Smart Failure and Risk Analysis in Complex Systems

Frank Zeihsel, Christian M. Thurnes, Svetlana Visnepolschi[1]

Abstract. Risk management and with this risk analysis and risk evaluation are mandatory for today's companies, not only because it is requested by laws and regulations but also to ensure the future existence of a company. Although methods are used to fulfill this task many failures occur after system launch, especially in complex systems. This paper presents a method that is able to generate potential failures not by asking what might go wrong, but by inverting the problem to how can we make it go wrong and finding a solution for preventing that failure from there. With its system based modeling and its systematic approach to failure generation an almost comprehensive set of failures and failure scenarios can be provided.

Keyword: Risk analysis, Risk Evaluation, Anticipatory Failure Determination AFD, Failure Prediction, Theory of Inventive Problem Solving - TRIZ

1 Introduction

Methods for risk management in systems, as well organizational as in technical systems, can be seen in Fig. 1. Especially the methods for Risk Analysis and Risk Evaluation (the steps of Analysis and Evaluation are often executed in parallel) may be considered. There in this area are only a few methods available, if the focus is set to technical systems:

- FMEA: Failure Mode and Effects Analysis
- HAZOP: Hazard and Operability Study

[1] Frank Zeihsel
Synnovating GmbH, Mozartstr. 25, 67655 Kaiserslautern, Germany
zeihsel@synnovating.com

Christian M. Thurnes
University of Applied Sciences Kaiserslautern; Amerikastr. 1,66482 Zweibrücken, Germany;
christian.thurnes@fh-kl.de

Svetlana Visnepolschi
Ideation International Inc., 32000 Northwestern Highway, 48334 Farmington Hills, MI , USA
vis@ideationtriz.com

- FTA: Fault Tree Analysis
- Cause and Effect Diagram

Amongst these methods the Failure Mode and Effects Analysis (FMEA) is the most established tool for risk analysis and failure prevention in engineering. The fact, that FMEA emerged as a standard in this area, is particular the result of the implementation by QS- 9000 within the automotive industry [2]. FMEA is hugely useful to identify possible, but in some degree expected, failures, e.g. the nonperformance of a function or the minor deviation from an expected data [3].

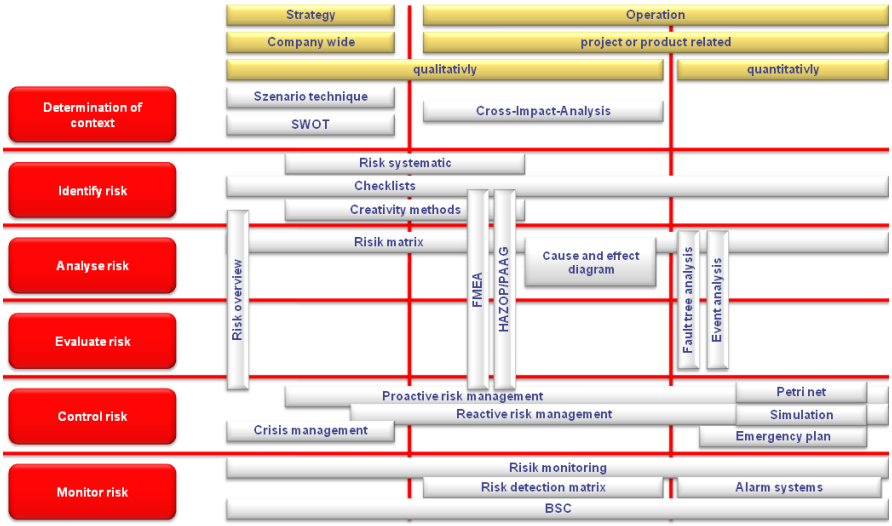

Fig. 1 Methods for risk management and their position in the risk management process (according to [1])

Sooner or later every company has to experience that the number of occurred defects is still too high. The impacts can either be quite innocent or of particular importance for companies, employees, regions or the whole mankind. Failures, not expected in the slightest, are particularly fatal. They happen, when the cause of trouble cannot be derived directly from the product or process structure. Moreover, the combination of several errors can cause more serious impacts, than each error itself. In most risk management methods the failures are derived by:

- Negating the intended function
- Brainstorming about possible failures
- Look for failures that have already happened

Anyway, locating possible and future failures is by no means automatism, but rather a procedure, that requires, besides a systematic approach, lots of creativity and inventive talent. According to Frenklach it requires not only asking the characteristically FMEA- questions "why" and "what", but furthermore asking the question "how" several times [7].

