Budapest University of Technology and Economics
Department of Measurement and Information Systems
Fault Tolerant Systems Research Group

Model Transformation-based Design of Dependable Systems

Abstract of the PhD Thesis

András Balogh
MSc in Technical Informatics

Supervisor: Prof. András Pataricza, DSc.
Tutor: Dániel Varró, PhD.

Budapest 2009

1 Preliminaries and Objectives of the Research

The main trends in embedded systems development for the past decade were the increasing complexity, and shortening life-cycle of systems, demanding a novel, more *effective development approach* that supports the management of system *complexity*, *non-functional aspects*, increases the sytem development *productivity*, and is compatible with the existing domain-specific standards by supporting *system certification* for safety critical applications.

A dominant trend in the systems development evolution is *modeling*, the definition of applications, platforms, and systems by high-level (and often visual) *modeling languages* that provide an intuitive yet precise representation formalism. UML (Unified Modeling Language) [Grom] is the most widely used language, although its limitations on specialization and the lack of formal semantics hinder its usage in several domains. Different domain-specific languages have also been evolved to support the specific requirements of separate application domains. The Object Management Group (OMG) [Gron] issued the Model-driven Architecture (MDA) [Grof] initiative in order to provide the model-based development projects with a common process. The MDA process separates the functional application development from the platform modeling, and application-platform integration. The later step is treated as atomic, automatic mapping between the two aspect models.

Although modeling is a key step of embedded systems design, the MDA approach could not gain significant importance as the typical embedded platform complexity, and the different non-functional or quality aspects involved in the development do not allow the automation of application-platform mappings. As a consequence, models are not properly integrated into the design flow and are often only used for documentation and (partial) simulation purposes while the final implementation of the system is the result of a separate, manual development process.

The objective of my research was to adapt and extend the traditional MDA approach in order to be able to support the development of dependable embedded systems, and to incorporate non-functional aspects during systems development. The work also included basic research on model-driven tools and technologies in order to further extend the usability and effectiveness of model management and transformation

tools that are to be used during model-driven systems development. More specifically, the following objectives have to be fulfilled:

- **Objective 1** *Improve the productivity* of systems development by introducing interactive, semi-automated tools and methods in different phases of the development process.
- **Objective 2** *Reduce cognitive complexity* of system designs by separating the architecture and behaviour of applications from the details of the implementation platform (as facilitated by the principles of Model-driven Architecture approach).
- **Objective 3** *Improve the quality* of system designs by the introduction of different consistency checks, analysis, and synthesis methods.
- **Objective 4** *Define a model-driven hardware-software integration methodology* that is capable of handling complex target architectures and several non-functional aspects like timeliness, dependability, and cost.
- **Objective 5** *Provide advanced language constructs* that support the reusability of model transformations.
- **Objective 6** *Provide support for the executable specification of design patterns* that allow the integration of best practices and common solution patterns into domain-specific modeling environments.
- **Objective 7** Provide support for the *integration of different metamodeling* environments using a precise semantical foundation.

2 Research method

The research objectives basically determined the main line of my research and the individual subtasks to be solved.

Supporting techniques for model-driven development. Initially, I investigated the metamodeling and model transformations frameworks, especially the VPM [VP03] model management framework and the VIATRA2 [Var04] model transformation tool. VPM and VIATRA2 are based on a precise foundation and can serve as a formal modeling and transformation environment for domain-specific languages, thus they are used for the specification of metamodels and transformation throughout the thesis.

I have also investigated the main domain-specific languages used in the embedded systems domain, and found that most of these are defined and implemented using the ECore [Foua] metamodeling environment that is a derivative of the standard MOF (Meta Object Facility) [Groe] framework.

In order to support the modeling languages based on MOF and ECore, I defined a mapping between these environments and VPM, moreover I defined a formal, operational semantics for ECore using the graph transformation (GT) [EEKR99] and the abstract state machine (ASM) [BS03a] formalisms.

I have also identified several improvement possibilities regarding the transformation language (GT-ASM) of VIATRA2 and defined advanced graph transformation language constructs that support the reusability and effective development, testing, and execution of transformation programs and components (Thesis 1).

