ELECTRONIC JOURNAL
OF INTERNATIONAL GROUP
ON RELIABILITY

JOURNAL IS REGISTERED
IN THE LIBRARY
OF THE U.S. CONGRESS

●

ISSN 1932-2321

●

VOL.1 NO.1,
MARCH, 2008

Gnedenko Forum Publications

Reliability & Risk Analysis Theory & Applications

№2
2008

Special Issue # 2 on SSARS 2007

Invited Editors E. Zio and K. Kołowrocki

San Diego

ISSN 1932-2321

http://www.gnedenko-forum.org/Journal/index.htm

Journal of International Group on Reliability

RELIABILITY & RISK ANALYSIS: THEORY & APPLICATIONS

Vol.1 No.2,
June, 2008

Special Issue # 2 on SSARS 2007

Invited Editors E. Zio and K. Kołowrocki

San Diego
2008

Journal Council

Send your paper

e-Journal ***Reliability: Theory & Applications*** publishes papers, reviews, memoirs, and bibliographical materials on Reliability, Quality Control, Safety, Survivability and Maintenance.

Theoretical papers have to contain new problems, finger practical applications and should not be overloaded with clumsy formal solutions.

Priority is given to descriptions of case studies.

General requirements for presented papers

1. Papers have to be presented in English in MSWord format. (Times New Roman, 12 pt , 1.5 intervals).
2. The total volume of the paper (with illustrations) can be up to 15 pages.
3. A presented paper has to be spell-checked.
4. For those whose language is not English, we kindly recommend to use professional linguistic proofs before sending a paper to the journal.

* * *

The Editor has the right to change the paper title and make editorial corrections.

The authors keep all rights and after the publication can use their materials (re-publish it or present at conferences).

Publication in this e-Journal is equal to publication in other International scientific journals.

Papers directed by Members of the Editorial Boards are accepted without referring.

The Editor has the right to change the paper title and make editorial corrections.

The authors keep all rights and after the publication can use their materials (re-publish it or present at conferences).

Send your papers to

the Editor-in-Chief ,
Igor Ushakov
igorushakov@gmail.com

or

the Deputy Editor,
Alexander Bochkov
a.bochkov@gmail.com

Table of Contents

analysis. The paper concludes by exploring the potentiality of the above methodology in providing a robust and flexible evaluation framework suitable to the characteristics of a hazard evaluation problem.

We have already examined the worldwide trends for outcomes (measured as accidents, errors and events) using data available for large complex technological systems with human involvement. That analysis was a dissection of the basic available, published data on real and measured risks, for trends and inter-comparisons of outcome rates. We found and showed how all the data agreed with the learning theory when the accumulated experience is accounted for. Here, learning includes both positive and negative feedback, directly or indirectly, as a result of prior outcomes or experience gained, in both the organizational and individual contexts. Our purpose here and now is to try to introduce some predictability and insight into the risk or occurrence of these apparently random events. In seeking such a general risk prediction we adopt a fundamental theoretical approach that is and must be testable against the world's existing data. Comparisons with outcome error data from the world's commercial airlines, the two shuttle failures, and from nuclear plant operator transient control behaviour, show a reasonable level of accord. The results demonstrate that the risk is dynamic, and that it may be predicted using the MERE learning hypothesis and the minimum failure rate, and can be utilized for predictive risk analysis purposes.

The existing ports are expected to handle ships bigger than those for which they were designed. The main restriction in serving these ships is the depth of port waters, which directly affects the safety of a manoeuvring ship. The under keel-clearance of a ship in the port water area should be such that a ship moves safely. In some specific conditions it happen the ship strike the sea bottom. The undesired impact against the ground can damage the ship hull. The paper presents the algorithm of ships movement parameters during contact with the ground

This paper discusses a proposal for a risk management tool for applications to risk reduction of natural hazards.

The analysis of field lifetime data is much more complicated than the analysis of the results of reliability laboratory tests. In the paper we present an overview of the most important problems of the statistical analysis of field lifetime data, and present their solutions known from literature. When the input information is partial or imprecise, we propose to use interval arithmetics for the calculation of bounds on reliability characteristics of interest. When this information can be described in a more informative fuzzy form, we can generalize our interval-valued results to their fuzzy equivalents.

Telecommunication systems become a key component of critical infrastructure. One of the main elements of such systems is computer system. The organizations which can be involved in crisis management (e.g. government agencies, etc.) need to know results of security drawbacks in their systems. Moreover, they should have a tool for analysing the results of decision made in security context. And often the following question is raised: why do security systems fail? To answer it in this paper the aspects of reliability are discussed. From this point of view the security systems are analysed. We hope that thanks to such approach we will be able to reach some characteristics of security incidents occurrence. Moreover, we hope to use our results to build security attributes metrics. In addition, we present thesis that predictions of occurrence of incidents is impossible, so we should focus on registration of incidents type. On such a foundation we can formulate conclusions about drawbacks in configurations or administration of information systems. In our research we have observed that in case of some class of information systems, the availability incidents are the most dangerous. And we conclude that only using technologies with good reliability characteristics can lead to solving this problem.

Present stability regulations developed over the years by IMO reached definite conclusion with the adoption of the Revised Draft of the Intact Stability Code. The criteria included there are design criteria of the prescriptive nature, based mainly on statistics of stability casualties. Currently IMO is considering development of criteria based on ship performance. Concept of such criteria is, however, at present not agreed. The criteria are working comparatively well with regard to the majority of conventional ships, however advent of very large and sophisticated ships of non-conventional features caused that those criteria may be inadequate. The author advances the idea consisting of application of safety assessment and risk analysis using holistic and system approach to stability. Safety against capsizing (or LOSA accident) is a complex system where design, operational, environmental and human factors have to be taken into account. Although this seems to be a very complex task, in the opinion of the author it may be manageable and could be applied for safety assessment of highly sophisticated and costly ships.

This talk is based on the Editorial of IEEE Transactions on Reliability, December, 2006 and discusses a framework for applying reliability principles and practices to the emerging nano technology fields.

Both organization and individuals deal with and manage knowledge. Considering the basic approach, we distinguish two principal clusters: tacit and explicit knowledge. The knowledge management is targeted at making the organization knowledge operation more effective and providing the right people with relevant information at the right time. Knowledge and information uncertainty components have become one of crucial assets of any company or organization. Their crucial potential consists in smart knowledge management handling, proficiency and art to fit the risky market needs better than competitors.

Climatological measurements for the assessment of snow loads on structures as practiced in Slovakia are discussed in the light of methodologies described in the relevant backgrounds to Eurocodes. The database of yearly snow load maxima based on the weekly measurements of water equivalent of snow cover on 660 rain-gauge stations in Slovakia recorded during the last 52 winter seasons is analysed. Special interest is focused on the influence of heavy snowfalls in the winters 2004/2005 and 2005/2006, particularly on the extreme cases observed.

The article presents a control system of ship motion in situations threatening with collision. The goal of the presented system is to support the navigator in decision making, with possible full replacement of his work in the future. In this article, it was introduced a system joining work of two computer techniques, evolutionary algorithms to marking of optimum path of passages and a fuzzy logic to control ship after set path of passage. The introduced system has to assure safe trip of a ship in any navigational conditions with regard of weather conditions and met navigational objects of static or dynamic nature. For testing of the operation, the system and the marine environment a simulator was used to present navigational situations in a 3D graphical mode at the poor hydro-and-meteorological conditions.

This article analyses the traffic accident rate on roads and highways and possibilities of risk evaluation related to traffic accident occurrence based on factors that were the causes of accidents. A new term – risk of traffic accident occurrence is a product of probability of accident occurrence and its impacts. The results are presented by way of example that uses selected statistical data of the Czech Republic traffic accident rate between 1993 - 2001. The article provides a brief methodological procedure of evaluation of the traffic accident rate using the risk of traffic accident occurrence.

The paper is focused on adaptation of an isochrones method necessary for application to a weather routing system with evolutionary approach. Authors propose an adaptation of the isochrones method with area partitioning assuring that the route found by the adopted method would not cross land. In result, when applied to a weather routing system with evolutionary approach, this proposal facilitates creation of initial population, resulting with routes of reduced collision risk and low costs of passage.

A ship, as an object for course control, is characterised by a nonlinear function describing the static manoeuvring characteristics. One of the methods, which can be used, for designing a non-linear course controller for ships is the backstepping method. It was used here for designing the configurations of non-linear controllers, which were then applied for ship course control. The parameters of the obtained non-linear control structures were tuned to optimise the operation of the control system. The optimisation was performed using genetic algorithms. The quality of operation of the designed control algorithms was checked in simulation tests performed on the mathematical model of the tanker completed by steering gear.

This paper analyzes the behaviour of a fuzzy expert system for evaluating the dependence among successive operator actions, through a sensitivity analysis on the fuzzy input partitioning and assessment. Preliminary results are presented with respect to a case study concerning two successive tasks of an emergency procedure in a nuclear reactor. Work is in progress to perform a thorough sensitivity analysis to generalize the results obtained.

In this paper, recently introduced topological measures of interconnection and efficiency of network systems are applied to the safety analysis of the road transport system of the Province of Piacenza in Italy. The vulnerability of the network is evaluated with respect to the loss of a road link, e.g. due to a car accident, road work or other jamming occurrences. Eventually, the improvement in the global and local safety indicators following the implementation of a road development plan is evaluated.

Guest Editorial

The papers collected in these 2 issues are works presented at the 1st Summer Safety and Reliability Seminars, SSARS 2007, held in Gdansk/Sopot, Poland, from 22nd of July 2007 until 29th of July 2007.

The Seminar was attended by 46 participants from 14 countries (Canada, Czech Republic, Germany, Greece, Italy, Lithuania, Netherlands, Poland, Portugal, Slovakia, South Africa, South Korea, Tunisia, United States).

The motivation behind this annual event series is to provide a forum for discussing, advancing and developing methods for the safety and reliability analysis of the complex systems and processes, which form the backbone of our modern societies. The subjects of the Seminars are chosen each year by a Program Board of selected experts in an effort to dynamically represent the methodological advancements developed to meet the newly arising challenges in the field of safety and reliability analysis.

This year the emphasis was addressed to the following subjects:

- Natural Hazards Analysis and Environment Protection Modeling;
- Reliability and Safety Data Collection and Analysis;
- System Safety and Reliability Modeling, Dependence, Dynamic Reliability;
- Risk Assessment and Management;
- Maintenance Modeling and Optimization.

