A new knowledge-based risk control method for risk sensitive devices

S. Plogmann[1], A. Janß[1], A. Jansen-Troy[2] & K. Radermacher[1]
[1]*Chair of Medical Engineering, Helmholtz-Institute for Biomedical Engineering Aachen, RWTH, Aachen University, Germany*
[2]*SurgiTAIX AG, Germany*

Abstract

Medical engineering is always closely linked to the well-being of the human. This close relation can strike out at two directions: although medical devices are intentionally designed to support diagnosis and therapy, they can also cause serious adverse events and harm patients, users and third parties. Therefore, according to ISO 14971, risk management – including risk identification, risk evaluation, risk control and market surveillance – is an important and inevitable chapter in medical device development. Unfortunately, the risk control process, which implies selection and application of countermeasures (generally through inherent, protective or descriptive safety measures), is not yet supported systematically and methodically. Therefore the Chair of Medical Engineering at the RWTH Aachen University has developed a methodological approach to generate appropriate countermeasures for given risks, helping to mitigate previously identified technical and human-induced errors or hazards in products and processes.

The methodology uses a knowledge-base, reorganizing prior experience, from by now fourteen risk analyses of medical systems, comprising research and industrial risk assessments. Case-tailored categories from error-taxonomies allow the user to hark back to his antecessors' knowledge in a user-friendly manner. The methods' basic structure is built on the Theory of Inventive Problem Solving (TRIZ) and can be fed with further data in the future. Purely technical and system-inherent, as well as Human-Machine-Interaction errors, have been organized in thirteen error categories, filing 61 individual failure modes, which represent the former (root) causes and failures from the analyzed risk analysis data base. The different possible combinations of cause and failure are displayed

WIT Transactions on The Built Environment, Vol 134, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130051

in a 2-D matrix, indexing a total of 41 abstract principles of risk control that suggest tailor-made solutions for a specific problem.

Evaluation of the method took place with different test groups, each time in comparison to conventional brainstorming as the state-of-the-art reference. Reassessment of risk priority numbers (after applying countermeasures) by a blind expert, shows a noticeable benefit, gained by the new method.
Keywords: healthcare/medical systems, risk control in risk management, system safety, theory of inventive problem solving (TRIZ), human factors.

1 Introduction

As the field of medical engineering is a highly risk sensitive one, the aim of assuring products' and processes' safety, is not only a question of patients', users' and third parties' security, but also a question of getting market approval from the respective regulative body, which is achieved by proving compliance with relevant standards, like DIN EN ISO 13485 or DIN EN ISO 14971 [7, 8]. Seen from this point of view, standards can easily be misunderstood as a hindering barrier between developing institutions and patient. To avoid this kind of dead-end, and to make standards an auxiliary implement that proactively helps the engineer to reach the formulated goals, it is important that standards supply readers with knowledge, which can be refined or incorporated in methods or action strategies, giving clear advice on how to deal with a certain challenge. This way, recommendations found in standards, do not form a regulative obstacle, but hint at the solution of the problem.

Regrettably, the risk control process (within the risk management process), which consists of selection and application of countermeasures, is not yet standardized and not even supported systematically and methodically.

2 State of the art

2.1 Risk management

Most of the existing methods in risk management focus on risk identification, risk evaluation and market surveillance. Well established methods, such as Fault-Tree-Analysis (FTA), Failure Mode and Effect Analysis (FMEA), Hazard and Operability Study (HAZOP), Hazard Analysis and Critical Control Points (HACCP) and Preliminary Hazard Analysis (PHA) provide little methodological help, when it comes to mitigating a detected risk. Exceptional cases, strongly influenced by the risk management guide for information technology systems [4], mainly arise from the information technologies (IT) sector, but are often restricted to providing decision making support for choosing only among a limited set of countermeasures. Furthermore, in most cases these countermeasures are not proposed in dependency of the particular hazard that forms the basis of the efforts to mitigate the risk.

A recent Risk Assessment and Optimization Model (RAOM), developed by Viduto *et al*. [3] proposes a numerical selection method for choosing within a

given list of potential countermeasures. Although this approach contributes to solving the selection problem, it shows two deficiencies. Firstly, it assumes a list of potential countermeasures that must previously be defined in an isolated step, where no methodological support is given. Secondly, the proposed procedural method for determining the countermeasure-to-vulnerability matching values is based on purely intuitive thinking and relies on conventional, insufficient procedures like opinion polls.