The aims of my work were a) to extend the applicability of the model transformation tools and methods to complex transformations, b) to improve the productivity of model transformation development by novel reusability concepts.

Extending the Model-driven Architecture I investigated the MDA approach and compared it to the typical design processes in the embedded systems area. This work has been done in the framework of the European IST Framework 6 IP DECOS (Dependable Components and Systems) [DEC] and resulted in the concept of *iterative, interactive* application-platform (or hardware-software) integration.

The iterative, interactive mapping concept has been developed in the DECOS project, with a prototype proof-of-concept tool that implemented the basic results of the research work. The mapping concept has been further investigated and generalized in order to be adaptable for different application domains and development processes.

The new mapping framework required the modeling of non-functional aspects of systems, therefore I proposed modeling notation for application architectures and platforms that are integrated with a uniform non-functional properties modeling language that is part of the upcoming standard MARTE (Modeling and Analysis of Real-time Embedded Systems) UML profile [Grok]. The proposed modeling notations are defined using the formal VPM approach and can be treated as an abstraction of most of the domain-specific languages in the embedded systems area assuring the portability of the methods and techniques defined in the thesis to these specific languages.

The introduction of complex, interactive mapping into the MDA process also required the development of *on-line, early consistency checking* methods that enable the rapid evaluation of potentially incomplete system models and provide feedback to the system designer on the potential design problems. I investigated the existing solutions and complemented the mapping framework with an open, extensible constraints checking solution (Thesis 2).

Model-based analysis and synthesis methods The iterative, interactive hardware-software integration method included several steps that perform complex operations (for example allocation of software components to hardware resources). The state-of-the art solutions either require manual interaction in these stages, or use heuristic algorithms to carry out these tasks automatically.

I proposed a new, high-level availability analysis method that enables the prediction of system availability on the platform-independent and on the platform-specific (allocated) system model levels. On one hand, this method can be used to validate the current system model against availability requirements, on the other hand it can be a basis for availability-driven (or more generally, dependability-driven) allocation.

Software to hardware allocation is a key step of the mapping process that is mostly done manually today (e.g. based on previous project experiences and best practices), resulting in a relatively low utilization of

computing resources. The allocation can be optimized at two levels: a) finding optimal platform architecture for the application, and b) optimizing the allocation itself. In order to support the platform architecture synthesis, I developed a cost and dependability driven architecture optimization method that is able to generate the high level architecture of a distributed system fulfilling dependability and performance related requirements in a cost-optimal way.

In time-triggered (synchronous) systems – often used for safety critical applications in different domains – the scheduling of network communication, and operating system tasks on the nodes is done statically at design time. The current design processes separate the allocation and scheduling phases (often also splitting communication and operating system scheduling) that results in an in-optimal solution from the performance and resource utilization point of view. Our experience has also shown that there may be allocation problems that (although the allocation itself is valid) can result in a failure in the scheduling phase. In such case, the designer has to manually change the allocation in order to get a valid schedule. As all of these processes are complex, the designer has to have a deep understanding of all the involved technologies, heuristics, and algorithms to be able to overcome the design problems.

I developed a single, integrated, optimization based solution for the allocation and scheduling of time-triggered systems that helps to overcome the problem of spited algorithms and tools. Furthermore, instead of getting a single feasible solution, the designer is able to combine several different objectives in order to synthesise the optimal allocation and scheduling for the actual system design (Thesis 3).

3 New Scientific Results

3.1 Tool Integration and Tool Generation

When investigating the current model transformation environments, I found that there are areas where the productivity of the transformation development could be improved. Moreover, by integrating different metamodeling approaches based on a solid formal foundation, the migration, verification and validation, and testing of transformations and tools will be feasible.

Thesis 1 *I have developed novel constructs for the composition of graph transformations on different levels.*

In particular, the following novel procedures were elaborated:

1.1 *I defined composition mechanisms on graph pattern and transformation rule level that extend the traditional graph transformation approach and reduce the complexity of transformation specifications. [2, 7, 8, 10]*

1.2 *I have developed a mechanism for the transformation-level compostion of graph transformations in order to achieve better runtime performance and to allow the reuse of transformations. [9]*

1.3 *I defined a formal, executable operational semantics for the ECore metamodeling environment. [2, 7, 9]*

The thesis is based on Chapter 3 of the PhD dissertation.

