Integrated Embedded System Development for Automotive and Aerospace Applications: The DECOS Concepts

András Balogh, György Csertán, András Pataricza, Balázs Polgár
Budapest University of Technology and Economics

Wolfgang Herzner, Rupert Schlick, Egbert Althammer, Erwin Schoitsch
Austrian Research Centers GmbH - ARC

Martin Schlager, Bernhard Leiner
TTTech Computertechnik AG

Bernhard Huber
Vienna University of Technology

Alain Le Guennec, Thierry Le Sergent, Bruno Martin
Esterel Technologies

Neeraj Suri, Shariful Islam
Darmstadt University of Technology

Jonny Vinter
SP Technical Research Institute of Sweden

Today, the development of embedded - and in particular safety-critical – systems in general follows a customized design approach, resulting in rather isolated applications and little reuse of components and code across different application domains. For instance, in modern cars sub-systems like power-train control, advanced driver assistance systems or the body electronic co-exist, each equipped with its own electronic hardware, communication cabling etc. This approach implies at least increased hardware costs, weight, and power consumption, last not least due to severely hampering the sharing of resources like sensors among the different sub-systems.

Therefore, the European project DECOS [1] aims at developing basic enabling technology for moving from federated to integrated distributed architectures [2] in order to reduce development, validation and maintenance costs, and increase the dependability of embedded applications in various application domains. 'Integrated' means, that several software 'IP'-blocks (Intellectual Property) of different criticality can be allocated to one node (ECU – Electronic Control Unit) without interfering with each other, ie, guaranteed encapsulation in space (memory) and time (each job has its reserved time slot). DECOS presumes the existence of a core architecture providing the core services: deterministic and timely message transport; fault tolerant clock synchronization; strong fault isolation; consistent diagnosis of failing nodes.
Any core architecture providing these services (eg TTP/C [3], FlexRay [4], or Time-Triggered Ethernet [5]) can be a basis for DECOS-based systems. On top of these core services, DECOS provides a set of architectural (or high-level) services: virtual networks (VN) and gateways; an encapsulated execution environment (EEE); diagnostics.
To minimize the dependency of application programming on a certain DECOS implementation, a Platform Interface layer (PIL) provides a techology invariant interface of the high level services for application tasks.

The DECOS Tool-Chain

A constituent element of such an enabling technology is a tool-chain, currently being developed by DECOS, which encompasses all embedded software design and development aspects, including configuration and testing. As illustrated in the figure, the DECOS tool chain essentially consists of three vertical 'lanes': on the left side, the integrated system configuration is determined and middleware is generated, in the middle the application functionality is developed and on the right side tools for testing and verifying the various (intermediate) results is shown.

The specification starts with the Platform Independent Models (PIMs) of the application sub-systems, defining their requirements with respect to communication (among the application tasks), performance, and dependability.
PIMs serve two purposes: firstly, together with the specification of the target cluster hardware and resources, the Cluster Resource Description (CRD), they are used to derive the Platform Specific Model (PSM), which contains allocation (of tasks to nodes) and other information relevant for the successive steps. Secondly, PIMs are used to guide the development of jobs (ie application tasks), by modelling their behavior with SCADE (a tool set of Esterel Technologies). If feasible, predefined Simulink models or modules written in conventional languages like C or Ada can be imported. After application

code is generated from these models, the results of both activities are integrated to achieve the target executables, which can then be downloaded to the application cluster.

The purpose of the CRD is to capture the characteristics of the platform relevant for the software-hardware integration. This includes computational resources (CPU, memory), communication resources and dependability properties. Before generating the PSM, it is possible to add information manually to the PIM (PIM marking), for example information on specific middleware requirements. Jobs are assigned to nodes taking into account functional and non-functional constraints using a multi-variable optimization approach [6].

Scheduling is the next step, which results in the schedule of communication and the EEE. Then, PIL is generated, providing generic message transfer, global time service and membership service (necessary to distribute information on the state of nodes). For behavior modeling, SCADE [7] (by Esterel Technologies) - based on a formally-defined data flow notation - has been chosen as a primary tool for DECOS. Existing Simulink [8] models can also be imported to SCADE.

In parallel with the design and development of the system, verification and validation activities also take place, with some focus on certification support. As shown to the right of attached figure, the DECOS Generic Test Bench offers a workflow-based automation of activities [9] integrating various industrial and academic tools that together form the toolbox of V&V activities. Besides the existing tools several interesting new techniques are introduced like checking correct use of physical units and scales in functional models [10], and ontology-based verification of models [11]. The Test Bench allows to test, verify, and prepare for certification all artifacts related to DECOS and its addressed technologies: tools and services as well as applications or their components.

The DECOS tool-chain comprises a wide variety of tools from model to deployment. To ease handling, a transformation tool VIATRA [12], developed at Budapest University of Technology and Economics, is used for convenient PIM specification by means of domain-specific editors, as well as backbone for model transformations (from PIM to PSM) and middleware generation. Four tools are used for the DECOS tool-chain: GME [13], VIATRA, SCADE and TTplan/build [14]; additionally, commercial and target-platform specific tools are used for deployment (compilation, linking, download). This tool-chain is designed for efficient configuration, development and validation of critical 'smart' embedded applications.