Sawik [5] follows a similar approach, while Asnar and Giorgini [2] developed the extended Tropos goal model, to offer a way of modeling the relationship between goals, events (risks) and treatments (countermeasures). An additionally presented taxonomy for countermeasures, which divides measures into the categories avoidance, prevention, alleviation, detection and retention serves as a tool for categorization, but not as a methodological help for the generation of proper countermeasures for identified risks.

Finally, Kayis *et al*. [12] developed the Intelligent Risk Mapping and Assessment System (IRMAS™). As the name already suggests, IRMAS is an instrument, designed to solve countermeasure selection problems, employing criteria such as costs or magnitude of risk, but is of little use for countermeasure generation.

Accordingly, there is no systematic approach for generation of countermeasures prior to selection of appropriate countermeasures at the present state.

2.2 Usability engineering and risk management process

As interaction errors between human and machine constitute a major share of serious adverse events, particularly in medical engineering [10], usability issues have a high significance in risk management. For this reason, selected extracts from DIN EN ISO 9241, DIN EN ISO 62366 and DIN EN ISO 60601-1-6 have been accounted for, during development of the method [13–15].

Indeed, usability engineering and risk management activities converge, concerning their aims and course of action. Similarities of the two standards are illustrated by Peijl *et al*. [16]. Thus activities can be parallelized and partly substituted by each other as both processes have an iterative character that starts with an initial analysis of use, respectively use-related risks (1). The next steps, defining criteria for usability/risk thresholds (2) and generating ideas for improved usability/risk control (3), are undertaken with different instruments, according to different clauses of IEC 62366 (for usability engineering) and ISO 14971 (for risk management), but with the same goal of simulating (4) and evaluating (5) the new degree of usability respectively the new residual risk after implementation of design improvements/countermeasures. The last elements of each iteration loop in IEC 62366 as well as ISO 14971, include identification (6) and evaluation (7) of new usability problems or risks, arising from implemented modifications of the foregoing steps as well, as a decision on whether to start a new iteration or interrupt and end with the usability and risk management procedure (8). Comparing the two processes, it becomes clear that UE is a means of the risk management process.

2.3 Weaknesses of current (non-systematic) practices

A common way to deal with an (intolerable) risk, is to just wait for the "eureka moment" to pop up. Though this technique is very popular, it has several disadvantages.

Firstly, it is not assured that an appropriate countermeasure will be found at all, as the outcome depends very much on the responsible persons' intuitive touch of genius and prior experiences and knowledge. Secondly, completeness of possible approaches is only unlikely achieved and the possibility that alternative countermeasures are omitted is high. This aspect is closely linked to the third reason for not relying on pure brainstorming: from a psychological viewpoint, people tend to think in continued and hardened ways, when trying to get directly from a formulated problem to an applicable solution [9]. This enhances the probability that the easiest, but not necessarily the best countermeasure is encountered. In this case, prior experience and knowledge may even have an adverse effect, as they enforce designation of popular measures that are often applied, without considering their effectiveness for the current case. As an example, teaching courses for employees are often named as potential risk reducing measures, although there might be alternative constructional safety measures, caring for inherent or protective security by improving the product's design.

2.4 Theory of inventive problem solving (TRIZ)

The present method has been developed on the basis of the inventive problem solving process by Genrikh S. Altshuller [9]. Figure 1 shows the schematic course of action, when applying the method. As the direct step from the specific problem to the specific solution is blocked by mental inertia and distorted by mental biases, mentioned above, TRIZ proposes a routine consisting of three steps to reach the desired specific solution:

1. The specific problem is raised onto an abstract level.
2. The TRIZ contradiction matrix proposes abstract solutions.
3. The abstract solutions are drilled down to gain a specific solution that is applicable to the use case.

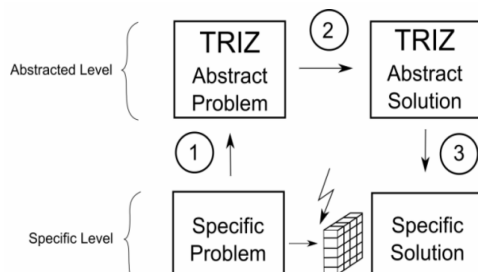

Figure 1: Problem solving process according to TRIZ.

