Model based Analysis of Complex Failure Chains by Generic Systems Engineering to Improve Dependability in Product Development

Nadine Schlueter
Research Group Product Safety and Quality Engineering
Bergische University Wuppertal, Germany

Petra Winzer
Research Group Product Safety and Quality Engineering
Bergische University Wuppertal, Germany

Abstract- In order to develop and manufacture dependable products, personal of several different specialist disciplines have to interact with each other. But their models and methodologies are often too specific to be connected with each other. Therefore, misunderstandings and failures arise. This paper focusses on the analysis of complex failure chains in interdisciplinary teams. There is a need for an interdisciplinary mobel-based Systems Engineering approach that offers a common system model and a procedure that offers different kind of discipline specific methodologies for engineering problems. How this approach does look like and how it can be applied will be shown in an example: the development of an ultra-cap electro-mobility concept for public transportation busses.

Keywords – Generic Systems Engineering, Demand Compliant Design, Complex Failure Chains, Electro-mobility

I. Introduction

Increasing complexity of products pose a problem to the industry regarding the use of State-of-the-Art methodologies. Although there are existing serveral approaches of model-based Systems Engineering (MBSE) that handle complexity in product development, those MBSE approaches are discipline specific and therefore, their methodologies and models are limited to that area [1]. An interdisciplinary respective transdisciplinary approach that integrated several specific disciplines in order to enable a dependable product development for complex systems did not exist [2] – until now. Thereby, the term dependability can be understood as a topical field that in his totality includes five different characteristics of a technical system: reliability, availability, maintainability, safety and security [3]. In order to avoid failures in the development of complex products regarding this comprehensive topical field, a MBSE approach is selected and introduced, that enabled the combination of discipline specific models and methodologies of failure analysis and therefore serves as an integrator as well as a communicator [4], [5].

The following article explains this innovative MBSE approach (the Generic Systems Engineering, see [1]) by carrying out a failure analysis during the development of an alternative electro-mobility concept for busses. It is pointed out, that GSE integrates and combines the risk analysis methods FTA and RBD within its procedure and enables an interdisciplinary problem solution.

II. Requirements concerning an interdisciplinary MBSE approach for dependable product development

A great number of methodologies for failure analysis are existing in several kind of different, specific disciplines. Just as an example: FTA, RBD, Ishikawa, FMECA, ETA, Markov, Bow Tie, Net-Structures, etc.

All above listed methodologies face the problem that they refer to different definitions of the term "failure". So, there is no common procedure regarding the formalization of failures. This means, it is not defined what is a failure and what is not. In some methodologies, incidents are declared as failures while other methodologies do not consider them as failures at all [6].

Additionally, it can be assumed that an increasing complexity of a system also increases the complexity of failure chains [7]. This way, failure chains can obtain multiple elements, whose interdependencies spread over several system levels or even different types of elements. Usually, methodologies only focus on the component perspective or the function perspective as well as on one system level. In order to complete a logical chain of failure elements regardless of its initial failure, a combination of methodologies is required.

Therefore, a new approach has to consider a loss of performance of single components or functions that – standing alone – are not considered as a failure, but cause a malfunction if interacting with other components or functions. Until today, methodologies focused solely on one single element and define the shortfall of a system only regarding the failure of one element ([8]).

By carrying out a qualitative modeling of interdependencies regarding cause and effect including several types of elements and applying and linking different kind of specific risk analysis methodologies, those functional limitations can be considered. The purposeful use of selected failure analysis methodologies linked to a common MBSE can create a basis for discussions for the interdisciplinary teams. The common information basis also increases the probability to identify critical failures [9].

If the weaknesses of failure analysis methodologies and consequential resulting requirements presented above are explored from the perspective of a MBSE approach, a requirements list can be developed: (I) the approach has to be designed in a way that it can be used in interdisciplinary teams while integrating discipline specific methodologies. (II) It has to use a system model that enables the modelling of the system and its environment in order to serve as a common information basis. (III) The model has to include components, functions and their interdependencies as well as processes on different system levels. (IV) Logical failure chains have to be traceable along different system levels and types of elements. Furthermore, the innovative MBSE approach requires (V) a continuous update of the model within its procedure. This way, the discipline specific methodologies can use the system model as input und feed their output back to the system model for further processing.