It is worth emphasizing that although the topic of the dissertation is focusing on the development of dependable embedded systems, the results of this thesis can directly be utilized in all model-driven development domains.

3.2 Model-driven Development with Quality Aspects

I investigated the traditional MDA approach and found that its simplified, atomic application-platform mapping solution cannot be utilized in complex domains like the domain of dependable embedded systems, as it lacks abilities like a) support for non-functional aspects, b) user interaction, c) integrated consistency checking and verification-validation.

Thesis 2 *I have developed a novel approach for model-driven development of distributed, dependable embedded systems.*

In particular, the following novel procedures were elaborated:

2.1 *I proposed a domain-specific architectural, platform, and system modeling style based on the combination of current modeling standards that follows strong component orientation and supports functional and non-functional property definition. [14, 19–21]*

2.2 *I extended the traditional MDA approach with an iterative, interactive hardware-software integration framework that is capable of handling complex system architectures and models. [3, 4, 13, 14, 19, 21]*

2.3 *I defined a static constraints checking framework that is integrated with the hardware-software design process in order to give early feedback on design errors to the developer. [3, 11, 17, 18, 21]*

The thesis is based on Chapter 5 of the PhD dissertation.

3.3 Dependability-driven Synthesis

One of the key steps in application to platform integration is the allocation of software components to execution units. I proposed novel methods that work on model-level, can be integrated in a model-driven development process, and automate the allocation, communication and network scheduling, and architecture synthesis steps based on mathematical optimization techniques.

Thesis 3 *I have defined analysis and synthesis methods supporting the model-based development of embedded real-time dependable systems.*

In particular, the following novel procedures were elaborated:

3.1 *I have defined a high-level availability analysis method that estimates the availability properties of the system under design at early stages of the development process. [4, 5]*

3.2 *I have developed a cost-driven method for the high level platform architecture optimization in distributed systems based on the required performance and availability attributes. [1, 6]*

3.3 *I have developed a multi aspect optimization-based approach for the allocation and scheduling of distributed embedded time-triggered systems. [3, 15, 18]*

The thesis is based on Chapter 6 of the PhD dissertation.

4 Utilization of New Scientific Results

In order to demonstrate the practical, industrial relevance of the basic concepts and methods worked out in the current thesis, we (where "we" also refers to several students working on their MSc or PhD thesis, and also my colleagues at OptXware Research and Development Ltd.) developed several tools supporting the model-driven development of embedded systems.

The Viatra2 model transformation framework. The current version of VIATRA2 includes all graph-transformation related constructs that have been discussed in Chapter 3 of the dissertation and has been successfully used in a number of international research projects.

The results related to ECore semantics definition and metamodel integration form the basis of a new tool component, called *Viatra-EMF* that enables the runtime integration between the two environments and will be part of the official VIATRA2 release. This technology will be utilized in several industrial projects at OptXware.

Iterative, interactive hardware-software integration The first prototype of the iterative, interactive hardware-software integration framework (relying on the results of Chapter 5 of the dissertation) has been developed in the DECOS [DEC] project. The results have also been used in the DIANA [DIA] project, and its application is foreseen in the upcoming INDEXYS [Conc] project where we aim at the development of critical embedded systems ranging from single-chip to large systems including several dozens of powerful computing nodes.

Allocation and schedule synthesis The allocation and scheduling methods discussed in Chapter 6 of the dissertation have been utilized in several projects. In DECOS, the scheduling algorithm has been tested using different time-triggered network protocols for aerospace and automotive systems.

There is an ongoing industrial project where the scheduling algorithm is adapted to the AutoSAR [Alla] environment and is used for the scheduling of time-triggered FlexRay [Con05] networks.

Ongoing development and future work An ongoing activity targets the development of a model-based tool chain for the INDEXYS

[Conc] project that will incorporate the results of the previous work and will be a new generation of model-driven tools for embedded systems. The integration between model-transformation based tool components, formal analysis and synthesis tools, and verification-validation solutions will be more tight and customizable. The tool development focuses also on creating a team-aware environment that enables the collaborative development of systems by real-time sharing of development artifacts (models, documents, source code, etc.).