While step one (induction) and two (deduction) require the developer's creative collaboration, step two fully relies on the knowledge, stored in the matrix.

For transferring the problem-solving concept to the field of risk management, we replace the list of abstract problems by generic risks and the list of abstract solutions by a set of principles of risk control.

3 mAIXcontrol – a new tool for countermeasure generation

To overcome the existing methodology gap, we developed a methodology, which allows systematic treatment of a particular risk in dependency of a previously identified weakness of a product or process. The method's knowledge base harks back to so far 14 risk analyses from industry and research. Core element is a two-dimensional matrix that allows different combinations of in total 61 error causes and failure modes that have been abstracted from the database, making up 1600 different possible combinations. On a superordinate level, error causes and failures are structured by terms of error taxonomy.

A given combination of two of these failure-chain elements makes reference to none, one or several abstract principles of risk control. In total, 41 different abstract principles of risk control have been acquired during evaluation of the database. As the index of the 41 principles consists only of short buzzwords, an explanatory reference work provides further detail, if necessary.

3.1 Composition of the method

After a detailed analysis of alternatives, the approach, implicating that principles of risk control be mapped as a function of error causes and failure modes turned out to be the most promising. Main reason for the final design is the insight that any harm originates from a combination of a root cause and an (unresolved) failure and that these are documented in almost any risk analysis.

As several reputable researchers have proven commutability of error cause, failure mode and consequence [17–20], we desist to make a clear distinction between root cause and failure for our application. Therefore, both elements, error causes and failure modes are mapped as coding information on the mirror-inverted axes of the matrix. We even observed the commutability of error cause and failure mode in our practical work, as we discovered several examples, where an incident that had been the failure for an upcoming adverse event, turned out to be the (root) cause for another consequence in a different risk analysis. These discoveries show that a clear distinction between (root) cause and failure is only possible in a very narrow, risk-analysis-dependent context. As we naturally secede from such a given context in our analysis-comprehensive approach, this strict distinction has been dropped.

3.2 Error taxonomy

The underlying error taxonomy for categorization of error causes and failure modes is depicted in Figure 2. Errors are attributed to the three categories

"human", "environment" and "machine". These categories have been chosen according to Bogner's Human-Machine-System Approach [11]. On a subordinated level, more detailed categories for human errors and machinery errors exist.

Human errors include slips, lapses, mistakes and basic personal skills or attitudes. According to Norman's action cycle and Rasmussen's skill, rule and knowledge SRK-based classification, human errors are filed into perception errors, cognition errors and action errors [21, 22]. Furthermore, categories from VDI 4006-2 are employed, distinguishing errors by addition from those that occur by omission or execution [11]. A category, called "psychologically rewarding behaviour" is introduced in reference to Reason [23].

Figure 2 shows some examples for the different error categories. The examples are taken from different risk analyses of our data base and can as well be found in the mAIXcontrol matrix. For that reason they bear either the character of an error cause or a failure mode.

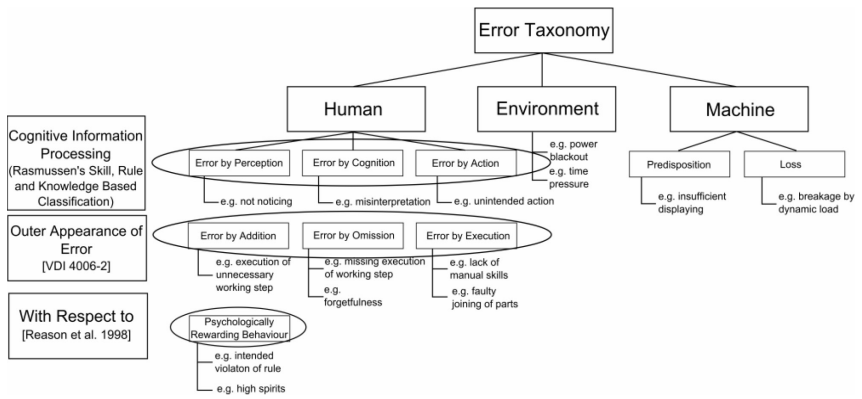

Figure 2: Error taxonomy for categorization of error causes and failure modes.

