International Conference on Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS, 2008

Different Approaches for Probability of Common Cause Failure on Demand Calculations for Safety Integrity Systems

Josef Börcsök[1, 2]
[1] *Computer Architecture and System Programming*
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel
GERMANY
[2] *HIMA Paul Hildebrandt GmbH + Co KG*
Albert-Bassermann-Str. 28, 68782 Brühl
GERMANY
j.boercsoek@uni-kassel.de,
j.boercsoek@hima.com

Peter Holub[1, 2]
[1] *Computer Architecture and System Programming*
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel
GERMANY
[2] *HIMA Paul Hildebrandt GmbH + Co KG*
Albert-Bassermann-Str. 28, 68782 Brühl
GERMANY
holub@uni-kassel.de, p.holub@hima.com

Abstract

The common cause failures (ccf) are the biggest part when calculating the probability of failure for redundant safety integrity systems. A ccf can occur, when a random hardware failure leads to a failure of several components. There are several methods to calculate the probability of ccf. Three models will be shown in this paper, with the help of which the beta-factor will be calculated. The ccf ratio for the calculation of the overall probability of failure is defined with the beta-factor.

1. Introduction

A safety-related system that fulfils functional safety requirements reduces the risk, which comes from the equipment under control, EUC, i.e. a refinery, with its about 100 km long pipeline networks and the existing integrated pumping stations. The danger for people, environment or machine via a EUC will be appraised through a risk analysis, e.g. with the help of a risk graph, a fault tree analysis, a Markov analysis or with a semi-quantitative method such as LOPA (layer of protection analysis). How small the residual risk shall be will be defined, on the one hand, by the organisation itself – at this point each individual will ask himself whether he is ready to accept that risk or not – and, on the other hand, will be influenced by the production availability. Since a system, which is first and foremost planned to make money, shall best always be running, even if, thereby, a bad risk will have to be accepted. The art of the engineer consists then in implementing appropriate safety architectures, which would permit reducing the conflict between the requirements according to high safety, equivalent with small residual risk, and high production availability, which exists in most of the systems implemented up to now. The optimised safety system offers an architecture having the two following criteria:

- The safety system has a hardware-fault-tolerance of equal or greater to two. It means that the equipment under control EUC- system, will run to a safe state after at least two faults in the safety system has occur.[1] Thereby the production availability will be guarantee.
- In safety systems two independent channels must always exist, which properly function so that, if in one or several channels dangerous failure occur, the EUC system will be driven in a safe state. These criteria guarantee the safety.

The 2oo4-architecture is one possible system architecture having these criteria.
The disadvantages of such a redundant structure, which by mono channels structures, with which a very small residual risk can definitely be achieved, do not occur according to the construction, are however:

- A higher Grad of the Design – this will have at a later stage, consequence during the assembling,

[1] A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function [1].

the commissioning and the maintenance of the system.

- The observance and valuation of an additional failure source, the so-called common cause failure (ccf), during the risk analysis.

This ccf, which by mono-channel structures do not occur according to the construction, constitute for redundant structures the main part of safety integrity systems (SIS) during the calculation of the probability of failure on demand. However this does not mean, that mono-channel systems, due to the not existing ccf, have a smaller failure probability. On the contrary, through the ccf one part of the failures, which also occur in mono-channel systems, will be evaluated with a weighted factor smaller as one. Should a ccf occur, the whole architecture will be affected. Whereas in mono-channel systems, only single failures (also called normal failures) can occur, failures in a redundant system can be divided in single and ccf, see figure 1 [1], [4]. Another often used presentation is shown in figure 2. Here both individual channels' single failures make the failures'intersection in a redundant system. Those are the ccf [1], [5], [6]. The evaluation of the ccf depends on the chosen model. Hence in this paper different models will be presented and the results will be compared with one another after calculating the failure probability.

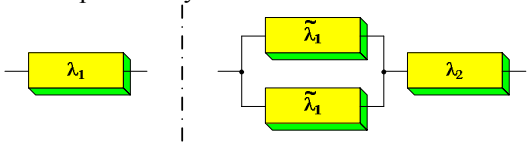

Figure 1. Reliability block diagram for a single channel (left) and a redundant system architecture (right). λ_1 and $\tilde{\lambda}_1$ are single failure rates, λ_2 = ccf rate.