Both 1-2 hours lectures on advanced methods and technical presentations of 20-30 minutes on applications of such methods were offered during the plenary sessions and the seminar sessions, respectively.

The Advisory, Editorial and Organizing Boards have carried out the preliminary evaluation of the 52 contributions selected for this year Seminars and sent out recommendations to the authors for improving their work.

The extended abstracts of all lectures and technical papers were collected in the SSARS Proceedings, which constitute an up-to-date reference textbook for the participants to the Seminars and all the researchers in the field.

The 43 papers and lectures presented at SSARS 2007 are presented in the two special issues of the Journal, grouped into a System Safety, Reliability and Maintenance Modeling Section and a Natural Hazards and Risk Assessment and Management Section.

Guest Editors
Krzysztof Kołowrocki, Enrico Zio
SSARS 2007 Chairmen

In memory of Sergei Antonov

Sergei ANTONOV
(1960-2006)

Graduated from Math Dept of Moscow State University.

Worked at Russian Academy of Sciences. Master of sport in alpinism. Multiple champion of alpinism of Moscow and Russia.

One of the first member of GNEDENKO FORUM, made number of joint projects with I. Ushakov.

Sergei died in Pamir mountains during climbing.

SPARE SUPPLY SYSTEM FOR WORLDWIDE TELECOMMUNICATION SYSTEM GLOBALSTAR

**Igor Ushakov, Sergei Antonov, Sumantra Chakravarty,
Asad Hamid, Thomas Keliinoi**

In memory of Sergei Antonov

ABSTRACT

This work describes the Optimal Spare Allocator (OSA), a software tool for Globalstar, which is a worldwide satellite telecommunication system designed at QUALCOMM (San Diego, USA). The Globalstar spare supply system is hierarchical and has three levels: Central Spare Stock (CSS), Regional Spare Stocks (RSS) and On-Site Spare Stocks (OSS). The tool allows solving direct and inverse problems of optimal redundancy. The OSA computer model has a user-friendly interface and a convenient reporting utility.

KEYWORDS

Spare allocation, reliability, optimization, cost, software tool, steepest descent algorithm

GENERAL DESCRIPTION OF THE SPARE SUPPORT SYSTEM

We consider a hierarchical spare supply system for satellite telecommunication system, the Globalstar. Globalstar is expected to have a number of base stations (gateways) dispersed all over the world. Successful operation of such a complex system depends on the ability to perform fast restoration of its operational ability after a failure. Fast and effective gateway restoration after a failure depends on a stock of field replaceable units (FRU). For this purpose, a hierarchical spare supply system (HSSS) is being designed (Ushakov 1994). HSSS includes the central spare stock (CSS), regional spare stocks (RSS), and on-site spare stocks (OSS).

Diversity of gateways and addition of new ones lead to the necessity of a computer tool capable of optimal spare allocation. The problems that arise are: (1) determination of optimal allocation of spares at each OSS depending on the size of a gateway, (2) determination of location and size of each RSS, and (3) determination of size of the CSS.

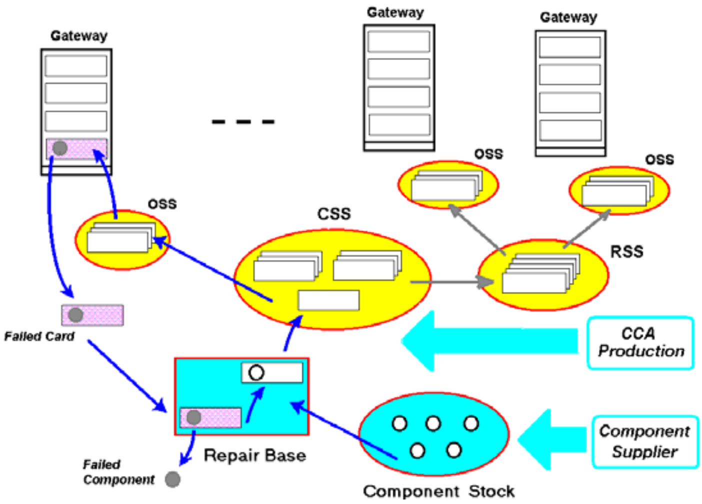


Figure 1. A hierarchical spare supply system

Gateway equipment consists of replaceable units. After each failure, a spare unit from the OSS replaces the failed unit. A failed unit is sent to the repair base. Regional and Central stocks are usually supplied periodically (with priority request for refilling if stock has reached some critical level). On-site stocks are small enough and use the advance delivery; this means that the OSS site sends a request to the RSS after each failure. Structure of Globalstar HSSS is presented in Fig. 1.

FORMULATION OF GENERAL PROBLEM OF OPTIMAL SPARE ALLOCATION

Let the operational system (gateway) consist of *N* different types of spare units. Request for spare unit of type *k*, *k*=1,2...*N*, arrives to the stock in accordance with a Poisson process with (failure) intensity λ_k. Costs of units, c_k, are assumed to be known. A spare stock contains $x_1, x_2... x_N$ units of different types. The problem is to find the optimal allocation, satisfying requirements on the stock reliability or the total cost.

Let $\mathbf{X}=(x_1, x_2... x_N)$ be a vector of spares at the stock site, x_i is the number of spares of type *i*; $P(\mathbf{X}, \theta)$ be reliability index characterizing the spare stock with **X** spares for period of time θ; and $C(\mathbf{X})$ be the cost of spares. Two optimization tasks (Gnedenko and Ushakov 1995) can be formulated as:

<u>Direct:</u> To minimize the total cost of spares at the stock under condition that the stock reliability index is not less than required level *P**, i.e.,

$$\min_{all\,\mathbf{X}} \{C(\mathbf{X}) | P(\mathbf{X},\theta) \geq P^*\}. \tag{1}$$

<u>Inverse</u>: To maximize the stock reliability index under condition that the total cost of spares at stock is not larger than a admissible level *C**, i.e.,

$$\max_{all\,\mathbf{X}} \{P(\mathbf{X},\theta) | C(\mathbf{X}) \leq C^*\}. \tag{2}$$

ON-SITE SPARE STOCK

We assume that gateways are highly reliable and its units are independent, so we neglect the possibility of overlapping of system down times due to different causes. For highly reliable systems, the approximate formula for the OSS unreliability coefficient, Q_{OSS} is

$$Q_{OSS} \approx \sum_{1\le k\le N} \beta_k q_k(x_k)\,. \tag{3}$$

The weights in Eq. 3 are defined as $\beta_k = \lambda_k n_k \left(\sum_{1\le k\le N} \lambda_k n_k \right)^{-1}$, $q_k(x_k)$ = unreliability coefficient of units of type k (cumulative Poisson function with parameter a_k=$n_k\lambda_k\theta$) , and x_k = number of spares of type k in the OSS. For highly reliable systems, approximate formula for the OSS unavailability coefficient, U_{OSS}, is

$$U_{OSS} \approx \theta \sum_{k=1}^{N} \frac{\lambda_k n_k q_k(x_k)}{x_k+1}\,, \tag{4}$$

where θ= time delay corresponding to advance delivery.

PREDICTING APPROXIMATE TRENDS

In many cases of practical interest, we are faced with the problem of sparing a highly reliable system. For a highly reliable system, $\max_k\{a_k\}$<<1 and the cumulative Poisson function may be approximated by its leading term (in practice, $\max_k\{a_k\}<0.1$ is acceptable). Typically, there is at least one spare for every type of unit in a commercially deployed system. On the other hand, total money allocated for sparing is generally limited. If $1 \le x_i \le 5$, $\ln(x_i!) \approx 0.9(x_i-1)$ is a workable approximation in the Poisson function. These two simplifications linearize the Lagrange equation determining the optimal values of x_i (Ushakov and Chakravarty 1998). For goal function shown in Eq. 3 and for the inverse problem of redundancy we obtain

$$x_k \approx round\left(\frac{K - \ln(c_k /(\beta_k C^*)) - a_k + \ln(0.9 - \ln(a_k))}{\ln(0.9 - \ln(a_k))} \right). \tag{5}$$

Constant K in Eq. 5 can be found from the cost constraint $C(\mathbf{X})=\sum_k c_k x_k = C^*$.

REGIONAL AND CENTRAL STOCKS

An RSS is periodically refilled from the Central Spare Stock (CSS). The number and location of gateways, which are served by a particular RSS may changing in time with the development of Globalstar. It seems that the best index characterizing the RSS is its unreliability coefficient (3). The same might be said about the CSS, which is replenished by production (probably with different period for different type of units). In principle, the solution for these cases is similar to the previous one with the difference that the advance delivery period starts with the installation of a failed unit.

OPTIMAL SPARE ALLOCATOR (OSA) SOFTWARE TOOL

The “Optimal Spare Allocator” software tool has been developed for use in Globalstar gateways. Globalstar is a worldwide satellite telecommunication system that has gateways dispersed all over the world.