Further activities aim at the development of scheduling tools for different communication protocols based on the generic solution described in the dissertation. Some target domains feature inherent hierarchy in the communication that will be utilized in order to achieve more efficient solutions. A second aspect of scheduling tool development is the support for multi-network scheduling with a global optimum criteria where the existing single-cluster approach should be extended.

5 Publications in Subject of the Dissertation

Book part

[1] András Balogh, László Gönczy, and András Pataricza. *Verification and Validation of Nonfunctional Aspects in Enterprise Modeling*, chapter 12, pages 257–298. Idea Group Publishing, 2006.

Journal papers

[2] András Balogh and Dániel Varró. The model transformation language of the VIATRA2 framework. *Science of Programming*, 68(3):187–207, October 2007.

[3] Shariful Islam, Neeraj Suri, András Pataricza András Balogh, and György Csertán. An optimization based design for integrated dependable real-time embedded systems. *Design Automation for Embedded Systems*, 2009. In press.

International conference and workshop papers

[4] Michalis Anastasopoulos and András Balogh. Model-driven development of particle system families. In *Proc. of the 4th International Workshop on Model-Based Methodologies for Pervasive and Embedded Software. (MOMPES 2007)*, pages 102–114. IEEE Computer Society, 2007.

[5] András Balogh and András Pataricza. Quality-of-service analysis of dependable application models. In *5th International Workshop on Critical Systems Development Using Modeling Languages (CSDUML 2006)*, pages 1–12, 2006.

[6] András Balogh, András Pataricza, and Dániel Varró. Model-driven optimization of enterprise application and service deployment. In *Proc. Of the 2nd International Service Availability Symposium (ISAS 2005)*, pages 84–98, 2005.

[7] András Balogh and Dániel Varró. Advanced model transformation language constructs in the VIATRA2 framework. In *ACM Symposium on Applied Computing*, pages 1280–1287, 2006.

[8] András Balogh and Dániel Varró. Pattern composition in graph transformation rules. In *(First) European Workshop on Composition of Model Transformations*, pages 33–38, 2006.

[9] András Balogh, Gergely Varró, Dániel Varró, and András Pataricza. Compiling model transformations to EJB3-specific transformer plugins. In *ACM Symposium on Applied Computing*, pages 1288–1295, 2006.

[10] Wolfgang Herzner, András Balogh, and György Csertán. Design patterns for domain-specific application modeling. In *Proc. of the DECOS/ERCIM Workshop on EUROMICRO 2006.*, Dubrovnik, Croatia, August 2006.

[11] Wolfgang Herzner, Berhard Hubert, András Balogh, and György Csertán. The DECOS tool-chain: Model-based development of distibuted embedded safety-critical real-time systems. In *Proc. of the DECOS/ERCIM Workshop on SAFECOMP 2006.*, Gdansk, Poland, September 2006.

[12] Wolfgang Herzner, Marting Schlager, Thierry Le Sergent, Berhard Huber, Md. Shariful Islam, Neeraj Suri, and András Balogh. From model-based design to deployment of integrated, embedded, real-time systems: The DECOS tool-chain. In *Informationstagung Mikroelektronik ME 2006 Workshop*, volume 43, ISBN: 3-85133-040-4, pages 204–213. Austrian Electrotechnical Association, 2006.

[13] Wolfgang Herzner, Rupert Schlick, Bernhard Leiner Martin Schlager, András Balogh, György Csertán, Alain Le Guennec, Thierry Le Sergent, Neeraj Suri, Shariful Islam, and Bernhard Huber. Model-based development of distributed embedded real-time systems with the decos tool-chain. In *SAE 2007 AeroTech Congress Exhibition*, 2007.

[14] Md. Shariful Islam, György Csertán, András Balogh, Wolfgang Herzner, Thierry Le Sergent, András Pataricza, and Neeraj Suri. A sw-hw integration process for the generation of platform specific models. In *Informationstagung Mikroelektronik ME 2006 Workshop*, volume 43, ISBN: 3-85133-040-4, pages 194–203. Austrian Electrotechnical Association, 2006.