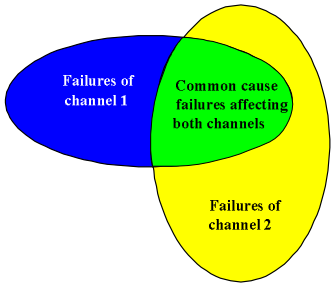

Figure 2. Relationship between single failures and ccf in a redundant system [1], [2], [5].

2. Definition of CCF

The term ccf was only clearly defined in the mid-80s, after the term "dependent failure "was introduced. A dependent failure means a failure, which occurs simultaneously in at least two systems coupled together. Thereby the occurrence probability of a dependent failures doesn't depend on the product of each single system' s failure probability, but barely on the conditional probability, that a failure occurs when both systems are coupled together, i.e. are functionally connected. With the introduction of the terms dependent failure the terms common cause-, common mode- and cascade failure could be clearly defined [5], [8], [9], [10], [11]. The definitions of these terms are gathered in Table 1.

Table 1. Definition of dependent failures [11], [5].

Dependent Failure	The probability of a group of events which probabilities cannot be expressed as a simple product of unconditional probability of failure of single components.
Common Cause Failure	This is a kind of dependent failure which occurs in redundant components in which a single common cause - simultaneously or near simultaneously- leads to failures in different channels.
Common Mode Failure	This definition applies to failures of common causes in which multiple elements fail similarly in the same mode.
Cascade Failure	These are all dependent failures that do not share a common cause, meaning they do not affect redundant components.
Additionally: The definition of „dependent failures" includes all definitions of failures that are not independent. This definition of dependent failures clearly implies that an independent failure in a group of events can be expressed as a simple product of conditional probabilities of failures of a single event.	

Common mode failures are therewith a sub-group of the ccf. Cascade failures count among all depending failures, which occurred in a series of reaction, caused through the failure of a single component. In the following part, only the ccf will be taken into account, according to the description from 1976 [12], [13]:

A ccf „*is an event having a single external cause with multiple failure effects which are not consequences of each other*".

2.1. Systematic and random Failures

In all standard frequently used to functional safety one finds the classification of failures in systematic and random failures. However, one starts making differences, because further classifications use a different terminology. A correlation of different concepts out of [1], [2] und [3] is gathered in figure 3.

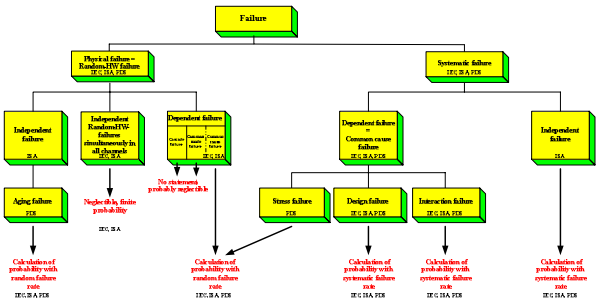

Figure 3. Failure classification, according to [1], [2], [3].

A random hardware failure means (according to Def. out of [1]) a „*failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.*" A systematic failure will be in [1] defined as a "failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors".

Should random hardware failure exist, it is possible to consider the probability with the help of random failure rates and to calculate the probability of failure. Systematic failures exist continuously in a system. They depend on special event, such as function processes and environmental conditions. The occurrence probability cannot be calculated with methods to define the probability but at the most, generally very inexactly and subjective averaged. To guarantee the functional safety, random as well as systematic failures will have to be control or prevent from happening. There, amongst others, a systematic and controlled developed process will be used as well as the use of guaranteed safety principles during the design and the realisation. Failure tolerance, automatic fault detection and the ability when acknowledging a failure to react are part of it.