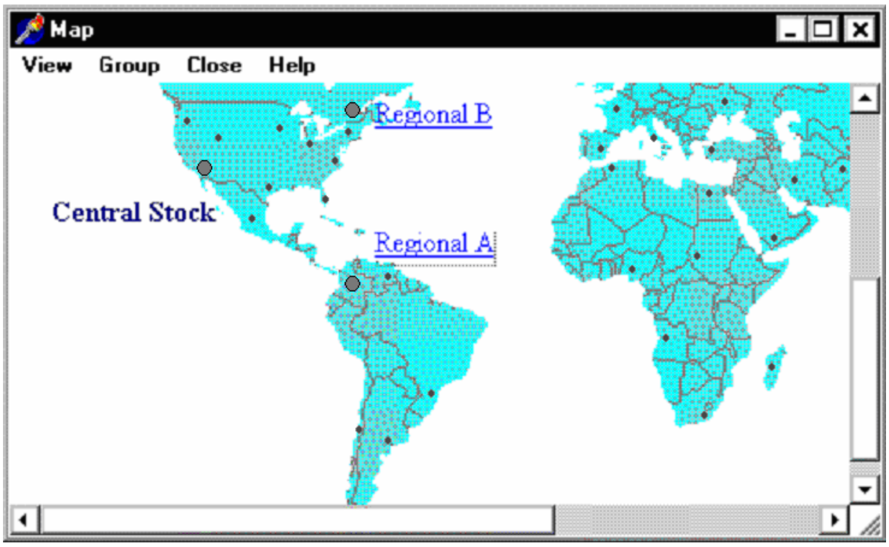
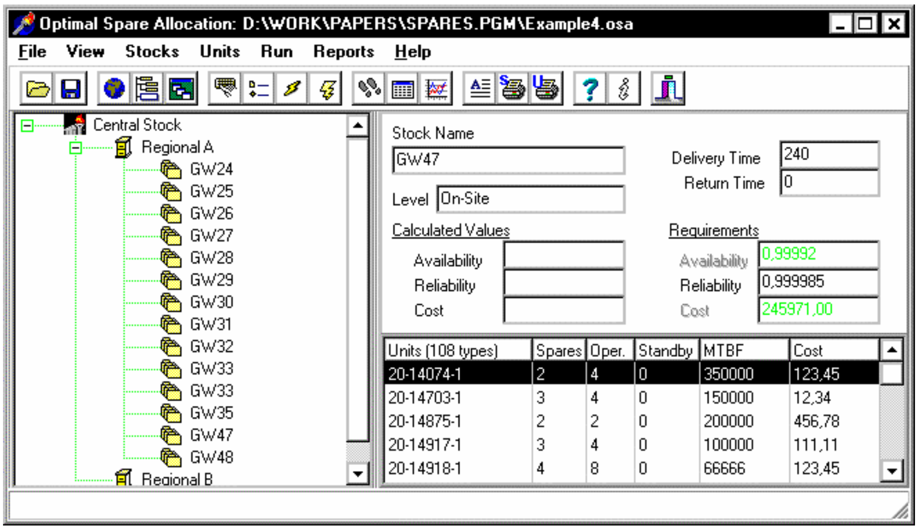


Figure 2. OSA tool: Map of hierarchical stock system.

Its spare supply system is hierarchical in nature. OSA is a GUI driven user-friendly tool designed to solve the direct and inverse problems of optimal redundancy for a multi level hierarchical spare supply system.



Stock Name GW47

Level On-Site

Delivery Time 240

Return Time 0

Calculated Values

Availability

Reliability

Cost

Requirements

Availability 0,99992

Reliability 0,999985

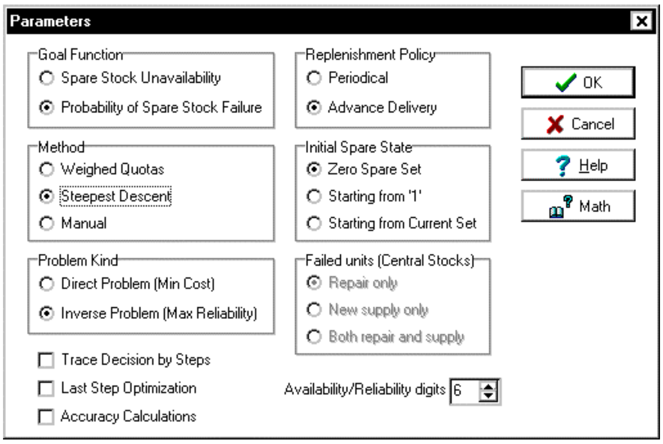
Cost 245971,00

Units (108 types)	Spares	Oper.	Standby	MTBF	Cost
20-14074-1	2	4	0	350000	123,45
20-14703-1	3	4	0	150000	12,34
20-14875-1	2	2	0	200000	456,78
20-14917-1	3	4	0	100000	111,11
20-14918-1	4	8	0	66666	123,45

Figure 3. OSA tool: a hierarchical spare supply system structure

It uses the relative increments of the goal function in respect to a unit of cost (steepest descent method) to solve the optimization problem.

A PC with Windows 95 or NT operating system is needed for installing and running the OSA tool. The program's main window includes a menu of all available commands and a toolbar with the most frequently used operations. It has other windows that depict the "hierarchical tree" of the stock supply system (Fig. 3), a table of parameters characterizing a particular stock, including a list of units and quantities used, embedded spares if any, their cost, their mean time between failures etc.



Goal Function
○ Spare Stock Unavailability
● Probability of Spare Stock Failure

Replenishment Policy
○ Periodical
● Advance Delivery

Method
○ Weighed Quotas
● Steepest Descent
○ Manual

Initial Spare State
● Zero Spare Set
○ Starting from '1'
○ Starting from Current Set

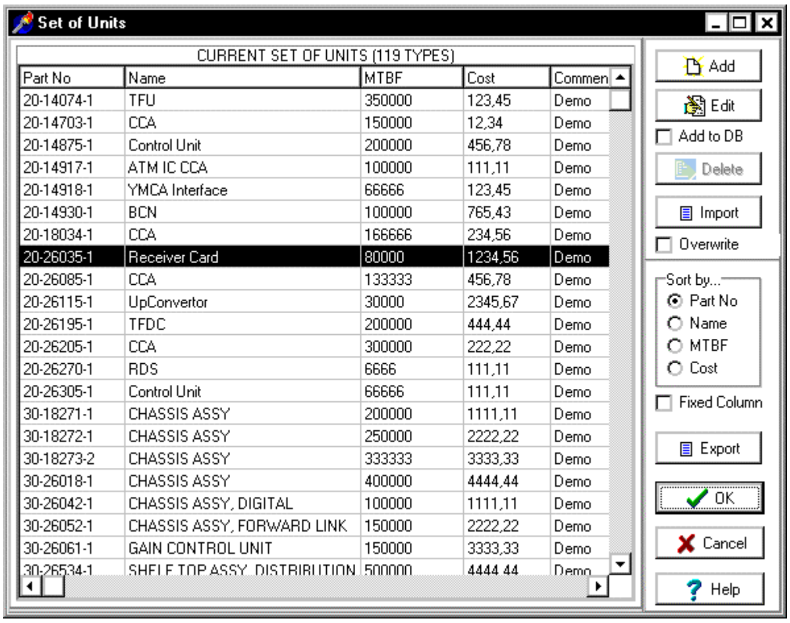
Problem Kind
○ Direct Problem (Min Cost)
● Inverse Problem (Max Reliability)

Failed units (Central Stocks)
● Repair only
○ New supply only
○ Both repair and supply

□ Trace Decision by Steps
□ Last Step Optimization
□ Accuracy Calculations

Availability/Reliability digits 6

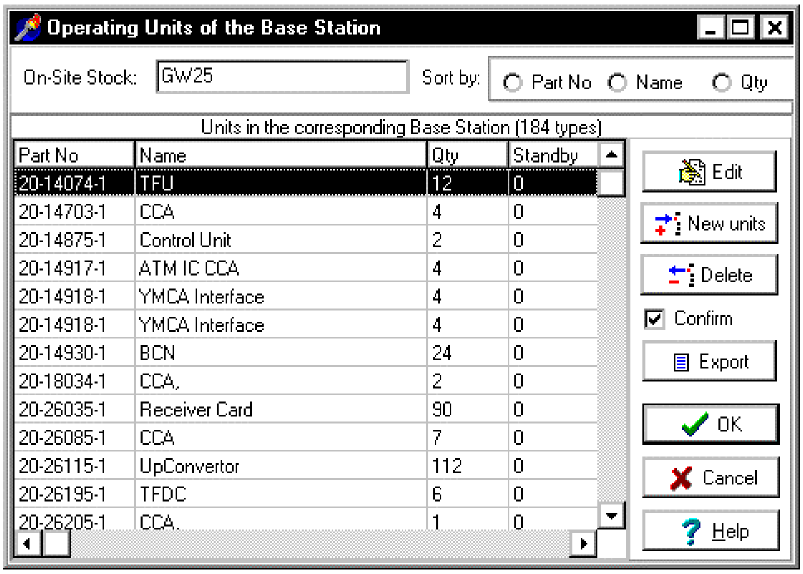
Figure 4. OSA tool: calculation options.



CURRENT SET OF UNITS (119 TYPES)

Part No	Name	MTBF	Cost	Commen
20-14074-1	TFU	350000	123,45	Demo
20-14703-1	CCA	150000	12,34	Demo
20-14875-1	Control Unit	200000	456,78	Demo
20-14917-1	ATM IC CCA	100000	111,11	Demo
20-14918-1	YMCA Interface	66666	123,45	Demo
20-14930-1	BCN	100000	765,43	Demo
20-18034-1	CCA	166666	234,56	Demo
20-26035-1	Receiver Card	80000	1234,56	Demo
20-26085-1	CCA	133333	456,78	Demo
20-26115-1	UpConvertor	30000	2345,67	Demo
20-26195-1	TFDC	200000	444,44	Demo
20-26205-1	CCA	300000	222,22	Demo
20-26270-1	RDS	6666	111,11	Demo
20-26305-1	Control Unit	66666	111,11	Demo
30-18271-1	CHASSIS ASSY	200000	1111,11	Demo
30-18272-1	CHASSIS ASSY	250000	2222,22	Demo
30-18273-2	CHASSIS ASSY	333333	3333,33	Demo
30-26018-1	CHASSIS ASSY	400000	4444,44	Demo
30-26042-1	CHASSIS ASSY, DIGITAL	100000	1111,11	Demo
30-26052-1	CHASSIS ASSY, FORWARD LINK	150000	2222,22	Demo
30-26061-1	GAIN CONTROL UNIT	150000	3333,33	Demo
30-26534-1	SHELF TOP ASSY, DISTRIBUTION	500000	4444,44	Demo

Figure 5. OSA tool: Unit database.