[15] András Patarcza, András Balogh, and Judit Rácz. Scheduling of embedded time-triggered systems. In *2nd Workshop on Engineering Fault-Tolerant Systems*, pages 44–49. ACM Digital Library, 2007.

[16] András Pataricza, András Balogh, and István Ráth. Automated verification and validation of domain specific languages and their applications. In *Proc. of 4th World Congress on Software Quality*, Sept. 15-18 2008.

Local conference and workshop papers

[17] András Balogh. Verification of harware-software integration processes. In *Proceedings of the 14th PhD Mini-Symposium*, pages 58–61, 2007.

[18] András Balogh, András Patarcza, György Csertán, and Balázs Polgár. Model-based analysis and synthesis methods for dependable embedded systems. In *Regional Conference on Embedded and Ambient Systems RCEAS 2007*, pages 123–130. ISBN: 978-963-8431-98-1, November 2007.

[19] András Balogh, András Patarcza, Gergely Pintér, Michalis Anastasopoulos Áron Sisak, and Jaejon Lee. Model-driven specification, analysis, and realization of assisted living systems. In *Regional Conference on Embedded and Ambient Systems RCEAS 2007*, pages 123–130. ISBN: 978-963-8431-98-1, November 2007.

Invited talks, technical reports

[20] András Balogh, György Csertán, Orsolya Dobán, István Majzik, András Pataricza, Dániel Varró, Szilvia Varró-Gyapay, Md. Shariful Islam, and Georg Weissenbacher. Design methodology and specification model. Technical report, Budapest University of Technology and Economics, 2005.

[21] Eila Ovaska, András Balogh, Sergio Campos, A. Noguero, András Pataricza, Kari Tiensyrja, and J. Vicedo. Model and quality driven embedded systems engineering. Technical report, VTT Technical Research Centre of Finland, ISBN: 978-951-38-7336-3, 2009.

[22] András Pataricza, Balázs Polgár, Szilvia Varró-Gyapay, András Balogh, and György Csertán. Formal checking of metamodels and models. Invited talk at DECOS/ERCIM workshop on SAFECOMP 2006, Gdansk,Poland, September 2006.

6 References

[Alla] AUTOSAR Alliance. The official AUTOSAR site. `http://www.autosar.org/`.

[BS03a] Egon Börger and Robert Stärk. *Abstract State Machines. A method for High-Level System Design and Analysis*. Springer-Verlag, 2003.

[Conc] INDEXYS Consortium. Distributed, equipment independent environment for advanced avionic applications. `http://indexys.eu/`.

[Con05] FlexRay Consortium. FlexRay communications system protocol specification version 2.1, 2005.

[DEC] DECOS. Dependable components and systems. an eu framework 6 integrated project. `http://www.decos.at/`.

[DIA] DIANA. Industrial exploitation of the genesys cross-domain architecture. `http://www.dianaproject.com/`.

[EEKR99] Hartmut Ehrig, Gregor Engels, Hans-Jörg Kreowski, and Grzegorz Rozenberg, editors. *Handbook on Graph Grammars and Computing by Graph Transformation*, volume 2: Applications, Languages and Tools. World Scientific, 1999.

[Foua] Eclipse Foundation. Eclipse Modeling Framework Homepage. `http://www.eclipse.org/emf`.

[Groe] The Object Management Group. Meta object facilty (mof) core specification version 2.0. `http://www.omg.org/docs/formal/06-01-01.pdf`.

[Grof] The Object Management Group. Model-driven architecture information portal. http://www.omg.org/mda.

[Grok] The Object Management Group. Uml profile for modeling and analysis of real-time and embedded systems (marte). http://www.omg.org/docs/ptc/08-06-08.pdf.

[Grom] The Object Management Group. Unified Modeling Language 2.0. http://www.omg.org/technology/documents/formal/uml.htm.

[Gron] The Object Management Group. Website. http://www.omg.org/.

[Var04] Dániel Varró. *Automated Model Transformations for the Analysis of IT Systems*. PhD thesis, Budapest University of Technology and Economics, Department of Measurement and Information Systems, May 2004.

[VP03] Dániel Varró and András Pataricza. VPM: A visual, precise and multilevel metamodeling framework for describing mathematical domains and UML. *Journal of Software and Systems Modeling*, 2(3):187–210, October 2003.