Anticipatory Failure Determination (AFD) encourages these questions. AFD is a TRIZ-based procedure. TRIZ (the Russian acronym for Theory of Inventive Problem Solving) is a set of methods developed by Genrich S. Altshuller for supporting creativity in the inventing and problem solving process [12]. To invent failures, by inverting the problem, enables us to use other TRIZ tools for revealing hidden failure mechanisms and for predicting unexpected future failures. Using TRIZ tools allows us to achieve innovative preventive measures respectively preventive system designs. Examples from different fields of application prove the success of this procedure (e. g. [7],[8],[9],[10],[11]). Hereafter this preventive aspect will be defined as AFD Failure Prediction (AFP).

Based on Altshullers insight that TRIZ offers powerful approaches for different scopes including research and development [12], the evolution of AFD is affected by the work of other well known names e.g. Zlotin and Zusman creating AFD method in the early eighties introducing the inversion and operators as key elements [4] or V. Mitrofanov who worked on problems regarding waste elimination in manufacturing using the principle of intensification. The evolution of the AFD is shown in detail in the book "How to deal with failures (The smart way)" [6].

The implementation of the main AFP idea can be done by using different TRIZ tools and different levels of standardization. Promising lines of action and potential software support exist and are published (e.g. [4], [5], [6]). But as a matter of fact, Anticipatory Failure Determination in general is still one of the TRIZ tools that is not used very frequently [13].

2 Anticipatory Failure Determination Prediction

Since there is no AFP-standard this work will refer to the detailed process description of S. Visnepolschi (one of the authors of this work). This process includes the following eight steps [6]:

2.1 Obtaining information (Step1)

In this first step the expectations for the AFP project have to be defined. Usually there is the need for a "practically safe" system – a system that will not collapse, injure anyone or cause some trouble for the responsible persons or institutions [15]. After this definition a set of well-proven questions supports the gathering and/or creation of necessary information. These questions help to explore the sys-

tem of interest, its structure, its functioning, undesired effects, its environment and the history of the system.

2.2 Developing a System Diagram (Step 2)

The System Diagram visualizes cause-and-effect connections in the functioning of the system. The favored notation is based on the problem formulation notation [16] [17]. So the system diagram for the AFP should include the useful and harmful functions (or operations). In this case an important event or a meaningful state of the system may also be considered as a "function". The functions are the knots of the diagram that are connected somehow by cause-effect links. The diagram also indicates the primary useful function of the system. The graphical representation of the system assures, especially for complex systems that nothing is forgotten and the risk analysis team gets more insight to the system itself. An example is given in Fig. 2.

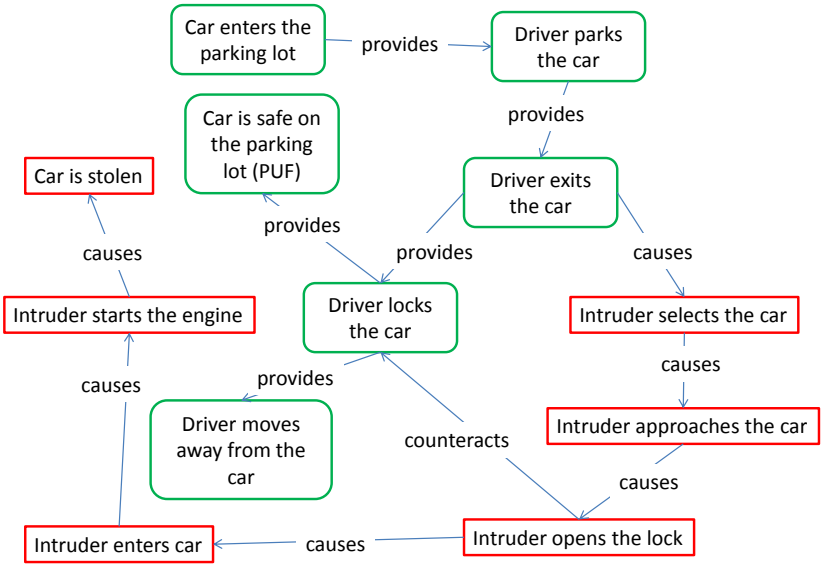

Fig.2 Example System Diagram [6].