A comparison of those requirements with different MBSE approaches (Bahill & Gissing 1998 [10], Sell 1989 [11], Haberfellner & Daenzer 1999 [12], Wulf 2002 [13], Ehrlenspiel 2003 [14], [15], Lindemann 2004 [16], [17], IEEE 1220-2005 [18], Sage & Rouse 2009 [19], [20], Haberfellner et al. 2012 [21], Winzer 2013 [1]) shows that only one is fulfilling the list of requirements in a satisfying way: the Generic Systems Engineering (GSE) by Winzer [1].

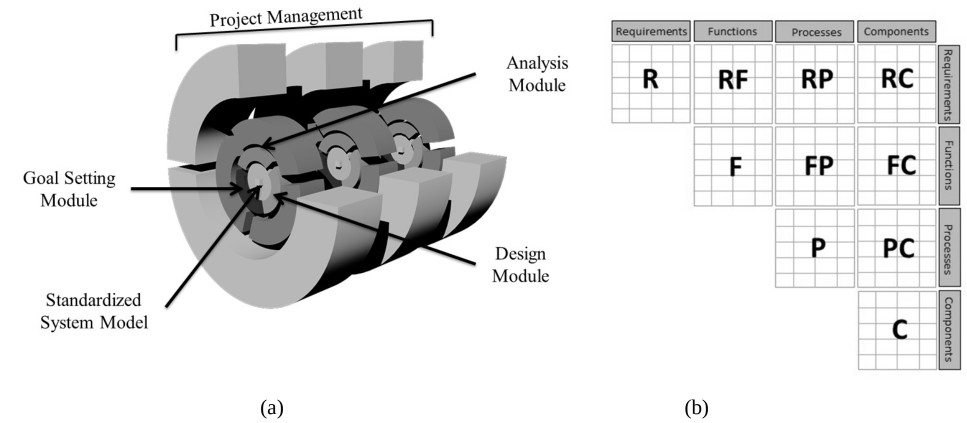


Figure 1. GSE approach by Winzer (in accordance to [1]) and Demand Compliant Design (DeCoDe) (in accordance to [22])

The procedure (respective procedural concept) of GSE is divided into three modules: project management, goal (setting), analysis and design as shown in Figure 1 (a). It offers a purposeful selection of failure analysis methodologies depending on the specific, focused problem. The weaknesses of single methodologies can be conteracted by establishing methodology workflows in GSE [23]. The project management module assures an effective and goal orientated work of the interdisciplinary team.

The availability of information and tracing of design decisions, including the integration of environmental circumstances, is realized by the use of a standardized and interdisciplinary system model, the Demand Compliant Design (DeCoDe) as shown in Figure 1 (b) [22].

DeCoDe provides a common form of presentation in order to link elements and their relations. It includes the requirement, function, component and process element views on the systems and their relations by using matrixes. By considering not only interdependencies between components but also to other types of elements (functions, requirements and processes) the requirement regarding consideration of different types of elements is fulfilled. Also, different system levels can be models by the hierarchical structure of each view. Thus, modelling of complex failure chains is possible.

All in all, Generic Systems Engineering (GSE) enables an interdisciplinary use of its system model by the four views of the Demand Compliant Design (DeCoDe): requirements, functions, processes and components. Former studies proof that linking different kind of failure analysis methodologies is possible (see DeCoDe and FMEA [24], DeCoDe and FTA [25], DeCoDe and RBD [25], DeCoDe and MTTF/MTTB [26]). Also, GSE integrates a continuous update of the DeCoDe system model in its procedure after each carried out methodology. Qualitative as well as quantitative analyses of the system model are possible. But there is no proof, that GSE enables a linking of the focused methodologies (RBD, FTA, FMECA, MTBF) for the analysis of complex failure chains.

Therefore, the combined and integrated use of RBD and FTA within GSE is tested in the following chapter by using design problems of an alternative electro-mobility concept as example.

III. Analysis of complex failure chains by using GSE during the development of K-VEC bus

In the project K-VEC (ERA-NET Transport: Ultrafast and distributed power charge system for high performance on-board energy storage devices, also see [11]) an alternative electro-mobility concept for public transportation busses was developed. Its main characteristic is the usage of ultra-caps, that have the advantage of storing a high amount of energy within seconds. The principle of K-VEC is based on two sub systems: the loading carpet and the contact probe. The loading carpet provides the energy so it can be transferred via the contact probe into the ultra-caps [23], as shown in Figure 2.