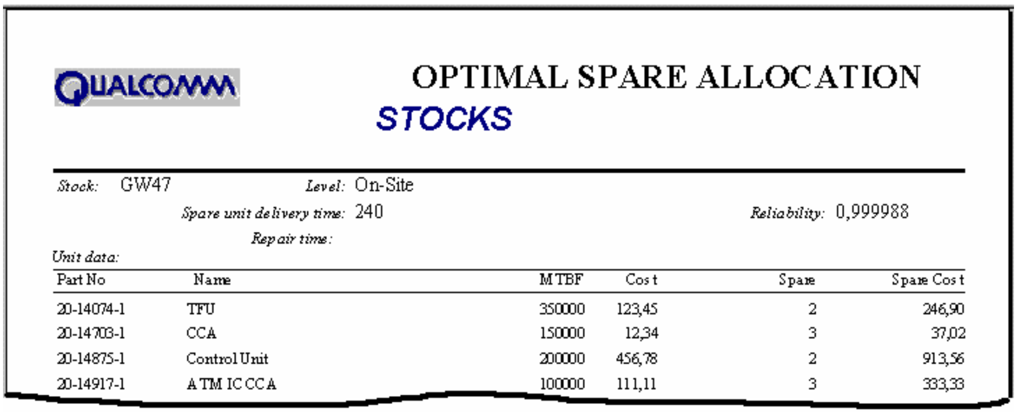
On-Site Stock: GW25

Sort by: ○ Part No ○ Name ○ Qty

Units in the corresponding Base Station (184 types)

Part No	Name	Qty	Standby
20-14074-1	TFU	12	0
20-14703-1	CCA	4	0
20-14875-1	Control Unit	2	0
20-14917-1	ATM IC CCA	4	0
20-14918-1	YMCA Interface	4	0
20-14918-1	YMCA Interface	4	0
20-14930-1	BCN	24	0
20-18034-1	CCA,	2	0
20-26035-1	Receiver Card	90	0
20-26085-1	CCA	7	0
20-26115-1	UpConvertor	112	0
20-26195-1	TFDC	6	0
20-26205-1	CCA,	1	0

Figure 6. OSA tool: Gateway specification



OPTIMAL SPARE ALLOCATION

STOCKS

Stock: GW47 *Level:* On-Site

Spare unit delivery time: 240 *Reliability:* 0,999988

Repair time:

Unit data:

Part No	Name	MTBF	Cost	Spare	Spare Cost
20-14074-1	TFU	350000	123,45	2	246,90
20-14703-1	CCA	150000	12,34	3	37,02
20-14875-1	Control Unit	200000	456,78	2	913,56
20-14917-1	ATM IC CCA	100000	111,11	3	333,33

Figure 7. OSA tool: sample of reporting

The OSA tool is flexible and offers various calculation options to the user. It is able to solve the direct and inverse problems of optimal redundancy with two different goal functions. It also offers two separate replenishment policies, and lets the user choose minimum number of spares consistent with the total cost. Results of calculations are presented in a report whose layout can be specified by the user. Reports generated by the OSA tool may be saved in ASCII format for further processing or documentation.

REFERENCES

1. Gnedenko, B. and I. Ushakov (1995). *Probabilistic Reliability Engineering*. John Wiley, New York.
2. Ushakov, I. (1994). *Handbook of Reliability Engineering*. John Wiley, New York.

SSARS 2007
Summer Safety & Reliability Seminars
22-29 July 2007 Sopot Poland
ESRA
PSRA

Special Issue # 2 on SSARS 2007

•

Invited Editors E. Zio and K. Kołowrocki

METHODS FOR THE TREATMENT OF COMMON CAUSE FAILURES IN REDUNDANT SYSTEMS

Berg Heinz-Peter, Görtz Rudolf, Kesten Jürgen

Bundesamt für Strahlenschutz, Salzgitter, Germany

Keywords

nuclear power plant, probabilistic safety assessment, simulation, common cause failure, modelling

Abstract

Dependent failures are extremely important in reliability analysis and must be given adequate treatment so as to minimize gross underestimation of reliability. German regulatory guidance documents for PSA stipulate that model parameters used for calculating frequencies should be derived from operating experience in a transparent manner. Progress has been made with the process oriented simulation (POS) model for common cause failure (CCF) quantification. A number of applications are presented for which results obtained from established CCF models are available, focusing on cases with high degree of redundancy and small numbers of observed events.

1. Common cause failure analysis in the frame of probabilistic safety assessment

Design, operation and maintenance of systems are performed to minimize potential failures such as random, systematic and dependent failures. Dependent failures comprise secondary failures caused, e.g., by violation of operational conditions and so-called commanded failures like component fails due to violation of interface conditions. The residual part of the group of commanded failures is called common cause failures (CCF). To identify dependent failures, approaches have been extended to encompass potential interpendencies between systems or components. Secondary and commanded failures are supposed to be modelled explicitly as far as possible in fault tree models of the system whereas common cause failures are taken into account in probabilistic safety assessment implicitly by parametric models.

In general, the most important defence against accidental component or system failures is the implementation of principles such as separation, diversity and redundancy. However, experience has shown that redundancy itself is not sufficient to avoid undesired events just because of possible dependent failures.

CCF of redundant safety relevant systems have been of concern since quantitative estimation of the reliability of these systems was developed starting in the early 70ies because this type of failures affect significantly their availability and reliability leading – in the worst case – to a simultaneous loss of all redundancies.

Typical examples of CCF are miscalibration of sensors, incorrect maintenance, environmental impact on the field device and use of a not appropriate process fluid, which plugs valves in different redundancies.

Experience from numerous probabilistic safety assessments has shown that, especially for highly redundant systems in nuclear power plants, common cause failures tend to dominate the results of these assessments such as the core damage frequency or large early release frequency.

As a consequence of generally rather effective defence against common cause failures in place, the number of really observed events in nuclear power plants is limited, in particular with respect to events involving failures of all or at least many redundant components. However, the operational experience contains some information on potential common cause failures, i. e., partial failures that could have evolved into the complete failure- of the common cause component group within a short period of time. This in turn requires in one way or the other an extrapolation based on parametric models, which is extremely difficult to verify.

Despite of these difficulties significant progress has been made in the last years due to increasing operational experience, more systematic data collection and analysis, growing experience in probabilistic safety assessment and an enhanced exchange on data and methods both nationally and internationally.

Although the use of plant-specific data in probabilistic safety assessment is preferred, in case of lack of events or of information it is helpful to provide a generic data base taking into account all national experiences and appropriate international data. Data bases like the OECD/NEA International Common Cause Failure Data Exchange Project allows collecting and analysing data of a lot of different components such as valves, pumps and diesel generators. Results of the analysis of these data also enable to assess and improve the effectiveness of defences against common cause failure events. For that purpose, data and information related to events observed in the operational experience with sufficiently detailed content have to be provided.

In general, the treatment of common cause failures within probabilistic safety assessment requires four main steps: development of a system logic model, identification of common cause component groups, common cause modelling and data analysis as well as quantification and interpretation of the results. For the quantitative part of the common cause failure assessment, models have still to be further developed, in particular with respect to applicability to highly redundant systems, suitability and traceability.

2. German practice

Probabilistic safety analyses (PSA) have been performed for all operating German nuclear power plants. Experience has shown that CCF in many cases tends to dominate the results of the PSA. Therefore, methods and results of CCF analyses receive a lot of attention in the discussions between regulator, technical experts, utilities and analysts.

Regulatory guidance is available in Germany for level 1+ PSA (a level 1+ analysis is understood to end at the onset of core damage but to take into account active containment functions) as part of periodic safety reviews of nuclear power plants. According to the importance of CCF, a chapter in the German regulatory guidance documents is dedicated to dependent failures [6]-[7]. These failures comprise secondary failures caused by violation of operational or environmental conditions as well as commanded failures - intact component failing due to violation of interface conditions, for example in the case of erroneous signals or failed energy supply. The residual part of the group of dependent failures is the common cause failures mentioned before. Secondary and commanded failures are to be modelled explicitly as far as possible in the fault tree models of the system. CCF, on the other hand, are taken into account in PSA by parameter models [2].

The guidelines mentioned before – they are currently undergoing final steps of revision in view of the fact that the Atomic Energy Act as amended in 2002 makes Periodic Safety Reviews (including PSA) mandatory – do not prescribe specific CCF models. Rather, they demand that the parameters of any model used are to be derived in a clearly described way from operating experience. Thus, in German PSA practice, a variety of models have been used [1], [9], [10].

3. A process oriented simulation model (POS) for CCF quantification

3.1. Rationale and objectives

The question can be raised whether an approach aiming at modelling the entire CCF process from the point in time of the root cause impact to failures taking effect or being detected in the common cause component group (CCCG) in a more mechanistic manner could support and complement the established modelling which is mostly aiming at failure probabilities. Such a process oriented modelling approach is described and discussed in this paper. It represents a further elaboration of the modelling stages described in [3]-[4].

3.2. Model description

The method of stochastic simulation offers a convenient way to describe the model and to quantify its results. The sequence of stochastic variables displayed in table 1 is supposed to adequately describe the CCF process.

Based on simulation of this sequence, the associated unavailability's can be calculated.

The following fixed-value parameters are used throughout a simulation sequence:

- operation time	T_B
- number of components in the CCCG:	r

- time between functional tests T_{FT}

The sequence of variables and calculations defines a single simulation of the common cause failure process. It is described how the variables are either derived from a stochastic assumption or are calculated deterministically.

The calculation of the probabilities *W(m,r)* for the event that the common cause impact will affect exactly *m* out of *r* components are calculated by a recursive scheme that is detailed in [3]. Here, only the formulae up to *r* = 4 are given. Model parameters are *a* and r_0.

$$W(2,2) = 1, \tag{1}$$

$$W(3,3) = a, \tag{2}$$

$$W(2,3) = 1 - a, \tag{3}$$

$$W(4,4) = a \cdot \left(a + (1-a) \cdot \left(1 - e^{-3/r_0}\right)\right), \tag{4}$$

$$W(2,4) = (1-a)^2, \tag{5}$$

$$W(3,4) = 1 - W(4,4) - W(2,4). \tag{6}$$

To facilitate handling of the necessary equations, model parameter r_0 is replaced by:

$$c = \exp(1/r_0). \tag{7}$$

In the applications presented here, a model version has been used that is based on a simplified assumption regarding the CCF identification. It is assumed that non-staggered testing is applied and that a CCF-event is identified at the functional test following the first component failure. It is well known that conditions in the field are more complex. To account for that from the information provided in the literature sources effective test intervals have been estimated for the POS-analyses. The model assumptions can be modified to account for other situations like staggered testing in a straightforward manner. As the prime purpose of this paper is to demonstrate key features of the POS model such refinements have been postponed.

3.3. Parameter estimation for the process oriented simulation model

The parameter estimation routine used here is closely related to the one described in [4]. It has, however, been simplified without significantly lowering its precision.

3.3.1. Frequency

The model has essentially four parameters that have to be estimated. The first is the frequency of CCF-events for which the usual estimator for failure rates is used.

3.3.2. Number of impacted components

The approach selected consists of an estimation of the distribution of the number of impacted components based on the observed events:

$$W_{est}(m,r) = \frac{N_m + 1/(r-1)}{K}. \tag{8}$$

The constant term 1/(r-1) is introduced into the estimator to avoid vanishing probabilities, which in practice are not expected. K serves for normalization. N_m is the number of events for CCCG size r and with number of impacted components m.