2.3 Identifying Focal Points (Step 3)

Focal Points are the zones or weak points of the system that may cause the biggest weakness of the system or the greatest danger. So using the system diagram the focal points are represented by useful functions that lead to big weakness and harmful functions that cause great danger. Typically focal points in the system diagram have a high number of incoming and outgoing links and are strongly connected with the systems functioning (Fig. 3). The approach to concentrate on Focal Points emphasizes the intention to identify the unexpected and especial critical failures. For each identified focal point the next step is executed.

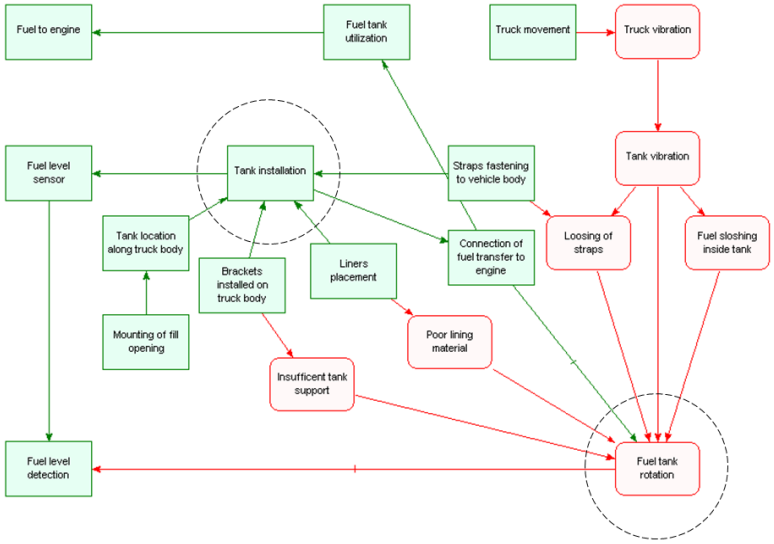

Fig. 3 Examples for focal points (circled elements).

2.4 Generating Failure Hypotheses (Step 4)

The generation of failure hypotheses is divided in two stages: the development of "AFP Directions" and the application of Checklists and Operators.

A systematic way to develop the AFP Directions is given by the consequent utilization of the SEOR-model regarding the Focal Points. The AFP Directions are abstract commands that are challenging readers to develop failure hypothesis (e.g.: Find ways to strengthen harmful impact on the Focal Point!). Fig. 4 shows the SEOR-configurations to formulate the AFP Directions.

An example for the SEOR-Model can be described as follows: to destroy (melt) an Object (a plastic pad) the harmful Source (a heating device) should be placed close the Object. Conversely: to protect the plastic pad (opposite effect), it should be moved away from the harmful Source (the heating device).

Answering the commands of the AFP Directions leads to a first list of failure hypotheses. With this systematic approach even more failure hypotheses can be found as just with intuition.

The Checklists and Operators can now be used to enforce this effect dramatically. This well structured lists (e. g. typically hazardous materials, typically hazardous processes, typically hazardous individuals ...) and Operators (concrete but not specific thought-provoking impulses, derived from different TRIZ-tools and experience in AFD) let the list of failure hypotheses expand even more.

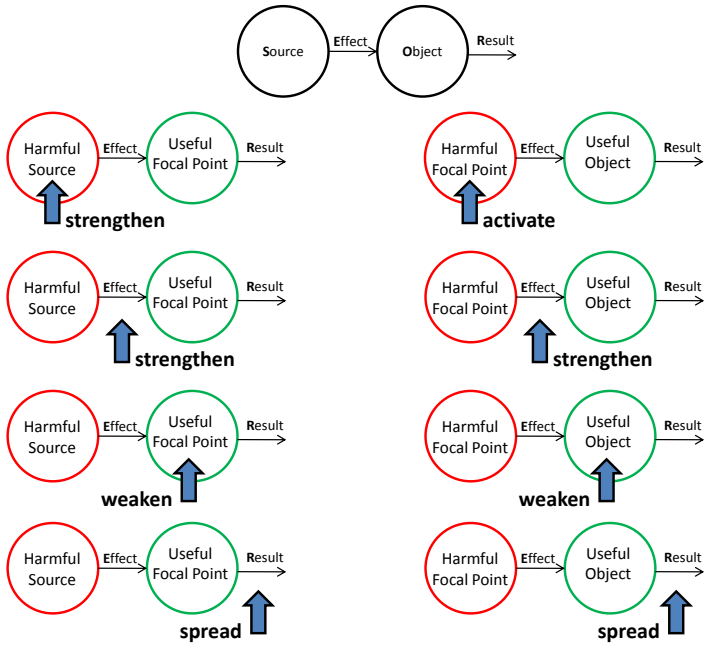

Fig.4 SEOR configuration [6].

