A Framework for the Improvement of Dependability of Self-Optimizing Systems

R. Dorociak*, T. Gaukstern, J. Gausemeier and P. Iwanek

Heinz Nixdorf Institute, University of Paderborn, Germany
*E-Mail: rafal.dorociak@hni.uni-paderborn.de

Summary: The conceivable development of communication and information technology opens up fascinating perspectives, which move far beyond current standards of mechatronics: mechatronic systems having inherent partial intelligence – the so-called self-optimizing systems. The design of dependable self-optimizing systems is challenging. On the one hand, it is challenging due to complexity of such systems and their non-deterministic behavior. On the other hand, self-optimization can be used to increase the dependability of the system during its operation. However, it has to be ensured, that the self-optimization works dependable itself. In order to accomplish this, suitable dependability methods have to be used. In this contribution a framework for the improvement of dependability of self-optimizing systems is introduced. It supports the developers by selection and planning of dependability methods, which are suitable for their particular development task.

Keywords: Reliability, Safety, Design Method, Mechatronic.

1. Introduction

The rapid development of communication and information technology opens up fascinating perspectives, which go far beyond the state of the art in mechatronics: mechatronic systems with inherent partial intelligence. These so called self-optimizing (s.o.) systems adapt their objectives and behavior autonomously and flexibly to changing operating conditions.

The design of such complex mechatronic systems is very challenging. This especially holds true for the assurance of their dependability[1]. Indicators for this are the great number of product recalls and increasing warranty costs of the recent years. On the one hand, securing the dependability of such systems is challenging due to their complexity and non-deterministic behavior. On the other hand, self-optimization can be used to increase the dependability of the system during its operation. However, it has to be ensured, that the self-optimization works dependable itself. Due to these challenges, the development of dependable s.o. systems is a difficult task. There is a great need for a framework for the improvement of dependability of s.o. systems, which supports developers by selection and planning of dependability methods to be used. In this contribution such a framework is presented.

The remainder of this contribution is organized as follows: In Section 2 a brief overview over the design of dependable s.o. systems is given. Section 3 introduces the framework for the improvement of dependability of s.o. mechatronic systems. Finally some related work is presented in Section 4.

2. Design of Dependable Self-Optimizing Systems

The s.o. system determines its currently pursued objectives on the basis of the encountered influences on the technical system of its environment. The key aspects and the mode of operation of a s.o. system are illustrated in Figure 1.

[1] Avizienis et al. [1] define dependability as availability, reliability, safety, integrity and maintainability. In this contribution we apply this definition with the exception of the integrity aspect, which is not considered.

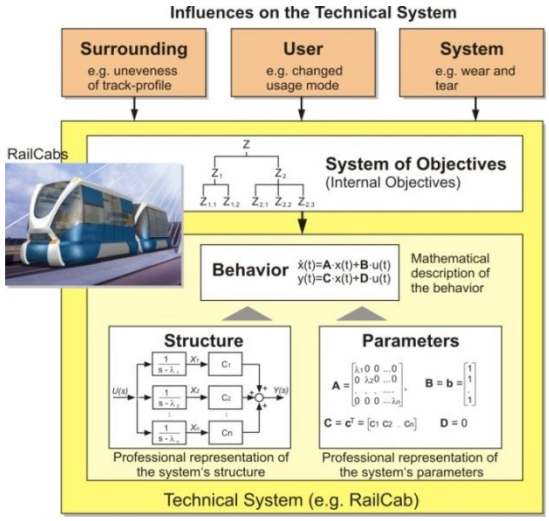

Figure 1. Aspects of self-optimizing systems [2].

New objectives can be added, existing objectives can be rejected or the priority of objectives can be modified during operations. Therefore the system of objectives and its autonomous changing is the core of self-optimization. Adapting the objectives in this way leads to a continuous adjustment of the system`s behavior. This is achieved by adapting parameters or reconfiguration of the structure (e.g. switching between different controller types) during the s.o. process.

The s.o. process consists of the three actions: Analysing current situation, determining the system`s objectives and adapting system`s behavior. In the first phase the observation differs in recalling the sensor data, analysing the fulfilment of objectives and the indirect release of information by communication with other systems. After analysing this information the system independently determines objectives. Objectives can be extracted by selection, adaption and generation. The loop of self-optimization is finished by adapting

the system`s behavior. This can be realized by adapting the (control) parameters and/or the structure of the system.

2.1. Design of Self-Optimizing Systems

The design of s.o. systems begins in the early development phase of conceptual design, the result of which is the principle solution. It describes the basic structure and the operation mode of the system. The principle solution is modelled using a specification technique developed within the CRC 614 [3]. The description of the principle solution is divided into the aspects environment, application scenarios, requirements, functions, active structure, shape, behaviour and system of objectives. Aspect spanning relations are also modelled. In particular, the s.o is described in the system of objectives partial model. The specification of the principle solution forms the basis for the communication and cooperation of the developers from different disciplines during further development phases.