As long as one deals with hardware failures [1], [2], [3] synonym concepts, such as physical failure, independent failure [2] or aging failure [3] can be found in the Norms

For the concept common cause failure it will be a bit more complicated. Generally assumed is the fact that dependent failures are ccf. Depending on the cause of a ccf, a ccf can present a systematic failure [1], [2], [3] as well as a random hardware failure [1], [2]. To the ccf as systematic failures belong stress failure [3], design failure [1], [2], [3] and interaction failure [1], [2], [3]. Here attention should be paid to the fact that the stress failure in [1] and [2] can be caused through physical failure and thereby belong to the random hardware failures. Hence in [1] and [2] the ccf caused though stress can be calculated with the help of a random hardware failure rate. Should however ccf exist in form of design failures or interaction failures, then they will be detected via the Life-cycle-management system, which is in [1], one of the central points during the evaluation of functional safety. In order to calculate design or interaction failures In [2] and [3], one will introduce an additional Parameter for the systematic failure rates. This Parameter can however only be averaged after long-time experience and the results are thus not always comparable, if the relevant data are unknown! For the random hardware failure rate however exist worldwide databank with comparable values, see [14] - [17], whereupon attention must also be paid for environmental conditions whose values account. Mentionable is, that in [3] the stress failures can also be calculated with the help of random hardware failure rate.

In the following models the relevant data, which are the cause of ccf physical failures, and that therefore the probability of failure of ccf can be calculated with the help of random hardware failure rates.

3. Basic Beta-Factor Model

The Basic Beta-Factor Model, which has already been introduced in 1974 by K. N. Fleming [7], describes the correlation between the independent, random hardware failures and the dependent failure, of the ccf, in a redundant system. Thereby the following data are relevant:

- The redundant system consists of identically constructed redundant components.
- The ccf find its origins in a physical failure, which can be described with a method of probability, the random hardware failure rate.

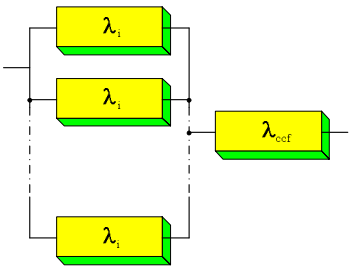

Figure 4. Reliability block diagram for a redundant structure with ccf component.

With the help of a checklist, given as an example in [5], [7], [8] or [18], criteria for the occurrence of can be evaluated, in order to define a value for the beta-factor. In [1] - [8] the following eight criteria are listed: 1. separation, 2. similarity/diversity, 3. complexity/design, 4. assessment/analysis, 5. procedures, 6. training, 7. control and 8. test.

Should any criteria be evaluated, then the process described in [5] or [18] is used:

- Identify the total failure rate for the device from published or internal data
- Review the failure modes to determine the portion that is expected to have a common cause affect
- Calculate/estimate the percentage of the failure rate that can be associated with the beta-factor.

The calculated values for the beta-factor averages ca. over 0 and 25 % [5],[18].

Once the beta-factor has been defined, then the ratio of the independent failure λ_i divided by

$$\lambda_i = (1-\beta)\cdot\lambda \qquad (1)$$

and the ratio for ccf λ_{CCF} divided by

$$\lambda_{CCF} = \beta\cdot\lambda \qquad (2)$$

with

$$\lambda = \lambda_i + \lambda_{CCF} \qquad (3)$$

will be determined.

The general valid equation for the failure probability will be calculated for n redundant channel out of the sum of the failure probabilities PFD_{single} for single failure and PFD_{CCF} for ccf:

$$PFD = PFD_{\text{single}} + PFD_{CCF} = \left[(1-\beta)\cdot\lambda\cdot t\right]^n + \beta\cdot\lambda\cdot t \qquad (4)$$

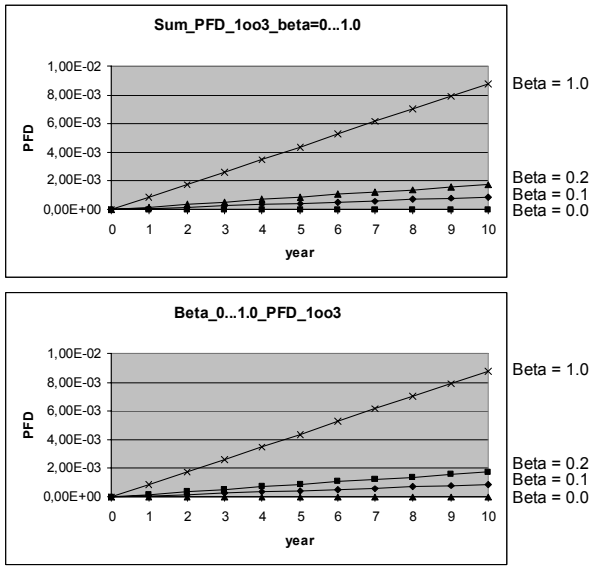

Figure 5. PFD-value for 1oo3-architecture. Top: Overall-PFD-value in accordance with equation (4); Bottom: only the ratio PFD_{CCF}