SEOR formulations for the truck tank modeled in Fig. 3 are (partial list):

1. Determine what typical harm can be provided to [the] (Tank installation).
2. Try to deteriorate the useful impact of [the] (Tank installation) on [the] (Connection of fuel transfer to engine) and (Fuel level sensor).
3. Consider additional ways to deteriorate [the] (Tank installation).
4. Try to increase the vulnerability of [the] (Tank installation).
5. Consider utilizing the resources of surrounding systems to deteriorate [the] (Tank installation).

6. Utilizing the resources of [the] (Tank installation) to deteriorate other systems.
7. Consider utilizing the resources of [the] (Straps fastening to vehicle body) to deteriorate [the] (Tank installation).
8. Consider utilizing the resources …

2.5 Generating Failure Scenarios (Step 5)

This step continues the search for failures in two ways: Inventing most dangerous failures and combining resources of multiple failures.

Inventing the most dangerous failures is a procedure supported through particular checklists. It encompasses the attempts to intensify already found possible failures and to explore possibilities to hide the failures. The combination of multiple failures helps creating failure scenarios with intensified impact on the system.

2.6 Assessing Risks (Step 6)

The process of evaluating the risks in AFP is based on the definition of hazard and likelihood. But these two factors may be used in a different way [6]:

Regarding the hazard failure hypotheses and scenarios have just to be judged whether they are causing injury to human beings, danger to the systems functioning or pollution to environment or not.

Regarding the likelihood estimation is very hard for potential critical errors that are invented by thinking about the most dangerous failures and the combination of different errors. Instead of guessing the likelihood of failure exposure the likelihood can be evaluated by the evaluation of the availability of the existing resources that are necessary to provide the failure.

As a result of this consideration failure scenarios and hypotheses can be defined as very important, if they are very hazardous and the resources to provide the failure are available (at the moment or under specific but possible conditions). Failures not very hazardous but likely to occur or failures very hazardous less likely to occur are designated as “second priority”. The lowest priority group includes the failure scenarios and hypotheses that are not very hazardous less likely to occur (Fig. 5).

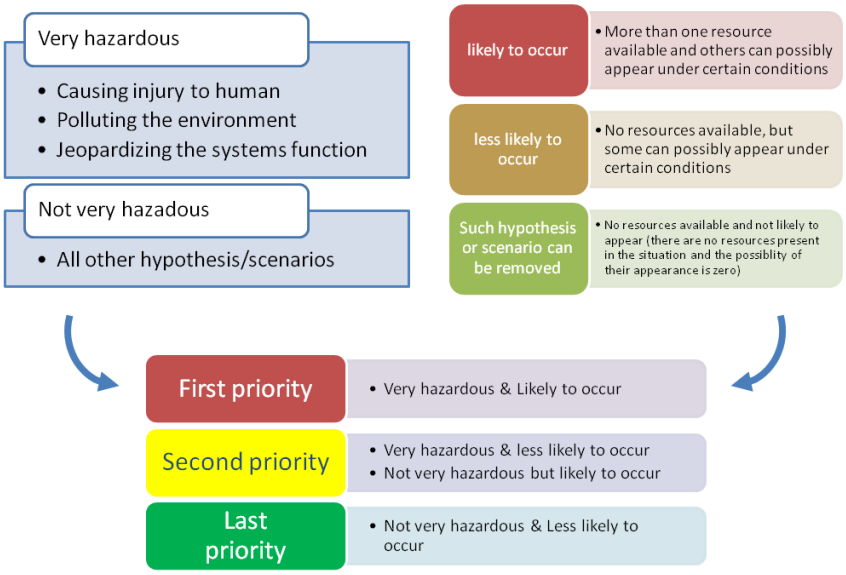

Fig. 5 Risk assessment depending on impact and likelihood of availability of necessary resources.