On the other hand, the probabilities can be calculated as functions of the model parameters. It can be shown that

$$W(2,r) = (1-a)^{r-2}. \tag{9}$$

Table 1. Overview of the POS model

Sequence of stochastic variables	Modelling assumptions for the stochastic variables Model parameter	 Assumption
Time t_{CCI} of common cause impact	Rate of common cause impacts r_{CCI}	Equally distributed in T_B, $r_{CCI} \cdot T_B << 1$,
Number $m < r + 1$ of impacted components	a, r_o	Probability $W(m, r)$, see formulae (1) to (6) and [3]
Failure rate R of the impacted components	Probability of instantaneous failure of all impacted components W_{inst}, interval for rates of non- instantaneous failures R_{MIN} to R_{MAX}	According to W_{inst} the m components fail either instantaneously or are logarithmic equally distributed in the interval R_{MIN} to R_{MAX}
Times of failure of the impacted components	$t_F(m)$	Either all impacted components fail at t_{CCI} or the times of failure are exponentially distributed with rate R
Identification of CCF-process by the functional test	—	For times > $t_F(i)$ the failure and the common cause process are identified, the components are immediately repaired and as good as new
Time of CCF identification t_{ID}	T_{FT}	The functional tests are performed at intervals T_{FT} . The first test time after the first failure occurring at the minimum of the $t_F(m)$ is equal to t_{ID}
Finally, from the failure times $t_F(i)$ $(i = 1, ..., m)$ in the time interval between t_{CCI} and t_{ID} the time periods are calculated in which zero, one, two, ... up to at most m components are failed: $\Delta(i)$ $(i = 0,1,2,..,m)$		
The average of $\Delta(i) / T_B$ $(i \geq 1)$ for many simulations is the unavailability.		

This relation suggests the following estimator:

$$a_{est}(2,r) = 1 - W_{est}{}^{1/(r-2)}. \tag{10}$$

In a second step, parameter c is estimated based on the mean of m:

$$< m >_{est} = \sum_{m=2}^{r} m \cdot W_{est}(m,r). \tag{11}$$

Again, the mean of m can be calculated as a function y of the model parameters a and c

$$< m >= y(a,c). \tag{12}$$

This can be used to estimate c based on the estimates a_{est} and $W_{est}(m,r)$ already obtained

$$c_{est} = y^{-1}(a_{est}, < m >_{est}). \tag{13}$$

Here, y^{-1} denotes function $y(a,c)$ inverted with respect to c.

There are, however, cases in which the non-linear equation (13) for c_{est} does not have a meaningful solution. This is avoided by applying the following transformation to the estimated $<m>_{est}$:

$$< m >'_{est} = y(a_{est},0) \cdot \left(\frac{< m >_{est} - 2}{r-2} \right) \qquad (14)$$

$$+ y(a_{est},1) \cdot \left(\frac{r - < m >_{est}}{r-2} \right).$$

The following estimator does always lead to meaning-full results:

$$c_{est} = y^{-1}(a_{est}, < m >'_{est}). \qquad (15)$$

3.3.3. Fraction of impacts leading to immediate failure

The last parameter to be estimated is the fraction of events that lead to failure of all impacted components immediately, W_{inst}. It can – in some cases – be derived from the event reports in a straightforward manner.
A quantity sensitive to this parameter is the ratio of the number of events N_f in which all impacted components failed to the number of all events N_{total}

$$f = N_f / N_{total} \, . \qquad (16)$$

For the mean value of this parameter holds

$$< f >= W_{inst} + (1 - W_{inst}) \cdot F_{cont} , \qquad (17)$$

F_{cont} denotes the probability that in case of a non-instantaneous failure event all impacted components fail. This quantity obviously depends on the time of CCF detection. The identity serves as motivation for the following estimator

$$W_{inst} = \max\{(1 \;\; /2 \cdot N_{total}), (f - F_{cont})/(1 - F_{cont})\}. \qquad (18)$$

The estimation procedure described here is easier to handle than the approach described in [4] which is based on minimization of Kullback's information measure [11].
The rationale for the estimation procedure is rather of heuristic nature and not supported by rigorous proof. It is therefore necessary to assess its appropriateness using a simulation test outlined in the following.

3.4. Test for the estimation procedure

The estimation procedure is seen as a practical approach that is not underpinned by sophisticated mathematics but rather by direct testing. The latter is possible because the POS model can be used to generate fictitious failure data which can than be subjected to parameter estimation. Comparing the estimated parameters with the "true" parameters used in the simulation will display the balance of the strengths and weaknesses of the estimation procedure. The possibility to carry out such a test is a further advantage of simulation modelling.

3.4.1. Failure data and comparison to estimated parameters

From the data given *Table 2*, a set of 30 simulated CCF event data sets was produced, comprising on average some three CCF events each.

Table 2. 'True' parameters and derived CCF failure multiplicities (assuming CCF rate of 0,075 a^{-1}) used for the model test

Parameters	a = 0,5	c = 2,0	W_{inst} = 0,1

Failure multiplicities	2-out-of-4	3-out-of-4	4-out-of-4
Failure probabilities	$1,3\cdot10^{-4}$ a^{-1}	$8,3\cdot10^{-5}$ a^{-1}	$9,7\cdot10^{-5}$ a^{-1}

This exercise representing a straightforward test of principle, all simulated failure events were supposed to affect CCCG of size r = 4. The low number of simulated events corresponds to the well-known fact that CCF events as such are rather scarce. For the parameter estimation, only the number of CCF events, the number of failed and the number of affected – but not failed – components in each event were used, together with the supposed observation time, given in component group years. To assess the predictive power of the model, the parameters estimated for each of the 30 data sets were used to predict a 4-out-of-4 failure probability which was compared to the 'fictitious reality' as given in *Table 2*.

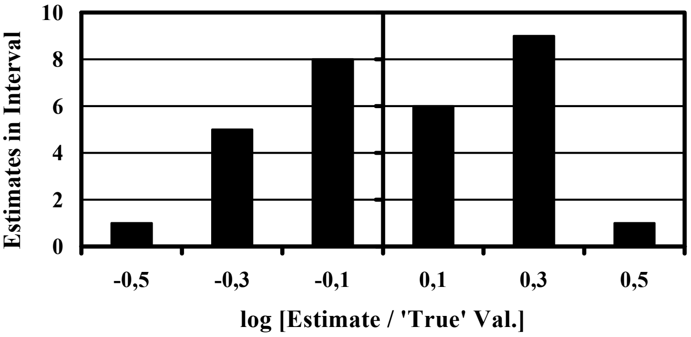


Figure 1. 'True' vs. estimated CCF probabilities for 4-out-of-4 failures

The result is shown in *Figure 1* above. In all cases, a CCF-detection time of 1.5 months has been assumed. Obviously, the estimation procedure gives rather satisfactory results. The conservatism introduced by the heuristic assumption of eqn. (18) results in a very moderate overestimation of the true value.

3.4.2. Data base and quality of prediction

In order to test the POS model's performance in case of a scarce data base, the estimation procedure as detailed above was repeated, this time using a data set of simulated CCF events based on a CCF impact rate corresponding, on the average, to one event in the observation period. Obviously, a data set with zero events does not make sense; therefore, in such cases the fictitious observation time was extended until an event was simulated.

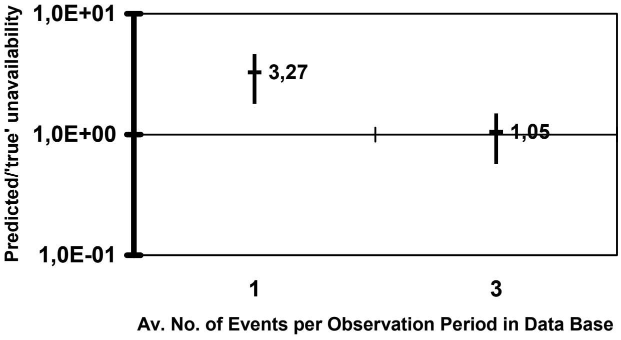


Figure 2. Comparison of predicted vs. 'true' unavailability's for 4-out-of-4 CCF on the basis of, on average, one or three events per database. Medians and standard error bars are given based on ten data sets for each case.

As can be expected, the conservative assumption implicit in equation (18) takes more effect in this case. *Figure 2* gives a comparison of predicted vs. 'true' failure rates for 4-out-of-4 CCF. As is evident from the comparison, the predictions based on scarce data tend somewhat to the conservative side.

On the other hand, it is demonstrated in *Figure 3* how the estimation is improved if more events are included in the database for a representative example. The parameter W_{inst} being rather sensitive to failure of all components is overestimated in the upper part of figure 3 based on 3 events in the average in the data set. In the lower part of figure 3, it can be seen how the enhanced number of events improves the estimate.

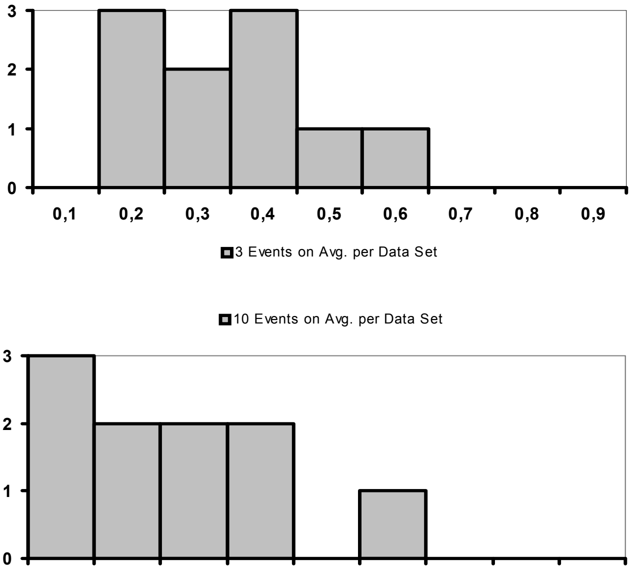


Figure 3. Dependency of parameter estimation quality on the number of events in the database. Estimated parameter: W_{inst}; true value: W_{inst} = 0.1 (cf. *Table 2*).

Upper diagram corresponds to 3 events on average, lower diagram corresponds to 10 events on average, showing improved estimation.