2.2. Dependability of Self-Optimizing Systems

It is of high importance, that s.o. systems have a high dependability. However, the improvement of the dependability of such complex mechatronic systems is highly challenging. The main reason is the adaptable non-deterministic behavior of s.o. systems as neither the environment conditions nor the resulting behavior of the system are fully known in advance.

Generally, there is a great number of dependability engineering methods available, which can be used for the improvement of dependability of s.o. systems. Those methods can be divided in three classes [4]:

1) **The use of classic methods for improvement of dependability:** A number of classic dependability engineering methods can be applied for the improvement of the dependability of a s.o. system. Some of are applied early in the conceptual design on the specification of the principle solution, e.g. the method for early integrative FMEA and the FTA [5]. Other examples of dependability methods are Preliminary Hazard Analysis (PHA), Functional Hazard Analysis (FHA) etc. [6]. The classical methods allow statements w.r.t. the dependability of the systems. Based on those, counter-measures (e.g. redundancy [7]) are derived and the system is made more dependable.
2) **Improvement of system dependability using self-optimization:** In addition, the dependability of a s.o. system can be increased by the use of the self-optimization itself during the operation of the system. E.g. the s.o. system is then able to compensate failures and to change its behavior into a safe state. The self-optimization has to be designed for this purpose [8]. This includes the incorporation of additional sensors and redundant system elements.
3) **Improvement of the dependability of the self-optimization itself:** Moreover, it has to be ensured, that the self-optimization works dependable itself. Methods such as advanced condition monitoring [9] are used to accomplish this.

There is a great number of methods, which can be used to improve the dependability of a s.o. system. Which of them are suitable for a particular system, depends on the underlying development task and the principle solution of the system. There is a high need to support the developers by choosing and applying of the appropriate dependability engineering methods. Therefore a framework for the improvement of dependability of s.o. mechatronic systems has been developed within the CRC 614.

3. A Framework for the Improvement of Dependability of Self-Optimizing Mechatronic Systems

The framework enables the developer to choose and plan the right dependability methods for the particular development task. The developer receives suggestions, which methods are to be used, how they depend from each other, how these methods can be combined as well as what their optimal chronological order is. The framework accompanies the developer through the whole development process.

The cores of the framework are a method database and a guide for planning of the selected methods in the engineering process. The method database contains the description of dependability methods. They are characterized by the dependability aspect (e.g. safety), discipline (e.g. control engineering), development phase (e.g. conceptual design), industry sector (e.g. automotive), corresponding norms (e.g. CENELEC 50128) etc. Links to the development process model and external documents are also included. In addition, the relationships to other methods are described. Following relationships are supported: “is a prerequisite for”, “requires”, “is the further development of”, “has been further developed to” and “can be supported by”. In order to find the suitable methods, the search function of the method database is used.

The guide for planning methods proposes in which sequence the selected dependability methods should be used. The recommendation is based on the analysis of input and output relations of the methods, which are stored in the database. In addition, it is possible to plan a corresponding sequence of development tasks. Beside the link between method and development process a database for the process steps is required.

The framework has been applied on the case example of the innovative railway vehicle RailCab [10]: First a search for dependability methods is performed using the method database (Figure 2 (1)). The selection of appropriate dependability methods takes then place (2). From the method database it is navigated to the corresponding process steps in the process model (3).[2] The software tool supports the planning of the sequence of chosen methods based on the underlying process model description (4). The planning is performed with regard to. the underlying development task and the user role: e.g. for a safety engineer a sequence of methods is proposed, which is conform to a given safety norm.

4. Related Work

A number of works deals with the combination of dependability methods. HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies) [11], which combine FHA and a variant of FMEA. Peikenkamp et al. [12] combine FTA, FMEA and Common Cause Analysis (CCA) to a unified model-based safety assessment method. Usually not more than three different methods are combined. The safety methods database [13] of the NLR (National Aerospace Laboratory) in the Netherlands is a document containing an overview of over 700 safety assessment methods and techniques. A corresponding software database is not publicly available.

[2] It is also possible to navigate in the other direction. From the process model to the corresponding method description.