2.7 Preventing Probable Failures (Step 7)

The prevention of the failures should be started by developing a system diagram (see step 2) for each failure hypothesis or scenario that is to consider. These diagrams are the starting point to find the solutions to prevent the failures. The diagrams show failure mechanism chains and contradictions. Just analyzing these diagrams can produce reliable solutions. With the help of checklists, operators or some other TRIZ-tools more effective solutions can be developed.

2.8 Evaluating Results (Step 8)

The evaluation of the results shows if the solution really can be implemented preventing the failure completely. To prove that the solutions should be examined in detail – like in the procedure described so far, now the solutions have also to be checked with a simplified Express-AFP procedure.

3 Example

As an example a part of a project is described – the dangerous safety label. The Failure Prediction was provided for one of the largest US manufacturers of household cleaning products and was related to the insecticide aerosol. While analyzing the features of the given product and taking into consideration its mass market the AFD specialists paid a particular attention to the spray safety label.

Fig. 6 Safety label on aerosol can

The label was positioned at the back of the product container and included the information regarding safe usage of the aerosol, as well as warnings against its possible fire and inhalation hazards. The information followed all the government safety regulations and was offered in two languages: English and Spanish.

The company management and engineering team considered the label as one of the strongest safety features in the product.

The AFD inverted forecasting task was formulated as follows:

> It is necessary to provide all imaginable harm to the aerosol's user in spite of, or even with help of the safety label

As a result of brainstorming this forecasting direction the following Failure Scenarios were generated:

- Many consumers experience difficulty reading labels due to:
  - Limited knowledge of English and/or Spanish
  - Vision problems (age- or otherwise related)
  - Limited visibility of the label in many positions of container

Each of the above may lead to the violation of expiration date, improper usage, storage, transportation and disposal.

- People also tend not to read the label, if container is similar in design (and/or style) to containers of other household products. In such case consumer may assume that a specific instructions is not necessary to handle a familiar-looking product.

- The same tendency exists regarding long texts provided in fine print. Only certain population demographic (highly educated, health-oriented customers) read them thoroughly. Therefore, the longer is the text on a label, the higher is the likelihood that information would not reach the customer.
- The information that can be provided on the label:
  - Is limited by available space on container surface, and
  - Does not protect from various ways of the product improper use or transportation. In particular it does not warn against carrying a container in the car salon left unsecured at the passenger seat. The cylindrical shape of the container is the critical failure resource. Such container can slip to the floor, roll under brake pedal and cause a road accident.

- When the above failure scenarios had been presented to the company's subject matter experts they evaluated them as very likely and a high priority. As a result the following solutions were developed to prevent issues with the safety label:

1. Different fonts and color for different pieces of information would provide better text visibility
2. Foldout label that can be easily unfolded provides additional space for information. Such label could also include additional advertisement or a coupon.
3. Double/triple-layered label. The first layer with sale information can be removed after purchase; then - the usage instruction and disposal information are exposed.
4. First layer covers the pressing button preventing accidental use.
5. A container with non-rolling shape (ellipsoid, in particular) would protect against brake-related accidents. It will also provide better text visibility.
6. The product cap can be considered as a space resource. Extra information can be printed on the cap.
7. Another (geometrical) resource is the round shape of the cap and container bottom. A round marketing text message can be placed on the top and a round warning text message - on the bottom part of the can.
8. Instruction provided by speaking microchip could be useful for blind/illiterate, forgetful customers.
9. It would be beneficial to add another label warning signal via tactile sensation to the user skin (label rough surface or a special pattern on the label surface, etc.)
10. Prioritize warnings. Most important messages should be positioned on the top of a container.
11. Using icons instead of instructions/warnings would save a lot of space. Young generation of computer and i-Phone users is very used to various icons.
12. A dynamic, chemically-sensitive label that changes information after purchase from marketing to usage/disposal instruction thus providing twice more information in the same space.

13. Changing picture/text (English/Spanish) visible under different angle (in different position of the can) could provide more information in the same space.
14. Gloves attached to each product container could protect hands from spilled liquid. Adding gloves to the product would demonstrate the manufacturer care of customer safety that is one of the major consumer trends. Variation: plastic glove-like extension protecting hand.
15. Protection kit in one package with spray (mask, gloves, simple shoulder/arms cover)
16. Hazardous product should have visibly different appearance (shape/ color) in order to be easily identified among others or in improper place/conditions.

