in a transparent manner and to efficiently expand a system, e.g. from specification via design to the final target system. The **Δ**-approach separates the components of a system into two principal classes:

"functional" and "communication" components. The topology which connects all the application components together is defined by data: this allows to re configure the system topology at run-time, a feature which is needed for fault-tolerant systems when recovering from a fault .

This flexibility is explained by the following example given by Fig. 4. It consists of two senders and a receiver which communicate through a network of four buses.

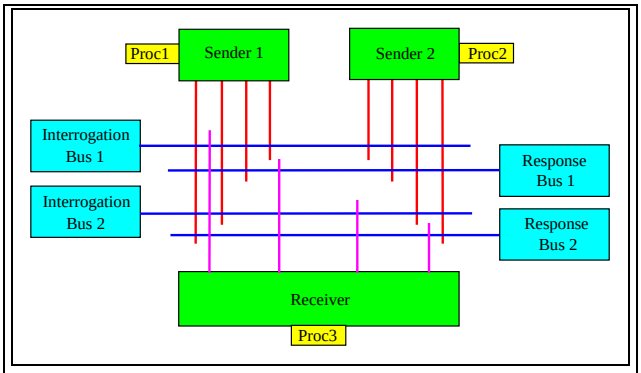


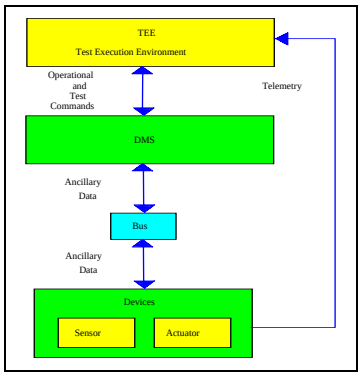
Fig. 4: A Sample Application for Flexible Change of Topology

A lot of combinations for data exchange are possible, each may have advantages and disadvantages. Now, EaSySim II allows (1) to change the communication topology and to investigate its impact on overall performance, (2) to change the time consumption of processes on the processors and more properties. And one can apply exhaustive simulation to all these different (performance) configurations easily.

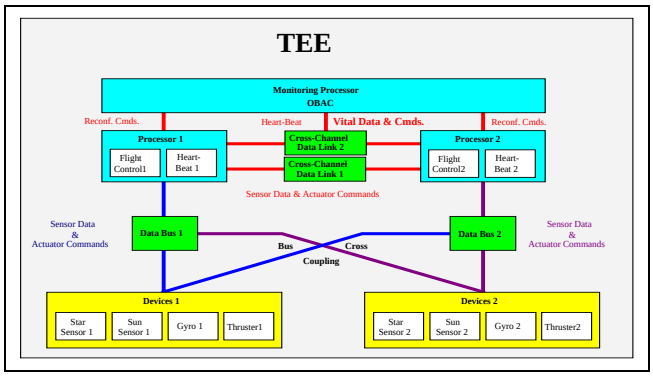
The evaluation of different architectures and performances is possible without re compilation of the SDL source code.

A sample Data Management System is shown by Fig. 5. It is a typical fault-tolerant system with one redundant set of components: processor, bus and peripheral devices.

This example was selected for demonstration of the capability to smoothly derive the final system from the specification (prototype). Only components had to be added to the specification model, but none of the existing components had to changed, except for refinement and extension of its functionality.



Specification Model: Logical View



Design Model: Architectural View

Fig. 5: From Specification to Design by Coherent Refinement

Conclusion

The EaSyVaDe development and validation approach and EaSySim II has now been applied to a number of applications in the area of space, air traffic control and telecommunication. It could be confirmed that EaSySim II satisfies (so far) the needs for efficient modelling and validation. By reuse of provided templates it was possible to get a prototype of the full data flow running within two days for a telecomunication project. The specification and design prototypes for above on-board data management system could be established and validated within two weeks. This covers simulation and code generation. These results prove the efficiency of the modeling approach and of the EaSySim II environment and disprove that it is expensive to apply formal techniques. Future activities are needed to incorporate this approach into the overall project development and management approach and to integrate it with other existing development and project managment tools.