A derivation of this equation can be found for example in [6]. Should for example a 1oo3-system with n = 3 redundant components exists, then the diagram calculated in figure 5 will be obtained. Thereby is assumed that the beta-factor varies between 0 and 1.0, a basic failure rate from λ = 1E-07 1/h and a time interval t, that averages between 1 and 10 years.

The calculation shows – as it can also be seen in figure 5 – that it is necessary to take the CCF into consideration, as well as the fact that the PFD_{CCF}-ratio is clearly bigger than the PFD_{single}. A Beta = 0.0 means, that an ideal redundant exist, in which no ccf occur. This is unrealistic in practice! However, if one give Beta = 1.0 in eq. 4, one obtains the probability of failure for a 1oo1-System. Therefore, as a comparison, the upper curve (Beta = 1) shows how, despite ccf, the introduction of a redundant system improves the PFD-value. Eq. 4 shows, that the PFD-Value for ccf does not depend on the amount of redundant components. The graph in fig. 5 underneath is therewith generally valid for redundant architecture, see fig. 4.

4. Beta-Model according to IEC 61508 and ISA TR84.00.02

The following beta-model will be described in both Standards. Thereby one must pay attention by ISA TR84.00.02, described with the abbrev. ISA in the following part, since approximation formulas are used at different places, which could lead during a wrong application to far too optimistic results.

The basis failure rate λ_B consists, in accordance with both norms, of safe and dangerous failure rates. To calculate the probability of failure only the latter dangerous failure rates are relevant [19]. Should automatic diagnostics tests be implemented in the safety-related system, then one part of the dangerous failure can be detected, the other part remains dangerous undetected. Both standards describe a CCF-Model, in which a ccf can occur via dangerous detected as well as dangerous undetected Random Hardware failure. This is the reason why in this Model both a beta-factor β for the dangerous undetected and a beta-factor β_D for the dangerous detected failures is required. Both beta-factors can be calculated via a checklist with variables and the formula given in the standards.

The correlation between these two beta-factors should be shown as an example for a 1oo2-system. The equation for the probability of failure of a 1oo2-system is (derivation s. [5]):

$$P(t) = P_1(t)\cdot P_2(t) + P_{DUC}(t) + P_{DDC}(t) \qquad (5)$$

Thereby the product for both single failure probabilities P_1 and P_2 is the probability of failure of independent single faults for the system. Both additive terms P_{DUC} and P_{DDC} make the ccf-ratio.

As for the simple basic beta-model the ccf-ratio is also here for the probability of failure the clearly

bigger term and – at least by the logic solver of a safety-related system – at least twice as big as the probability of failure of the single fault. The PFD_{avg}-equation for the ccf-ratio via dangerous undetected failures is [1], [2], [5]:

$$PFD_{avg,\,\beta\,DU} = \beta \cdot \lambda_{DU} \cdot (T_1 + MTTR) \qquad (6)$$

and for the ccf-ratio via dangerous detected failures:

$$PFD_{avg,\,\beta\,DD} = \beta_D \cdot \lambda_{DD} \cdot MTTR \qquad (7)$$

Eq. 6 describes the probability of failure for dangerous undetected failures during the Interval [T_1 + $MTTR$], i.e. in the span of time of the proof test interval T_1 and the mean time to repair $MTTR$. eq. 7, however, describes that during the mean time to repair $MTTR$ – within this time a system's redundancy is not given and herewith intersections' comparisons of test values via equipment diagnosis are not possible – also a safety related risk occurs via the dangerous detected failure. As a consequence a probability of failure for the safety related system occurs. Both equations 6 and 7 apply in accordance with [1] and [2] not only for a 1oo2-architekture, but also for any redundant architecture.