4. Analysis of a highly redundant system with the POS model

Hauptmanns [8] has published a challenging case study on a highly redundant CCCG. It concerns the combined impulse pilot valves which in German nuclear power plants govern the function of pilot operated safety or relief valves. For German Boiling Water Reactors (BWR), there are up to 22 such impulse pilot valves governing the function of the automatic depressurisation system (ADS).

CF quantification for such highly redundant systems is demanding, due to the sparse base of observed events, which, in addition, will mostly consist of events with only a limited number of failed components. Even in Hauptmanns' case, where the database consists of twelve events, there are only two cases with more than half of the CCCG actually failed (cf. *Table 3* below).

In [8], Hauptmanns compares CCF rates predicted for 1-out-of-22 through 22-out-of 22 failure multiplicities using the classical binomial failure rate (BFR) model to those predicted with his improved multi-class binomial failure rate (MCBFR) model. For the latter, the events in the database are sorted into different classes according to engineering judgement, and attempts to estimate individual coupling factors p for all of the defined event classes. Detailed information on the models and the calculation method are in [8].

Table 3. Observed CCF and degradations for combined impulse pilot valves (failure mode: does not open); adapted* from [8]

Event No.	No. failed components	No. degraded components	CCCG size *r*	Operation time T_B *[a]*
1	2	0	9	9
2	6	2	8	10
3	2	0	22	7
5*	1	15	16	9

6	2	5	16	7
7	2	10	12	6
8	7	1	8	10
9	1[a]	13[a]	14	9
11*	2	6	12	6
12	2	0	4	9

* H's events # 4 and 10 were omitted because with 1 failed and 0 degraded but not failed components they do not correspond to the definition of a CCF used in this paper, which is based on at least two components impacted by the common cause.

[a] In H's event # 9, one of the 14 components found degraded is assumed failed, because the analyses with the POS model presented here do not handle 'zero failure' events.

In case there is at least one CCF event in the database where all or nearly all components of the CCCG were failed, the MCBFR model can be expected to yield less unrealistic failure rates for high failure multiplicities than the classical BFR model.

Using the raw data as given in [8] with the exception of omitting events #4 and #10 and assigning event #9 one failed and 13 affected components instead of 0 failed and 14 affected, cf. table 3 – the CCF rates for a CCCG of size 22 were calculated. Total operation time of 165 component group years was used in estimating the CCF rate.

The results obtained with the POS model do not exhibit the unrealistic low failure rates for higher multiplicities. They do not coincide with the MCBFR results but are comparable especially in the range of higher failure multiplicities. Key difference to the MCBFR approach is that for the POS application no decomposition of the event base had to be performed. The approach is integral. It can be concluded that the POS model is a candidate for CCF analyses of highly redundant systems.

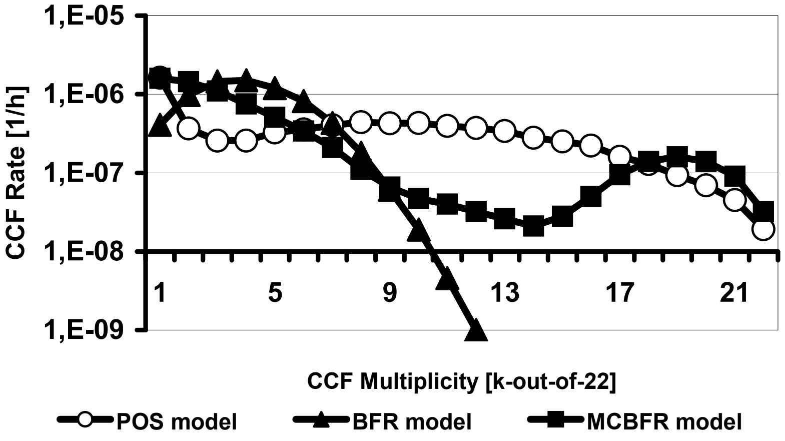


Figure 4. CCF-rates for pilot valves in German NPP according to Hauptmanns for the (BFR) and the (MCBFR) model. The results with the POS model have been obtained with the parameter estimation procedure described in this paper.

5. Calculating alpha-factors with the POS model

In [13], approaches to CCF quantification are outlined, especially the use of parametric models. In the report [12], common cause failure parameter estimations have been provided for some 40 different component types, various failure modes and common cause component group sizes from two up to six. One of the models for which parameter distributions have been derived is the Alpha-Factor Model. From the point of view of demonstrating the usefulness of the POS model, this large amount of systematically derived information was seen as a possibility to apply POS and compare to results obtained with established methods.

As pointed out before, for the POS parameter estimation information is required on the number of components, which are affected by the event. This kind of information is not available in [12]. Therefore, for this exercise a simplified approach has been selected [5].

The alpha factor α(k,l) is by definition the probability that in a CCF component group of size l exactly k components have failed as consequence of a CCF basic event. Hence, the quantities are normalized with respect to the failure multiplicity k = 1,2, ...l. The first simplifying assumption is that the failures with k equal to 2 and greater are determined by dependent failures only. The conditional probabilities w(k,l) for these events are calculated with the POS model. In [7], the numbers of independent and dependent events are given and thus the ratio q of dependent to total number of events is at hand. The alpha factors than can be calculated as follows:

$$\alpha(k,l) = w(k,l) \cdot q \ + (1 - q) \cdot \delta(k,1) \qquad (19)$$

$$\delta(k,1) = 0 \text{ for } k > 1 \text{ and } \delta(1,1) = 1 \qquad (20)$$

The selection of POS-parameters is – as pointed out before – simplified. The values of $W_{inst} = 0.1$ and of $r_0 = 3$ are taken as default values throughout the exercise. These values are typical values based on other applications. Parameter a is the fitted such that α(4,4) is equal to the value tabulated in [12] for the component type and failure mode under consideration.

This program has been carried out for six different combinations of components and failure modes. These were selected primarily based on large numbers of dependent failures to make sure that the comparison has a solid statistical basis. Furthermore, a mix of technically different components has been chosen. Furthermore, only those components were included for which CCF group sizes up to 6 are covered in [12].

For the comparison with the empirical data from [12] a metric for the deviation of the quantities is required. In [12], the mean, but also the 5-, the 50- and the 95-percentile of the alpha factor distributions are displayed. This suggested to use the logarithm of the ratio of the alpha factor derived from the POS model to the 50-percentile from [12], divided by logarithm of the ratio of the values of the 95-percentile to the 50-percentile. This means a deviation X = 1 if the calculated value equals the value of the 95-percentile

$$X = \log (\alpha_{POS} / \alpha_{50}) / \log (\alpha_{95} / \alpha_{50}). \qquad (21)$$

Eq. (21) holds for values of α_{POS} larger than the median of the distribution, the analogous measure is used for α_{POS} smaller than the median. In that case, the deviation X = -1 is obtained if the calculated value equals the value of the 5-percentile.

A similar picture is obtained by considering complete CCFs (failure of all components). This is displayed in Figure 5. *It is not surprising that the agreement is better for α(5,5) and α(3,3) than for α(2,2) as the parameter adjustment was done for α(4,4). For small sizes of the component group the deviations are larger. The assumption that the failure multiplicities > 1 are due to dependent failures only might here be wrong and thus lead to greater deviations.*

Considering the severe simplifications that were made in the exercise, the results obtained with the POS model adjusting only one of three possible parameters are satisfactory especially for high failure multiplicities.

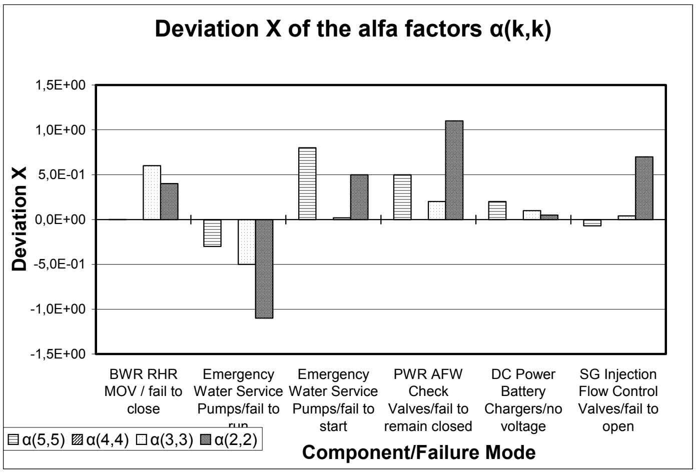


Figure 5. *Deviation X of the alfa factors α(k,k) calculated with the POS-model from values tabled in [13].*

6. Summary, conclusions and outlook

The POS model for CCF quantification is based on the following model structure:

- Time of CCF impact, simulated with a constant CCF impact rate,
- Number of components of the CCCG affected by the impact and subsequently failing immediately or time-delayed,
- Times of failure of the impacted components, and
- Time of detection of the CCF process by inspection or functional testing.

As a last step to prepare practical application of the model, a procedure for estimating the four free model parameters – rate of CCF impact, parameters a and c determining the probabilities of the number of impacted components and fraction of instantaneous failures – has been suggested and tested.

The POS model can be used to generate fictitious failure data which can than be subjected to parameter estimation. Comparing the estimated parameters with the "true" parameters used in the simulation gave a good agreement with a slightly conservative tendency. The low number of events – roughly three on the average – on which the estimation has been based, makes this observation remarkable. In situations with even less events the conservative overestimate of the unavailability becomes more visible but still results are not totally out of bounds.

CCF analyses for pilot valves in German nuclear power plants present a real challenge as component group seizes range up to 22. The POS application has no problem whatsoever with this situation. It does not show the totally unrealistic behaviour predicted by the BFR-model. The results show some agreement with a multi-class-BFR approach suggested by Hauptmanns without the need to decompose the observed events into different technical classes.

As a bottom line, the results obtained increase the confidence into the model and the parameter estimation procedure. The next steps will be directed towards enhancing the number of applications. This work will be directed to areas of application where CCF failure data covering many component types and a larger range of component group sizes have been produced with well established models, [12] cf. e. g. In such cases, parameter estimates can be obtained from data derived from events in component group sizes up to 4 and extrapolated to higher degrees of redundancy. This will constitute a real test of the model and the parameter estimation procedure.