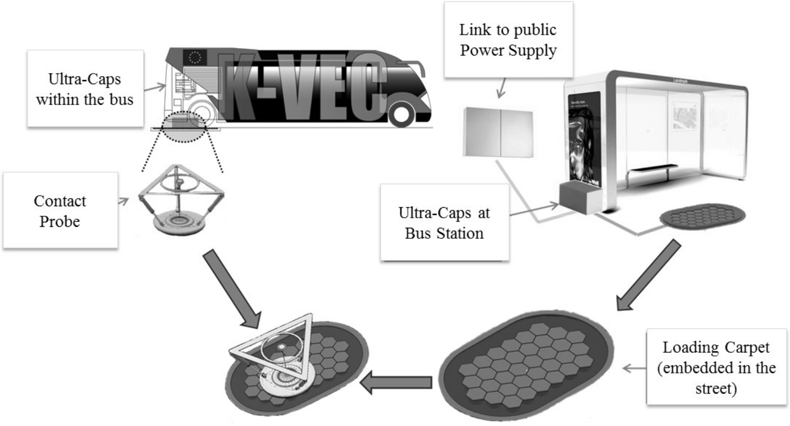

Link to public Power Supply
Ultra-Caps within the bus
K-VEC
Contact Probe
Ultra-Caps at Bus Station
Loading Carpet (embedded in the street)

Figure 2. Principle of K-VEC (in accordance to [23])

When the bus stops at the bus station, the contact probe lowers down onto the loading carpet. After establishing contact closure, energy is transferred to the ultra-caps [23]. In order to develop a dependable prototype for this concept, potential failure sources had to be identified and neutralized. For this, the K-VEC system and its environment was defined at first by using the scenario technique. In the following, the product system was modelled like suggested by GSE and DeCoDe.

The established DeCoDe-based model served as an information basis to identify complex failure chains during in the analysis module of GSE. After identifying potential failure chains the goal setting module was used to select different kind of failure analysis methodologies to assess risks in a qualitative and quantitative way. The employment of the different methodologies was planned and managed via the project management module of GSE. In this case, the interdisciplinary team decided to carry out FTA, RBD, FMECA and MTBF in a combination. While FTA, RBD and MTBF were part of the analysis module, FMECA was transferring the results to the design module, because it suggested actions to prevent the failures.

The identified failure chains had different kind of characterstics that needed to be considered during the methodology selection:

a) Failure chain along several system levels,

b) Failure chain including different kind of element types and

c) Failure chain including environmental circumstances.

In the following, the characteristics (a) and (b) are pointed out.

A. Failure chain along several system levels

During the charging process the output of sensors that detect the position of the contact probe on top of the loading carpet might by incorrect. But only after a successful localization of contact probe to loading carpet as well as connection confirmation the energy transfer is authorized.

If the incorrect sensor output is tracked along its relations on several system levels, the following context (see Figure 3) for the whole system can be identified.

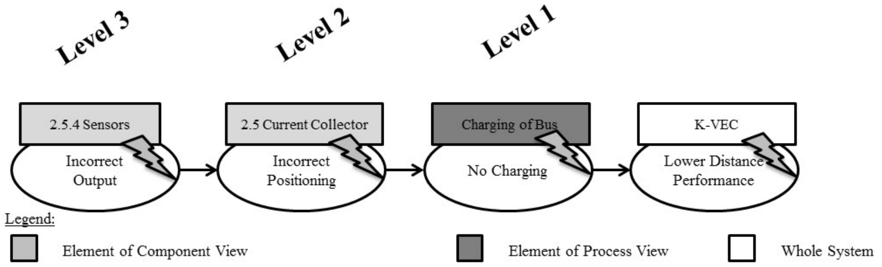


Figure 3. Failure on the lower system level effects the whole system (in accordance to [9])

While the sensor is part of the third system level, he influences the current collector on the second system level. In turn, this component is part of the process “Charging of the vehicle” on the first system level. Hence, a faulty sensor on the third system level can cause effects that affect the higher system levels up to the highest level and cause a performance loss of the whole system.

B. Failure chain including different kind of element types

In another scenario the frequency converter of the loading carpet was focused. The function of the frequency converter is converting alternating current to direct current. This causes an electro-magnetic field that spreads into the environment (see Figure 4). This can cause disturbances in the communication system. If only considered from the component view, this failure cannot be detected. But the interaction with the function shows the problem regarding the electro-magnetic compatibility.