As a result of the Failure Prediction project many safety issues related to the insecticide aerosol had been prevented and expensive potential law suits for the company have been avoided.

4 Conclusion

Finding important potential failures in complex systems should not be based on serendipity. Beyond traditional tools and methods AFD Prediction is a system-based structured method for unveiling hidden and dangerous failures. Following the process of AFD Prediction one can achieve a comprehensive set of potential failures and, furthermore, generate and evaluate failure scenarios from combinations of single failures that might be more dangerous than the single failure itself (combination of earthquake, tsunami, and loss of electrical power in Fukushima power plant).

References

[1] Woll, R. 2007, ""Risikomanagement – Aufgabe für das Qualitätswesen in klein- und mittelständischen Unternehmen? – Ergebnisse der DGQ-Arbeitsgruppe 124 Risikomanagement"; DGQ-Regionalkreis Berlin, 16. Oktober 2007; http://www.dgq.de/dateien/dgq-RK.pdf.

[2] McDermott, R. E.; Mikulak, R. J. Beauregard, M. R., 2008, "The Basics of FMEA", Productivity Press 2nd edition, ISBN 9781563273773, 91 pages.

[3] Hippel, J., 2006, "Predictive Failure Analysis: How to use the TRIZ in Reverse", www.triz-journal.com/archives/2006/09/06.pdf.

[4] Kaplan, S.; Visnepolschi, S., Zlotin, B; Zusman, A., 1999, "New Tools for Failure and Risk Analysis: An Introduction to Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring", ISBN 1-928747-05-1.

[5] Ungvari, S., 1999, "The Anticipatory Failure Determination Fact Sheet", http://www.triz-journal.com/archives/1999/10/a/index.htm.

[6] Visnepolschi, S., 2008, "How to Deal with Failures (The Smart Way)" Ideation International Inc. Farmington Hills, MI, USA

[7] Frenklach, G. 1998, “Diversionary method”, http://www.triz-journal.com/archives/1998/04/a/index.htm
[8] Proseanic, V., Tananko, D., Visnepolschi, S., 2000, “The experience of the Anticipatory Failure Determination (AFD) method applied to an Engine Concern”, http://www.triz-journal.com/archives/2000/06/c/index.htm
[9] Proseanic, V., Visnepolschi, S., 2000, “TRIZ Electing a President”, http://www.triz-journal.com/archives/2000/04/e/index.htm
[10] Ruhe, T., 2003, “ Anticipating Failures with Substance-Field Inversion – A TRIZ Methods Case Study”, http://www.triz-journal.com/archives/2003/03/b/02.pdf
[11] Zlotin, B., Zusman, A., Kaplan, L., Visnepolschi, S., Proseanic, V., Malkin, S., 2000, TRIZ beyond Technology. The theory and practice of applying TRIZ to non-technical areas. Proceedings of TRIZCON 2000, pp. 135-176
[12] Altshuller, G.S. 1984. Creativity as an Exact Science. Translated by Williams, S. NY: Gordon and Breach Science Publishers.
[13] Livotov, P., 2004, “The underevalued innovation potential”, http://www.triz-journal.com/archives/2004/03/2004-03-06.pdf
[14] VDA – Verband der Automobilindstrie (Ed.), 2009, Qualitätsmanagement in der Automobilindustrie Band 4 – Sicherung der Qualität in der Prozesslandschaft, Berlin, ISSN 0943-9412
[15] Visnepolschi S., Proseanic V., 2003, “Focal Points of the System, SEOR Principle and their contribution into creation of the Practically Safe System” – TRIZCON 2003, Conference Proceedings
[16] N.N., 2005, „Problem Formulator“, Ideation International Inc., Farmington Hills, MI, USA, http://www.ideationtriz.com/new/materials/ProblemFormulation.pdf
[17] Terninko, J., Zusman, A., Zlotin, B., 1998, “Systematic Innovation: An Introduction to TRIZ”, CRC St. Lucie Press, ISBN 1-57444-111-6
[18] Däuble, H. et al., 1995, System FMEA – Leitfaden für Anwender, Mercedes Benz AG, Stuttgart