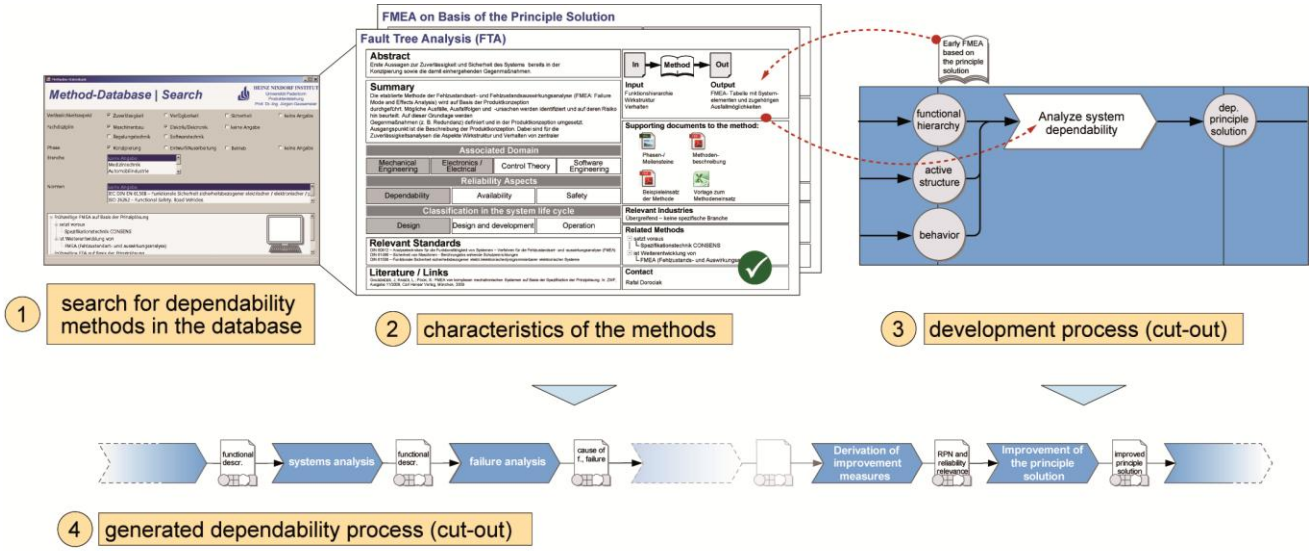

Figure 2. Selection and planning of dependability engineering methods with regard to the underlying development task.

Faerber et al. [14] classify methods by development tasks and Design for X (DfX) criteria. Their software-tool Process Navigator is a database containing methods and the description of the process. The focus lies on Design-for-X methods and processes; selection and planning of methods is not supported and dependability is not addressed explicitly.

5. Concluding Remarks

In this contribution a framework for the improvement of dependability of self-optimizing systems was presented. Its substituent elements are a method database and a guide for planning of the selected methods in the engineering process. An appropriate software-support is also given. The framework supports developers of complex mechatronic systems by selection and planning of dependability methods, which are suitable for their particular development task. In particular, methods for the improvement of the dependability of intelligent mechatronic systems such as self-optimizing systems are found.

Acknowledgements

This contribution was developed in the course of the Collaborative Research Centre 614 “Self-Optimizing Concepts and Structures in Mechanical Engineering” funded by the German Research Foundation (DFG).

References

[1] Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C., 2004, Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, 1/1:11–33.

[2] Collaborative Research Centre (CRC) 614, 2012, the project web site [online]. Available from: http://sfb614.de/ [Accessed 5 March 2012].

[3] Gausemeier, J., Frank, U., Donoth, J., Kahl, S., 2009, Specification Technique for the Description of Self-Optimizing Mechatronic Systems. Research in Engineering Design, 20/4:201–223.

[4] Sondermann-Woelke, C., Hemsel, T., Sextro, W., Gausemeier J., Pook, S., 2010, Guideline for the dependability-oriented design of self-optimizing systems. 8th IEEE International Conference on Industrial Informatics – INDIN2010, July 13-16, Osaka, Japan.

[5] Dorociak, R., 2012, Early Probabilistic Reliability Analysis of Mechatronic Systems, Reliability and Maintainability Symposium, January 23-26, Reno, NV, USA.

[6] Ericson, C.A., 2005, Hazard Analysis Techniques for System Safety, John Wiles & Sons, Inc., Hoboken, New Jersey

[7] Birolini, A., 2007, Reliability Engineering. Theory and Practice. 5th ed. Springer-Verlag, Berlin Heidelberg.

[8] Pook, S., Gausemeier, J., Dorociak, R., 2012, Securing the Reliability of Tomorrow's Systems with Self-Optimization, Reliability and Maintainability Symposium, January 23-26, Reno, NV, USA.

[9] Lee, J., Ni, D., Djurdjanovic, H., Qiu, H., Liao, H., 2006, Intelligent prognostic tools and e-maintenance. Computers and Industrie, 57:476–489.

[10] RailCab – Neue Bahntechnik Paderborn, 2011, the project web site [online]. Available from: http://railcab.de/ [Accessed 5 March 2012].

[11] Papadopoulos, Y., McDermid, J., Sasse, R., Heiner, G., 2001, Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure. Reliability Engineering & System Safety, 71:249–247.

[12] Peikenkamp, T., Cavallo, A., Valacca, L., Böde, E., Pretzer, M., Hahn, E.M., 2006, Towards a Unified Model-Based Safety Assessment, Lecture Notes in Computer Science, 4166(2006), Springer-Verlag, Berin Heidelberg:275–288.

[13] The Safety Methods Database, 2012, National Aerospace Laboratory in the Netherland [online]. Available from: http://www.nlr.nl/documents/flyers/SATdb.pdf [Accessed 5 March 2012].

[14] Faerber, M., Jochaud, F., Stöber, C., Jablonski, S., Meerkamm, H., 2008, Knowledge oriented process management for DfX. 10th International Design Conference – DESIGN 2008, May 19-22, Dubrovnik, Croatia.