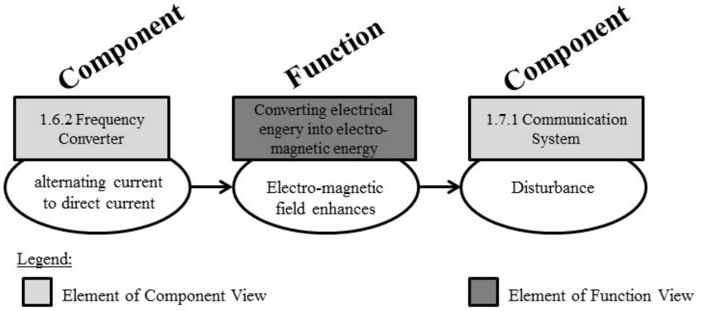

Component
Function
Component
1.6.2 Frequency Converter
alternating current to direct current
Converting electrical engery into electro-magnetic energy
Electro-magnetic field enhances
1.7.1 Communication System
Disturbance
Legend:
Element of Component View
Element of Function View

Figure 4. Failure chain including different kind of element types (in accordance to [9])

C. Identification of Failure Chains by using Loomeo® Software

Above mentioned, exemplary failure chains are included in the DeCoDe-based system model in a latent way. In order to identify those failure chains, the DeCoDe-based product model of K-VEC was visualized by using the software-tool Loomeo® (www.teseon.de), as shown in Figure 5. The software was designed for complexity management and enables the visualization of DeCoDe matrixes as matrixes but also in graphs (elements and their relations). By focusing on one element and its relations during workshops the interdisciplinary teams can discuss different cause-effect-chains.

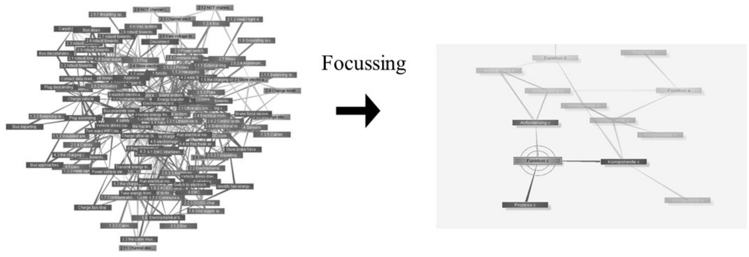


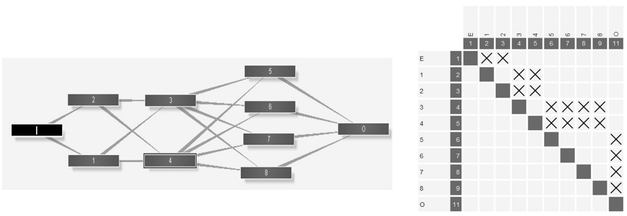
Figure 5. Exemplary visualization of cause-effect-chains of a single element by using Loomeo®´s navigation function regarding the environment of an element (in accordance to [13])

Every failure chain that is identified is recorded and receives an unique ID in order to process it on the method workflow later on.

D. Implementation of model-based failure analysis

In order to carry out a qualitative analysis of failure chains without media disruption, a method workflow for FTA, RBD, FMECA and MTBF was designed and linked to the system model by using Loomeo®. While [27] points out this approach for FMEA, the following example shows the procedure for FTA and RBD.

After identifying failure chains and transferring them into separate models by using Loomeo®, the input and output of each failure chain is defined. This way, every failure chain can be differentiated from other, similar variants. Figure 6 shows such a failure chain with its starting and ending in the graph modus (Figure 6 (a)) and the matrix modus (Figure 6 (b)) of Loomeo®. Due to non-disclosure agreements, the elements are not named but numbered.



(a) (b)

Figure 6. (a) Visualization of failure chains by Loomeo® in graph and (b) matrix modi (in accordance to [9])

FTA as well as RBD set the goal to identify weaknesses in the construction design regarding shortfall of single components. Already, a qualitative analysis in accordance to RBD like shown in Figure 6 (a) points out the high reliability of the system due to redundant designs of components. Carrying out a FTA additionally points out which components have to fail in order to cause a shortfall of the whole system.