References

[1] Berg, H.-P. et al. (1996). Status of Common Cause Failure Analyses in PSA in Germany. *Proc. International Topical Meet Probabilistic Safety Assessment, PSA '96*, Park City, Sept 29 – Oct 3, La Grange Park: ANS, 777 – 782.

[2] Berg, H.P. & Görtz, R. (1998). Regulatory Guidance on PSA in Germany, *Kerntechnik* Vol. 63 (No. 5-6): 278-281.

[3] Berg, H.-P. & Görtz, R. (2001). A Model for Common Cause Failures in systems of redundant components. *Proc KONBiN'01,* Szczyrk, May, 22 - 25, 2001. Warszawa: Wydaw. Inst. Tech. Wojsk Lotn. Vol. 3: 7- 15.

[4] Berg, H.-P., Görtz, R. & Schimetschka, E. (2004). Parameter Estimation for the Process Oriented Simulation (POS) Model for Common Cause Failures. *Proc. PSAM 7 – ESREL '04,* Berlin, June, 14 – 18, 2004. London: Springer: 837 – 842.

[5] Berg, H.-P., et al. (2006). Calculating Alpha-Factors with the Process-oriented Simulation Model. *Proceedings PSAM 8,* New Orleans 2006.

[6] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2005). *Safety Review for NPP According to § 19a of the Atomic Energy Act - Probabilistic Safety Assessment Guide* (Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes – Leitfaden Probabilistische Sicherheitsanalyse, 31. Januar 2005, Bekanntmachung vom 30. August 2005), Bundesanzeiger Nr. 207a vom 03. November 2005.

[7] Facharbeitskreis Probabilistische Sicherheits-analyse für Kernkraftwerke (2005). *Methods for PSA for NPPs*, (Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005), BfS-SCHR – 37/05, Salzgitter, Oktober 2005.

[8] Hauptmanns, U. (1996). The Multi-Class Binomial Failure Rate Model. *Reliability Eng and Syst Safety* Vol. 53 (No. 1): 85 – 90.

[9] Knips, K. & Kreuser, A. (1997). *GVA-Benchmark.* Schriftenreihe Reaktorsicherheit und Strahlenschutz BMU-1998-514. Bonn: Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit.

[10] Kreuser, A. & Peschke, J. (2001). Coupling Model: a Common Cause Failures Model with Consideration of Interpretation Uncertainties, *Nuclear Technology*, Vol. 136, 255 – 260, December 2001.

[11] Kullback, S. (1951). *Annals of Math Statist*, Vol. 22: 79 – 84.

[12] Marshall, F. M., Rasmuson, D. M. & Mosleh, A. (1998). *Common-Cause Failure Parameter Estimations*, Washington DC: US Nuclear Regulatory Commission, NUREG/CR-5497.

[13] Mosleh, A. Rasmuson, D.M. & Marshall, F.M. (1998). *Common - Cause Failures in Probabilistic Risk Assessment.* NUREG/CR - 5485 (INEEL/ EXT-97-01327), US Nuclear Regulatory Commission, Washington DC.

ANALYSIS OF THE IMPACT OF EXTERNAL FLOODING TO NUCLEAR INSTALLATIONS

Berg Heinz-Peter, Fröhmel Thomas

Bundesamt für Strahlenschutz, Salzgitter, Germany

Winter Christian

Universität Bremen, Bremen, Germany

Keywords
nuclear power plant, probabilistic safety analysis, external flooding, protection, tsunami

Abstract

The German regulatory body has issued probabilistic safety assessment guidelines, elaborated for a comprehensive integrated safety review of all NPP in operation and containing a newly developed graded approach for the probabilistic assessment of external flooding. Main aspects are explained such as the underlying probabilistic considerations and the mathematical procedures for the calculation of exceedance frequencies. Exemplarily it has been investigated if extreme events such as tsunami waves could be a hazard for NPP at coastal sites in Germany.

1. Introduction

Knowledge of high-water discharge levels in small and large basins is a prerequisite for the optimal protection of humans and animals, landscape and infrastructure. In order to deal with many safety-related issues it is important to have information about discharge volumes at peak waters, the risk of these high waters, as well as the course and volumes of discharged water.

Along many large rivers, monitoring stations have been set up, which have observation records at their disposal that go back many years. Based on these sets of measurements, the required high-water discharge parameters, as well as statistical high-water values, can be assessed.

However, not all the monitoring stations on small rivers and rivulets have extensive sets of measurements at their disposal, while, in some cases, there are no sets of measurements at all. This makes it more difficult to retrieve the necessary high-water information. In accordance with the varying situations relating to hydrological data, topography, geology, soil conditions and the objectives, numerous models have been designed for the formation and concentration of discharge.

Thus, an international consistent methodology for flood risk analysis is necessary.

2. External flooding in the safety assessment for German nuclear power plants

The effects of flooding on a nuclear power plant site may have a major bearing on the safety of the plant and may lead to a postulated initiating event that is to be included in the plant safety analysis. The presence of water in many areas of the plant may be a common cause failure for safety related systems, such as the emergency power supply systems or the electric switchyard, with the associated possibility of loosing the external connection to the electrical power grid, the decay heat removal system and other vital systems [8].

Considerable damage can also be caused to safety related structures, systems and components by the infiltration of water into internal areas of the plant, induced by high flood levels caused by the rise of the water table. Water pressure on walls and foundations may challenge their structural capacity. Deficiencies in the site drainage systems and in non-waterproof structures may also cause flooding on the site. This has happened in many cases in the past, with consequent large-scale damage documented, and the possibility should be considered in the hazard evaluation and in the design of measures for site protection.

In principle methods to systematically analyse existing nuclear facilities regarding the adequacy of their existing protection equipment against external flooding can be of deterministic as well as probabilistic nature.

The German Incident Guidelines require a determination of a sufficient water level as design-basis and appropriate structural protection measures against this hazard in the design of the plants to avoid radiological consequences for the environment. The adequacy of the protection measures have been shown in the past only on a deterministic basis. New probabilistic safety assessment guidelines (PSA) recently issued by the German regulatory body now prescribe also probabilistic analyses of external hazards [2].

This assessment can be very comprehen-sively and inadequately. Additionally, as explained in [1], the collective experience with probabilistic safety assessment of external flooding is limited. Therefore, it is necessary to locate parts of a NPP where no further analysis is required or to apply graded procedures which take into account plant- and site-specific conditions for the respective hazard.

Appropriate screening procedures are those which on the one hand allow to constrain the complexity of the analysis and, on the other hand, ensure that relevant information are not lost during the screening process and that all safety significant parts of the plant are taken into account. The approach for these screening processes is different for each type of external hazard.

The German PSA Guide, issued in 1997, contained reference listings of initiating events for NPP with Pressure Water Reactor (PWR) and Boiling Water Reactor (BWR) respectively, which have to be checked plant specifically with respect to applicability and completeness. Plant internal fires and plant internal flooding were included in these listings, but not explicitly external hazards.

In 1997 detailed instructions have been provided in technical documents on PSA methods, which have been developed, by a working group of technical experts from nuclear industry, authorities and technical safety organizations chaired by Bundesamt für Strahlenschutz (BfS).

In October 2002, the Commission on Reactor Safety of the States Committee for Atomic Nuclear Energy has agreed to a new draft of the PSA Guide. An updated draft had then been completed in September 2004. The corresponding documents on PSA method and data have been revised and discussed in the respective committees including the German Reactor Safety Commission. All documents have been issued in autumn 2005 [4], [6], [7].

Regarding external hazards, the updated probabilistic safety assessment guidelines require probabilistic considerations of aircraft crash, external flooding, earthquake and explosions pressure waves.

A graded approach for the extent of a probabilistic assessment in case of external flooding containing deterministic and probabilistic elements has been developed and is described in [6]. This approach takes into account site-specific aspects like the NPP grounded level compared with surroundings level and plant-specific aspects such as design with permanent protection measures and prescribed shut down of the plant according to the instructions of the operation manual at a specified water level which is significantly below the level of the design flooding.

3. Extent of the graded approach in PSA for external flooding evaluation

With respect to the phenomena leading to a flooding event, in principle the sites can be differentiated as follows:

a) Sites on rivers and on inland lakes, which are endangered by, flood runoffs from the prevailing drainage areas.
b) Coastal sites endangered by flood levels of the ocean.
c) Sites on tidal rivers endangered both by flood runoffs from the prevailing drainage areas and by flood levels of the ocean.

German nuclear power plants were erected at sites of type a) (without inland lakes) and c). In the first case a high water-level situation may arise from an unfavourable ratio of water inflow to outflow, in the second case the coincidence of storm, flooding and high tide is the determining factor. In the proposed method, the yearly probability of reaching extremely high water levels (in the following named as exceedance frequency) is determined by an extrapolation of actually measured water-level data according to various established methods [11], [13]. The under-lying probabilistic considerations and mathematical procedures to calculate the exceedance frequencies has recently been developed and issued in November 2004 as part of the German Nuclear Safety Standard “Flood Protection for Nuclear Power Plants” [12].

The graded approach for external flooding can be summarized as given in *Table 1*. The main two substantial modifications and innovations of the revised standard are:

The design of the protection of nuclear power plants against flooding emanates from a rare flooding event with an exceeding frequency of 10^{-4}/a, but it is underlined that the methods used to determine the design water level must be different for river sites without and for sites with tidal influences. For river sites without tidal influence, the design water level can be assessed using the runoff of the river with the given exceeding frequency as basis.

For river sites with tidal influences, an extreme flood event - tide combined with storm water level set-up - must be assumed.

Therefore, it is necessary to determine statistically the storm-tide water level with an exceeding frequency of 10^{-2}/a plus a site-specific addend. In conclusions, a storm-tide must be covered with an exceeding frequency of 10^{-4}/a.

Table 1. The graded process of evidence regarding external flooding

Criterion	Extent of analysis
Flooding of plant site can be practicable excluded due to the NPP grounded level compared with surroundings level	No analysis necessary
1. The plant is designed against the design-basis flood with an exceedance probability of 10^{-4} per year 2. Design with permanent protection measures 3. Shut down of the plant according to the instructions of the operation manual at a specified water level which is significantly below the level 4. Conditional probability for water impact in case of the design-basis flood less than 10^{-2}	Determination of possible water paths in relevant structures and estimation of the conditional probability for water impact in case of the design-basis flood
Other design	Determination of the exceedance for the design-basis flood of the plant up to a value of $\geq 10^{-4}$ per year, detailed event sequence considerations including the quantification of core damage frequency

In the context of the analysis, design-basis flood is that particular flood event on which the flood protection of the plant is based, specifically with regard to meeting the safety objectives. The permanent flood protection is that flood protection which is effective at all times (e.g. protection by flood-safe enclosure, by structural seals). The loads due to the design-basis flood must be combined with other loads:

- external loads of normal usage (e.g. operational loads, earth thrust, wind load),
- loads due to the design-basis flooding (e.g. static water pressure due to the design water level, streaming water, waves, upswing, flotsam, ice pressure),
- loads of events as a consequence of the design flooding (e.g. undermining, erosion).