Technical errors have been divided into the two categories "predisposition" and "loss", dividing system faults that are inherent to the design of the product or process from those that emerge during the use-cycle. With other words, "loss" represents insufficiencies that become manifest in the actual (time dependent) condition of the product, while the concept of "predisposition" refers to those insufficiencies that are inherently designed into the product or process during the very early stage of development. A comparable approach for classification of technical errors was proposed by Chappelow [24].

3.3 Principles of risk control

The 41 principles of risk control have been summarized by the four categories "Established", "Creative", "Technical" and "Knowledge and Organization" (Table 1).

Table 1: Principles of risk control, divided into four categories.

Established			
[1] Compatibility	[5] Have Replacement in Store	[9] Exit Strategy	[13] Shift of Competence
[2] Repetition	[6] Maintenance	[10] Redundancy	[14] Wait for Reassurance
[3] Give Constraints	[7] Feedback	[11] Highlighting	[15] Display / Presentation /Illustration
[4] Simplicity	[8] Labeling	[12] Durability	

Technical			
[22] Discrete Adaption Mechanism	[26] Calibration at Beginning of Operation	[30] Thermal Behaviour	[34] Choice of Material
[23] Locking Mechanism	[27] Inseparability	[31] Avoid Lumen	[35] Anti-Adhesion
[24] Tender Velvet	[28] Enable Dismantlement	[32] Enable Free Movement	
[25] Accuracy of Fit	[29] Help for Assembly (Techn. Device)	[33] Alignment and Accessibility	

Creative		Knowledge and Organisation	
[16] Prevent	[20] Eliminate Disturbances	[36] Atention to Details in Instructions	[40] Expertise and Culture
[17] Overdo	[21] Resistency	[37] Check and Control	[41] Supply Patient with Information
[18] Divide / Seperate		[38] Standards	
[19] Reduce		[39] Anamnesis of Patient	

3.4 Test set-up

The method has been assessed in two trials. One test has been conducted with a test group of medical engineering students, the other with professionals from the field of medical engineering. Each time the test population has been divided into two groups who had to deal independently from each other with an exemplary problem case. While group A and B had a flexible timeframe for accomplishment of the task, group C and D have been instructed to solve the task within a period of 45 minutes. Each group had to assess the same problem case two times: once, with conventional brainstorming and a second time, with help of the methodology. In order to detect biases (such as recall biases), the order in which the groups assessed the problem case has not been the same. Free accessible expert knowledge was provided to the randomized chosen participants on the basis of an on-hand risk analysis. The underlying software-tool CARAD (Computer Aided Risk Analysis and Documentation, SurgiTAIX AG, Herzogenrath) provided further information in form of commentary text fields that could be called up by the participants during the evaluation session, if necessary. The provided information was part of a risk analysis that had been carried out at an earlier stage and not by the participants. After the assessment, participants completed a six pages questionnaire on test-level basis.

A surgical process (especially the intraoperative part) has been employed for application of the methodology during evaluation. The process comprises computer based processing of anatomical data for planning of an patient-individual mold (step 1), manufacture of the mold with a molding cutter (step 2), drill-holing and finishing of the mold (step 3), positioning and fixing to the tibia bone (step 4) and affixment of the cutting gauge to the mold (step 5).

3.5 Results and interpretation

Psychometric data in form of the questionnaires has been collected, as well as experimental results in form of proposed countermeasures that mitigate sensitive risks.

For measuring risks before and after implementation of countermeasures, we rely on a commonly used approach that measures risk by the risk priority number, which is the product of the probability of its occurrence (O), the probability of detection (D) and the severity (S) of its outcome [8]. This mathematic relation is expressed by

$$RPN = O \times D \times S \quad (1)$$

Relying on the bare number of measures for risk control according to Tables 2 and 3, the methodology shows predominance over brainstorming with a slightly deviance in the case of group C (medical engineering professionals). It is particularly noticeable that in the case of group B, the number of countermeasures, generated with the method is higher than the number generated, when using brainstorming, as the method had been used before the brainstorming here. Obviously, in this case, the benefit of the method outranges the recall effect.

Table 2 illustrates the success of the method, measured by RPN. Group A managed to reduce the total risk from 170 to 145, when working with brainstorming and twice as much (down to 120), when working with the method. In the second case, group B achieved a total risk of 135, when working with the method and 140, when working with brainstorming.