During the use of Loomeo® it became evident that a separate modelling of RBD and FTA in corresponding, specific software-tools is not necessary. The results of RBD and FTA are already evident in the matrix modus of Loomeo® (see Figure 6 (b)). A cluster of relations within the matrix identifies redundancies of single elements. This is especially useful for models with an enormous number of elements. This way, the transfer of data and required resources for RBD- and FTA-Software-Tools can be cut. Furthermore, the matrix modus enables the identification of cluster or the lack of it within a second. This way, statements upon the redundancy of the system can be gained in short time. Additionally, “bottle-necks” in the construction design regarding the reliability of the product system can be identifies as fast.

IV.CONCLUSION

As products become more and more complex, potential failure chains do the same. Thus, failure analysis methodologies have to be enhanced. Today, methodologies in the field of failure analysis are usually discipline specific, lack a common understanding of the term failure and cannot handle complex failure chains. They are either deductive or inductive and cannot handle failure chains along several system levels, different types of elements or include the environmental circumstances.

Corresponding to that, a model-based SE approach was chosen, the Generic Systems Engineering (GSE), to support an interdisciplinary development of an electro-mobility concept by applying a model-based method workflow for failure analysis. GSE enables the integration of different discipline specific failure analysis methodologies, so that the best method for the problem at hand can be selected. Furthermore, it provides a standardized model that serves as an information basis for the interdisciplinary team. This improves communication. And as the model is updated continuously after each step, the information is always up to date.

According to GSE the system and its environment was defined in a first step. Then the model of K-VEC was designed by using the Demand Compliant Design (DeCoDe) and the software tool Loomeo®. By using the standardized DeCoDe views (requirements, functions, processes, components) and applying the “environment”-function of Loomeo®, several potential complex failure chains were identified and transferred into separate DeCoDe-based models for further processing with the failure analysis method workflow. The method workflow included FTA and RBD. A transfer of data to specific software tools for FTA and RBD was not necessary. Loomeo® was able to visualize the data in its matrix mode in a way that a qualitative analysis regarding redundancies or the lack of it could be carried out within seconds. This way, media discontinuities and additional resources for specific software tools were cut.

By using the iterative procedure of GSE the product model was updated continuously within the project. This way, the interdisciplinary team always had an up to date model and information basis to work with. Summarized, it can be stated that the listed requirements regarding the enhancement of MBSE approaches and failure analysis methodologies for complex failure chains are fulfilled in a satisfying way.

In the following research, more methods are evaluated regarding their integration into GSE. Thereby, the focus is on failure analysis methods at first. But in the future, it is appropriate to consider also methods of other fields like requirements management, construction design, etc. The fundamental question is, if GSE can be used to promote the integration of specific disciplines and their methodologies, so that a common basis for the whole engineering can be achieved.

REFERENCE

[1] Winzer, P.: Generic Systems Engineering - Ein methodischer Ansatz zur Komplexitätsbewältigung. Springer Vieweg Verlag 2013. ISBN 978-3-642-30365-4.

[2] Dhillon, J.S. (2005): Reliability, quality, and safety for engineers, CRC Press.

[3] Malassé O., Buchheit G., Pock M., Walter M. (2010) Dependability Evaluation of Complex Embedded Systems and Microsystems. In: IEEE Conference Publications of Reliability and Maintainability Symposium, 2010, p. 1.

[4] Bahill T, Gissing B (1998) Re-evaluating systems engineering concepts using systems thinking. IEEE Trans Syst Man Cybern Part C Appl Rev, 28: 516–527.

[5] Calvano C. N., John P. (2004) Systems engineering in an age of complexity. In: IEEE Engineering Management Review, Vol 32, Issue 4, 2004, pp. 29-38.

[6] Willing, M.; Winzer, P. (2015): Fehler vermeiden heißt Fehler verstehen – Anforderungen an eine neue Methodik. In: Bracke, S.; Mamrot, M.; Winzer, P. (Hrsg.), Qualitätsmethoden im Diskurs zwischen Wissenschaft und Praxis, Bericht zur GQW-Jahrestagung 2015 in Wuppertal. Band: 2015,17. Reihe: Berichte zum Qualitätsmanagement. 2015, pp.303 – 320.

[7] Velandia D. S., Conway P. P., Wilson A., West A. A., Whalley D. C. (2007): A Modelling Framework for the Reliability of Safety Critical Electronics. In: IEEE Conference Publications of the International Conference on Thermal, Mechanical and Multi-Physics Simulation Experiments in Microelectronics and Micro-Systems (EuroSime), 2007, pp. 1-6.