Figure 6 presents the PFD-Value for ccf, which is the result of the sum of equations 7 and 8. In order to compare figure 5 with 6, the same values for the failure rate λ_D and the interval (now described as proof test interval T_1) have been chosen. $MTTR$ is assumed with 8 h. For both beta-factors β and β_D the following values will be used (presented in pairs: (0 // 0), (0.1 // 0.05), (0.2 // 0.1) and (1.0 // 1.0). The DC-value, which is described by the diagnostic coverage, has the value 90 %.

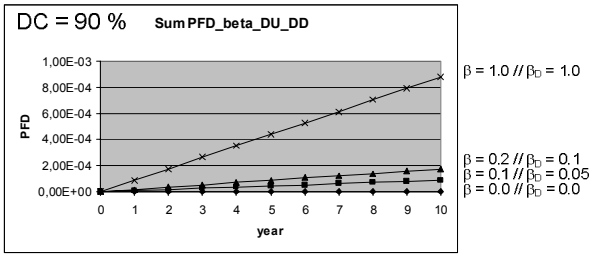

Figure 6. PFD-value for PFD_{CCF} for β and β_D according to IEC 61508 and ISA TR84.00.02

The statement for the basic-beta-model, underneath figure 5, also apply for the beta-model in accordance with IEC 61508 and ISA TR84.00.02. Through the determination of the beta-factor in β and β_D to determine the ccf, which will be caused through λ_{DU} and λ_{DD}, the probability of failure will be reduced depending from the DC-factor compared to the basic beta-model. Should any diagnosis (DC = 0) exist, then both model are identical.

5. PDS-Beta-Model PDS

As a basis for the PDS-beta-model – PDS is the Norwegian acronym for „reliability of computer-based safety systems" – the beta-model is applied in accordance with IEC 61508. The PDS-model, described in details in [3], extended the beta-factor from the IEC to the factor C_{MooN}. MooN means, that at least M out of N redundant components have to work properly, in order to perform correctly the safety function. Through this factor, called configuration factor, the influence of the architecture, which has been chosen for a safety system, will be taken into account. In the IEC there is only one beta value for all architectures and thereby no differences will be made concerning the ccf in a 1oo2, 2oo3 or 2oo4-System. However, the practice [3] has shown that one must distinguish, whether the ccf in two, three or even more components of a redundant systems occur. The beta-factor in PDS-beta-model means therefore:

$$\beta_{MooN} = C_{MooN} \cdot \beta \quad \text{with (M < N)} \qquad (8)$$

In [3] and [20] the non-trivial derivation is given to define the C_{MooN}-value. The Parameter β will still be defined with the help of the above mentioned criteria and checklists. A summary of the values calculated in [3] is given in table 2.

Table 2. C_{MooN}-factor for different architectures according [3], a summary.

N \ M	M = 1	M = 2	M = 3
N = 2	$C_{1oo2} = 1.0$	---	---
N = 3	$C_{1oo3} = 0.3$	$C_{2oo3} = 2.4$	---
N = 4	$C_{1oo4} = 0.15$	$C_{2oo4} = 0.75$	$C_{3oo4} = 4.0$

The PFD-equation for ccf considering the configuration factors is then:

$$PFD_{CCF,PDS} = C_{MooN} \cdot \beta \cdot \lambda \cdot t \qquad (9)$$

Figure 7 presents the graph of the PFD_{CCF}-value for the 2oo4-architecture. The values for the 1oo2-System correspond to the values, which have been calculated with the IEC-Beta-Model, if the β_D-ratio = 0 is. Because $C_{2oo3} > C_{1oo2}$ is, the PFD-values for a 2oo3-System are twice as worse. For a 1oo3- and 2oo4-System it is the contrary: The PFD-value for these Systems are better as the PFD-value of a 1oo2-Systems.