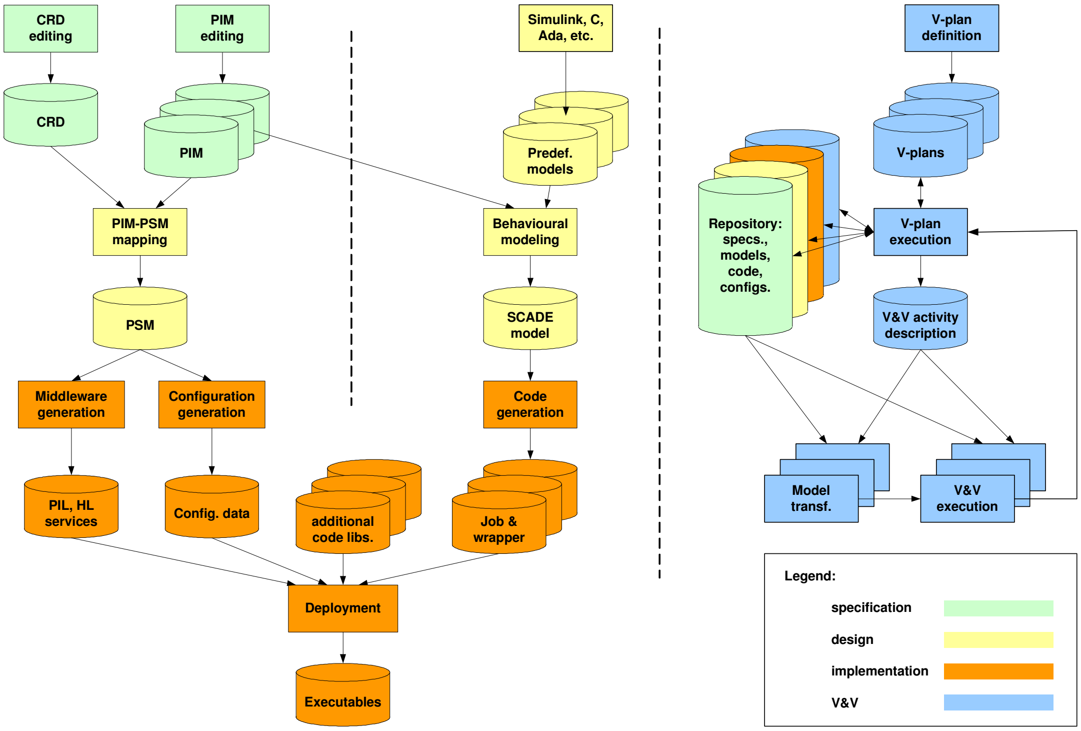
References

[1] DECOS EU FW6 IP. http://www.decos.at/

[2] H. Kopetz, R. Obermaisser, P. Peti, and N. Suri. *From a federated to an integrated architecture for dependable embedded real-time systems*. Technical Report 22, Technische Universitat Wien, Institut für Technische Informatik, Treitlstr. 1-3/182-1, 1040 Vienna, Austria, 2004.

[3] TTP/C Protocol http://www.vmars.tuwien.ac.at/projects/ttp/ttpc.html

[4] Flexray Consortium, http://www.flexray.com/



[5] H. Kopetz, A. Ademaj, P. Grillinger, K. Steinhammer. *The Time-triggered Ethernet (TTE) Design*, In Proc of 8th IEEE International Symposium on Object-oriented Real-time distributed Computing (ISORC), Seattle, Washington, 2005.

[6] S. Islam, Gy. Csertán and W. Herzner. *Multi Variable Optimization Approach for SW-HW Integration*, IEEE High Assurance Systems Engineering Conference (HASE2005), Heidelberg, Germany, 13-14 October 2005 (Fast Abstract).

[7] SCADE Suite. http://www.esterel-technologies.com/products/scade-suite/

[8] Mathworks. Matlab/Simulink tool. http://www.mathworks.com/

[9] E. Schoitsch, E. Althammer, H. Eriksson, J. Vinter, L. Gönczy, A. Pataricza, and Gy. Csertán. *Validation and certification of safety-critical embedded systems - the DECOS test bench.* In Proceedings of The 25th International Conference on Computer Safety, Security and Reliability (SAFECOMP2006), Lecture Notes in Computer Science, Gdansk, POLAND, September 25-29 2006. Springer

[10] Schlick, W.Herzner, T.Le Sergent. *Checking SCADE Models for Correct Usage of Physical Units*, In Proc of The 25th International Conference on Computer Safety, Security and Reliability (SAFECOMP2006), Lecture Notes in Computer Science, Gdansk, POLAND, September 25-29 2006. Springer

[11] A. Pataricza, B. Polgár, Sz. Gyapay, A. Balogh, Gy. Csertán. *Formal checking of metamodels and models* In Proc. of the DECOS/ERCIM Workshop on SAFECOMP 2006.

[12] VIATRA2 An Eclipse GMT Subproject http://www.eclipse.org/gmt

[13] Generic Modeling Anvironment (GME). http://www.isis.vanderbilt.edu/projects/gme/

[14] TTTech AG., TT Tools Suite. http://www.tttech.com/