[8] European Standard DIN EN 61025; August 2007: Fehlzustandsbaumanalyse.

[9] Bielefeld, O; Darnsfeld, H.; Kemper, P.; Schlüter, N.; Winzer, P.; Witkowski, U.; Yazdanmadad, S. (2016): Modellbasierte Analyse komplexer Fehlerketten. In: Schulze, S.-O.; Muggeo, C.: Tag des Systems, Hanser Verlag, München..

[10] Bahill T, Gissing B (1998): Re-evaluating systems engineering concepts using systems thinking. IEEE Trans Syst Man Cybern Part C Appl Rev, 28: 516–527.

[11] Sell R (1989): Angewandtes Problemlösungsverhalten. Denken u. Handeln in komplexen Zusammenhängen, 2. Aufl. Springer, Berlin.

[12] Haberfellner R, Daenzer W F (1999) Systems Engineering: Methodik und Praxis. Verl. Industrielle Organisation, Zürich.

[13] Wulf J (2002): Elementarmethoden zur Lösungssuche. Verlag Dr. Hut, München.

[14] Ehrlenspiel K (2003): Integrierte Produktentwicklung: Denkabläufe, Methodeneinsatz, Zusammenarbeit. Hanser, München.

[15] Ehrlenspiel K., Hundal M. S. (2006): Cost-Efficent Design, Springer / ASME Press, Berlin, 2006.

[16] Lindemann U (2004): Methodische Entwicklung technischer Produkte: Methoden flexibel und situationsgerecht anwenden. Springer, Berlin.

[17] Lindemann U., Maurer M., Braun T. (2008): Structural Complexity Management: An Approach fort he Field of Product Design, Springer, Berlin, 2008.

[18] IEEE Std 1220-2005 (2005): IEEE standard for application and management of the systems engineering process. IEEE Computer Society. IEEE, New York.

[19] Sage AP, Rouse WB (Hrsg) (2009): Handbook of systems engineering and management. Wiley, Hoboken.

[20] Sage A. P. (1996): Manufacturing systems engineering and management. In: IEEE Conference Publications of the International Conference on Systems, Man and Cybernetics, Vol. 1, 1996, pp. 1-9.

[21] Haberfellner R, Vössner S, Weck O, de Fricke E (2012): Systems Engineering. Grundlagen und Anwendung. Orell Füssli, Zürich.

[22] Sitte, J., Winzer, P. (2011): Demand Compliant Design. In: IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, Volume 41, No. 3.

[23] Schlüter, N.; Winzer, P.; Willing, M. (2013): Integrating Safety and Quality Into the Requirements Oriented Product Development by the Example of a New Electro Mobility Concept. In: Acta Mechanica Slovaca, Journal published by Faculty of Mechanical Engineering. Volume 17, No. 2/2013, p. 54-63.

[24] Ott, St. (2009): Konzept zur methodischen System-Modellierung in der anforderungsgerechten Produktentwicklung. In: Berichte zum Generic-Management. Band: 2009,3. Shaker Verlag, Aachen.

[25] Hartmann, C.; Winzer, P. (2011): DeCoDe+X in KitVes - Using the Demand Compliant Design in the Development of a Solution for Harvesting High-Altitude Winds for Energy Generation on Vessels. In: Jaca, C.; Mateo, R.; Viles, E.; Santos, J. (Hg.): Proceedings 14.QMOD Conference on Quality and Ser-vice Science 2011. Pamplona, Spain: Servicios de Publicaciones Universidad de Navarra (14), p 721 – 737.

[26] Willing, M.; Riekhof, F.; Winzer, P. (2011): Reliability in early product development phases - Using the DeCoDe+X approach for a data-based discussion of design decisions. In: Jaca, C.; Mateo, R.; Viles, E.; Santos, J. (Hg.): Proceedings 14.QMOD Conference on Quality and Ser-vice Science 2011. Pamplona, Spain: Servicios de Publicaciones Universidad de Navarra, pp. 1831 - 1847

[27] Riekhof, F.; Winzer, P. (2012): Optimisation of the requirement-oriented product development by a functions differentiation within a holistic system description. In: Total Quality Management & Business Excellence, pp. 1–8.