Table 2: Results from evaluation (test subjects: students medical engineering).

Test Subjects: Students Medical Engineering	Test Group A		Test Group B	
	Brainstorming	mAIXcontrol	mAIXcontrol	Brainstorming
Number of Generated Countermeasures	54	64	55	51
Required Time [in Minutes]	50	63	80	50
Countermeasures per Minute	1,08	1,02	0,69	1,02
Sum of RPN after Countermeasures (Reference Value before Countermeasures: 170)	145	120	135	140

Table 3 shows the efforts of medical engineering professionals in reducing the total risk. Risk could by lowered from 170 to 145 in a first run by group C, when using brainstorming and down to 165, when using the method. Group D finally lowered the total risk to 90, when using the method and down to 128, when relying on conventional brainstorming.

Table 3: Results from evaluation (test subjects: professionals medical engineering).

Test Subjects: Professionals Medical Engineering	Test Group C		Test Group D	
	Brainstorming	mAIXcontrol	mAIXcontrol	Brainstorming
Number of Generated Countermeasures	26	25	81	73
Required Time [in minutes]	45	45	45	45
Countermeasures per Minute	0,58	0,56	1,8	1,62
Sum of RPN after Countermeasures (Reference Value before Countermeasures: 170)	145	165	90	128

Referring to group A and B (students medical engineering), evaluation of the questionnaires shows a "slight advantage" of the method, compared to brainstorming. Although users estimate the time/benefit – ratio of the method lower than that of brainstorming, they value the higher completeness of matrix-generated results and the potential learning effect for experienced users. This makes 83% of the polled participants state that they would prefer using the method, if they were able to choose for an equivalent task.

Group C and D (professionals medical engineering) estimate an "enormous advantage" of the method, compared to conventional brainstorming. Participants estimate both time/benefit-ratios – those of the method and of the brainstorming – as equal, when rating them as "good". Participants of both groups state that they prefer the method, when having to work on an equivalent task.

The results, shown in Table 2, agree with our anticipations: Generally the method has more potential than conventional brainstorming. The method's predominance is overlaid with recall biases. In the case of group A and C, they have an amplifying effect on the method's success, whereas in the case of group B and D their impact is weakening. Still, the method's advantageousness dominates the recall biases in the case of group B and therefore, the total risk, achieved by application of the method, is still lower than what is achieved with pure brainstorming.

The results, displayed in Table 3, are highly paradoxical. For both groups, the result of their respective first attempt is more successful than their second attempt. Obviously, the participants of both groups, C and D, made little use of their memories, when assessing the risks a second time. Furthermore, group D can be seen as the stronger group, as the average results of group D show lower risks than those of group C. It has to be noted that test group C did not finish the task within the given timeframe of 45 minutes, when working with the method. This is a good argument, why the total risk priority number for that case is comparatively high.

4 Discussion

Assessing the efficiency of the method, it has to be considered that all subjects have been novice users. This implicates a higher expenditure of time. As the reference method for this study (brainstorming) does not fulfill the criteria of a regular methodical procedure, the time-dependent disadvantage is compensated by qualitative deficits of brainstorming concerning reproducibility, documentation and justification of results.

Integration of data from additional risk analyses into the mAIXcontrol matrix is a huge venture, but important for clearing white spots on the map. This would be beneficial for broader coverage of error-cause – failure-mode combinations.

Furthermore, for our classification of error types, we lack appropriate categories for technical failures. The foundation for classification of technical errors in literature is far behind the state of the art, classification of human errors has achieved. A progress in this field would be helpful for our application.

Acknowledgement

The work described has been conducted in the framework of the AiF/FQS SysRisk project, which is funded by the Federal Ministry of Economics and Technology (BMWi) under grant number 16745N.