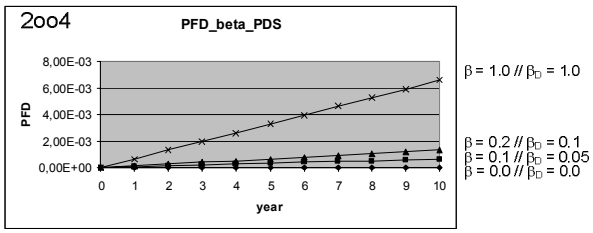

Figure 7. PFD-value for PFD_{CCF} for β according to PDS-Beta-Model

6. Conclusion

In this three different beta-Models have been compared to one another to calculate the probability of failure of ccf. Compared to the basic beta model, one can also with the IEC/ISA beta model evaluate and calculate the failure of probability, which can be caused through dangerous detected failures. Further in Step with actual practice to calculate the probability of failure for ccf is the PDS beta model. Here, during the calculation of probabilities of failure, the architecture will be taken into account with the help of the configuration-factors. Thereby ccf, which do not exist in all components but only between single components, can be evaluated. The PDS-beta model does not take into account, that also detected dangerous failures at some precise time, e.g. during the repair-time of redundant systems, can cause a safety critical ccf. Consider these failures in an extended PDS-Beta-Model will be part of another further task.

10. References

[1] IEC 61508, *International Standard 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission, Geneva, 2000.

[2] ISA-TR84.00.02-2002, *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL)*, ISA - The Instrumentation, Systems, and Automation Society, North Carolina, 2002.

[3] SINTEF, *Reliability Prediction Method for Safety Instrumented Systems*, SINTEF Technology and Society, Trondheim, Norway, 2006.

[4] D. J. Smith, *Reliability, Maintainability and risk*, Elsevier Buuerworth Heinemann, 7th ed., Amsterdam, 2007.

[5] J. Börcsök, *Functional Safety*, Hüthig, 2007.

[6] M. Rausand and A, Hoyland, *System Reliability Theory, Models, Statistical Methods and Applications*, Wiley-Interscience, 2nd ed., Hoboken, New Jersey, 2004.

[7] K. N. Fleming, "A Reliability Model for Common Mode Failures in Redundant Safety Systems", *General Atomic Report*, GA-13284, Pittsburgh, PA, 1974.

[8] P. Humphreyes, B. D. Johnston, "Dependent Failure Procedure Guide SRD-R-418", *United Kingdom Atomic Energy Authority*, Safety and Reliability Directorate, 1987.

[9] EPRI NP-3837, "A Study of Common Cause Failures. Phase 2: A Comprehensive classification System for component fault analysis.", *Los Alamos Technical Associates, Inc.*, 1985.

[10] B. D. Johnston, J. Crackett, "Common Cause Failure Reliability Benchmark exercise. SRD-R-383", *United Kingdom Atomic Energy Authority*, Safety and Reliability Directorate, 1985.

[11] G. Mauri, "Integrating Safety Analysis Techniques, Supporting Identification of Common Cause Failures", Doctor of Philosphy thesis, University of York, Department of Computer Science, 2000.

[12] "Task force of the IEEE APM subcommittee - Common mode forced outages of overhead transmission lines", *IEEE Trans. on Power Apparatus and Systems*, PAS-95, 1976

[13] R. Billinton, R. N. Allan, *Reliability Evaluation of Engineering Systems, Concepts and Techniques*, 2nd ed., Plenum Press, New York, London, 1992.

[14] CNET, RDF 93, *Recueil de Données de Fiabilité des Composants Electroniques*, Lannion, CENT, 1993 British Telecom Rel. HDBK HRDS and Ital-tel Rel. Pred. HDBK IRPHB93, 1993.

[15] IEC 61709, *Electronic Components Reliability-Reference-Condition for Failure Rates and Stress Models Conversions*, International Electrotechnical Commission, Geneva, 1997.

[16] MIL HDBK-217, *Reliability Prediction of Elec. Equip.*, Ed. F, 1991, Not. 2, 1995.

[17] Siemens, SN 29 500, Ausfallraten Bauelemente, München, Siemens 1991, bzw. DIN 40039, 1988.

[18] A. E. Summer, K. A. Ford, G. Raney, "Estimation and Evaluation of Common Cause Failures in SIS", *Chemical Engineering Progress*, Houston, 1999.

[19] J. Börcsök, P. Holub, M. H. Schwarz, "How safe is my system - Calculation of PFD-Values for a safety related System", IEEE conference, Martinique, 2007.

[20] P. Hokstad, "A Generalisation of the Beta Factor Model", *Probabilistic Safety Assessment and Management*, Proceedings from PSAM7-ESREL '04, Springer 2004.