References

[1] Reason J: Human Error, Cambridge University Press (1990)
[2] Asnar, Y., Giorgini, P.: Modelling Risk Identifying Countermeasure in Organizations, Italy, CRITIS 2006, LNCS 4347, pp. 55–66, Springer-Verlag, Berlin Heidelberg (2006)
[3] Viduto, V., Maple, C., Huang, W., López-Peréz, D.: A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem, Decision Support Systems 53 (2012) 599–610, Elsevier (2012)
[4] Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology (NIST SP800-30). Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg (2002)
[5] Sawik, T.: Selection of Optimal Countermeasure Portfolio in IT Security Planning, Decision Support Systems (2013)
[6] Washington, S., Oh, J.: Bayesian methodology incorporating expert judgment for ranking countermeasure effectiveness under uncertainty: Example applied to at grade railroad crossings in Korea, Accident Analysis and Prevention 38, 234–247, Elsevier (2006)
[7] DIN EN ISO 13485: Medical devices. Quality management systems. Requirements for regulatory purposes (ISO 13485:2003); German version EN ISO 13485:2003, Beuth Verlag GmbH, 10772 Berlin (2003)

[8] DIN EN 14971: Medical devices – Application of risk management to medical devices (ISO 14971:2000); German version EN ISO 14971:2001, Beuth Verlag GmbH, 10772 Berlin (2000)
[9] Gadd, K.: TRIZ for Engineers; Enabling Inventive Problem Solving, WILEY: A John Wiley and Sons, Ltd., Publication (2011)
[10] Leape, L.: Error in Medicine, JAMA, December 21, Vol 272, No.23 (1994)
[11] VDI 4006-2: Menschliche Zuverlässigkeit, Methoden zur quantitativen Bewertung menschlicher Zuverlässigkeit "VDI 4006-Teil2", Beuth Verlag GmbH, 10772 Berlin (2003)
[12] Kayis, B., Arndt, G., Zhou, M., Amornsawadwatana, S.: An Intelligent Risk Mapping and Assessment System (IRMAS™). A Risk Mitigation Methodology for New Product and Process Design in Concurrent Engineering Projects Annals of the CIRP Vol. 56/1/2007 Elsevier (2007)
[13] DIN EN 62366: Medical devices – Application of usability engineering to medical devices (IEC 62366:2007); German version EN 62366:2008, VDE VERLAG GMBH, 10625 Berlin (2008)
[14] DIN EN 60601-1-6: Medical electrical equipment – part 1–6: general requirements for basic safety and essential performance – collateral standard: usability (60601-1-6:2007); VDE VERLAG GMBH, 10625 Berlin (2007)
[15] DIN EN ISO 9241-110: Ergonomics of human-system interaction – Part 110: Dialogue principles (ISO 9241-110:2006); German version EN ISO 9241-110:2006, Beuth Verlag GmbH, 10772 Berlin (2006)
[16] Peijl v.d. J., Klein, J., Grass, C., Freudenthal, A.: Design for risk control: The role of usability engineering in the management of use-related risks. J Biomed Inform (2012)
[17] Hollnagel, E.: Reliability and safety analysis: Context and control. London: Academic. Reliability Engineering & System Safety Volume 52, Issue 3, pages 327–337 (1996)
[18] Sutcliffe, A., Rugg, G.: A Taxonomy of Error Types for Failure Analysis and Risk Assessment, International Journal of Human-Computer Interaction, 10(4), 381-405 (1998)
[19] Käppler WD: Menschliche Fehler als Unfallursachen: Untersuchungen und Ergebnisse mit ARIADNE. In: Grandt, M. (Ed.) Verlässlichkeit der Mensch Maschine-Interaktion: Deutsche Gesellschaft für Luft- und Raumfahrt e.V. Report 04-03, Bonn, S. 197-212 (2004)
[20] Rasmussen, J.: Reasons, causes and human errors. In J. Rasmussen, K. Duncan, and J. Leplar (JEds.), A New technology and human error (pp. 53-61). Chichester: Wiley (1987)
[21] Rasmussen, J.: Skills, rules, knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man and Cybernetics, 13, 257-266 (1983)
[22] Norman, D. A.: The Design of Everyday Things. New York, Doubleday/Currency Ed (1983)
[23] Reason, J., Parker, D. Lawton, R.: Organizational Controls and Safety: The Varieties of Rule-related Behaviour. Journal of Occupational and

Organizational Psychology, The British Psychological Society, 71, 289-304 (1998)
[24] Chappelow, J.: The Risk of Human Error: Data Collection, collation and Quantification. Paper presented at the RTO HFM Workshop on "The Human Factor in System Reliability – Is Human Performance Predictable?", held in Siena, Italy, 1-2 December 1999, and published in RTO MP-032 (2000)