4. Steps of the external flooding analysis

The probabilistic safety assessment of external flooding can be distinguished into four main steps:

- hazard analysis of the site,
- check that starting from an assumed water level of the plant which is equivalent with the design-basis flood, the non-availability of safety functions for the electrical energy supply and for the residual heat removal in a time schedule of five days for river sites and one day for tidal sites is less than 10^{-2},
- analysis of the event sequence and quantification of the contributions to the total frequency of core damage states,
- conduct of an uncertainty analysis.

5. Example of an event in Germany

In Germany, up to now only one event happened (in 2006). The plant was in full power operation. In the control room a flooding was detected by a signal from the reactor building drainage system for the pump room of one of the four nuclear secondary cooling water loops.

At that time, the storm-tide water level was 4.5 m above normal level. The flooding happened through a cable penetration, which was not used anymore. The room contained a drive motor of the secondary cooling water pump and the isolating butterfly valve, driven by a motor, which were both unavailable. The root cause investigation showed that the cover plate to close the cable penetration has loosened. Due to corrosion and the static water pressure on the cover plate the tie-rod of the cover plate screwed up.

As a back fitting measure the unused cable penetration was welded. The damaged electrical components were changed. The check of the other redundancies did not show any comparable conditions.

The event had no large safety significance because three further redundancies of the residual heat removal chain were available. Two chains are already sufficient for a safe shutdown of the plant.

6. Determination of flood runoffs and storm tide water levels with a probability value of 10^{-4}/a

6.1. Basics

The flood protection for nuclear power plants in accordance with [12] presumes a flood event with a probability value (p-value) of 10^{-4}/a, i.e. an extremely seldom flood event. Depending on whether the site is located on inland waters or on coasts with or without tidal waters, different procedures are required for determining the design-basis water level in the vicinity of the plant components to be protected and in the vicinity of the protective structures of the nuclear power plant.

In the case of inland water sites, the base assumption is a flood runoff with this p-value for the respective water body. A procedure for determining such a seldom flood runoff is presented in Section 6.2. In individual cases other site-independent procedures may be employed [13]. For inland water sites both the conditions at the site (maximum possible flow) as well as the large-area water retention effects of the water catchments area (water shed) shall be taken into consideration.

In the case of such a seldom flood event it cannot be assumed that the inland water dyke system in the water catchments area will still be fully effective.

In the case of coastal sites and sites on tidal waters, the base assumption is a storm-tide water level with this probability value. A procedure for determining such a seldom flood level is presented in Section 6.3.

On the basis of the flood runoff or of the storm tide water level, the corresponding site specific water level in the vicinity of the plant components to be protected and the protective structures of the nuclear power plant shall be determined, e.g. by hydraulics calculations.

6.2. Determination of water runoffs for a flood with a probability value of 10^{-4}/a for inland water sites

To determine the decisive water runoff of floods for inland water sites, a statistical extrapolation based on the convention introduced in [13] covering the simultaneous occurrence of unfavourable influences shall normally be employed. In this case the following standardized distribution function shall be employed in its expanded form:

$$HQ_{(10^{-4})} = MHQ + s_{HQ} \cdot k_{(10^{-4})},$$

where

$HQ_{(10^{-4})}$: peak-level water runoff of a flood with a probability value of 10^{-4}, in m³/sec,

MHQ: average peak-level water runoff of a flood over an extended measurement period, in m³/sec,

s_{HQ}: standard deviation of peak-level water runoff of a flood over an extended measurement period, in m³/sec,

$k_{(10^{-4})}$: frequency factor for an event with the probability value 10^{-4}/a.

In this procedure the peak-level water runoff of a flood event with a probability value of 10^{-4}/a is extrapolated from the peak-level water runoff of a flood event with a probability value of 10^{-2}/a. Hereby, it is assumed that the peak-level water runoff of a flood event with a probability value of 10^{-2}/a is determined using standard statistical procedures [5]. The extended extrapolation is then performed using the Pearson-III probability distribution. This is the basis on which the necessary frequency factors are determined. The convention introduced in [13] calls for a maximization of the skewness coefficient, c, to the value of c = 4.

The statistical parameters MHQ and s_{HQ} and the actual skewness coefficient, c, shall be calculated from the observed data of a representative flood level.

The frequency factor, $k_{(10^{-4})}$, shall be calculated as the product of the frequency factor, $k_{(10^{-2})}$, and a quotient, f, as follows:

$$k_{(10^{-4})} = k_{(10^{-2})} \cdot f.$$

The frequency factor, $k_{(10^{-2})}$, for a flood with the probability value of 10^{-2}/a shall be interpolated from *Table 2* based on the actual skewness coefficient, c, of the observed data. The frequency factor may, alternatively, be calculated with sufficient accuracy from the following equation

$$k_{(10^{-2})} = 2.3183 + 0.7725 \times c - 0.0650 \times c^2.$$

The quotient, f, shall be calculated for a maximized skewness coefficient, c = 4, from the frequency factor, $k_{(10^{-4})\max}$, and from the frequency factor, $k_{(10^{-2})\max}$, as follows

$$f = k_{(10^{-4})\max} / k_{(10^{-2})\max} = 12.36/4.37 = 2.8.$$

Both frequency factors are independent of site-specific data.

6.3. Derivation of water levels for a storm tide with a probability value of 10^{-4}/a for coastal sites and sites on tidal waters

The storm tide water levels for nuclear power plants on coastal sites and sites on tidal waters shall normally be derived employing the following statistical extrapolation procedure. The water level for a storm tide with a probability factor of 10^{-4}/a, $\mathrm{SFWH}_{(10^{-4})}$, shall be determined as the sum of a base value, $\mathrm{BHWH}_{(10^{-2})}$, and an extrapolation difference, ED, as follows:

$$\mathrm{SFWH}_{(10^{-4})} = \mathrm{BHWH}_{(10^{-2})} + \mathrm{ED}\ ,$$

where

$\mathrm{BHWH}_{(10^{-2})}$: base value of the water level for a storm tide with a probability value of 10^{-2}/a at the site,

ED: extrapolation difference representing the water level difference between the water level of a storm tide with a probability value of 10^{-4}/a and the base value.

The base value, $\mathrm{BHWH}_{(10^{-2})}$, shall be determined on the basis of a quantitative statistical extreme-value analysis (in accordance, e.g., with [9] and [10]) taking relevant parameters [5] into consideration. The quality of the data shall also be taken into consideration.

The base value can be determined employing suitable statistical procedures, because

- the spread of the base values, $\mathrm{BHWH}_{(10^{-2})}$, is relatively small due to the usually extensive and high quality water-level time series available for coasts and tidal waters,
- the $\mathrm{BHWH}_{(10^{-2})}$ water level as a function of the observation duration of the individual time series still is partly in the interpolation region or in the near extrapolation region,
- the $\mathrm{BHWH}_{(10^{-2})}$ water level is assured by extensive investigations and is verifiable by physical as well as numerical models.

The water-level data shall be homogenized considering that the storm-tide water levels are dependent on the development of the water level at the coast – especially the secular rise of the sea level – as well as on the anthropogenic changes to the tidal waters.

The extrapolation difference for coasts or for the mouths of tidal rivers shall be determined, e.g., in accordance with [9] and [10].

The local tide-related excessive wave amplitude is not included in the extrapolation difference.

Table 2. Frequency factors, k, for an event with a probability factor of 10^{-2}/a and the actual skewness coefficient, c, of the observed data

c	**0.0**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**	
k	2.326	2.399	2.472	2.544	2.615	2.685	2.755	2.823	2.891	2.957	
c	**1.0**	**1.1**	**1.2**	**1.3**	**1.4**	**1.5**	**1.6**	**1.7**	**1.8**	**1.9**	
k	3.022	3.086	3.149	3.211	3.271	3.330	3.388	3.444	3.499	3.552	
c	**2.0**	**2.1**	**2.2**	**2.3**	**2.4**	**2.5**	**2.6**	**2.7**	**2.8**	**2.9**	
k	3.605	3.656	3.705	3.753	3.800	3.845	3.889	3.931	3.973	4.012	
c	**3.0**	**3.1**	**3.2**	**3.3**	**3.4**	**3.5**	**3.6**	**3.7**	**3.8**	**3.9**	**4.0**
k	4.051	4.088	4.124	4.159	4.192	4.224	4.255	4.285	4.314	4.341	4.367

7. Results of a sensitivity study for a flood event with extreme waves in the German north sea

PSA regulations consider extreme events of recurrence intervals of 10000 years. Beside the frequently occurring extreme storm flood events, it has been investigated to which extent other events have to be considered. One example is the possible impact of an extreme wave triggered by an offshore landslide. Geotechnical records give evidence for three tsunamis in the North Sea between 8000 and 1500 years ago [3]. One well-explored source region is the Storegga slide, which was released approximately 8100 cal years bp [14].

In the framework of a dedicated study on behalf of BfS, a numerical model was applied by the Centre of Marine Environmental Sciences (MARUM) of University of Bremen to simulate the propagation and development of extreme waves in the North Sea towards the German Bight.

Based on an implicit finite differences modelling system, a hydrodynamic numerical model of the European continental shelf sea has been set-up in order to provide high-resolution data on the hydrodynamics of the North Sea. The rectilinear spherical grid covers the region between W13/N48 and E13/N62 with a resolution of 2.5nm (1/24°) in the latitudinal and 3.75nm (1/16°) in the longitudinal direction (*Figure. 1*). The model bathymetry was interpolated from sea floor topography derived by satellite altimetry and digitised sea-charts [15]. For this study the propagation of an extreme wave event (tsunami) initiated by a hypothetical slide at the continental margin off the Norwegian continental margin has been simulated. Soliton waves were prescribed as water level boundary conditions at the northern open sea boundary of the model.

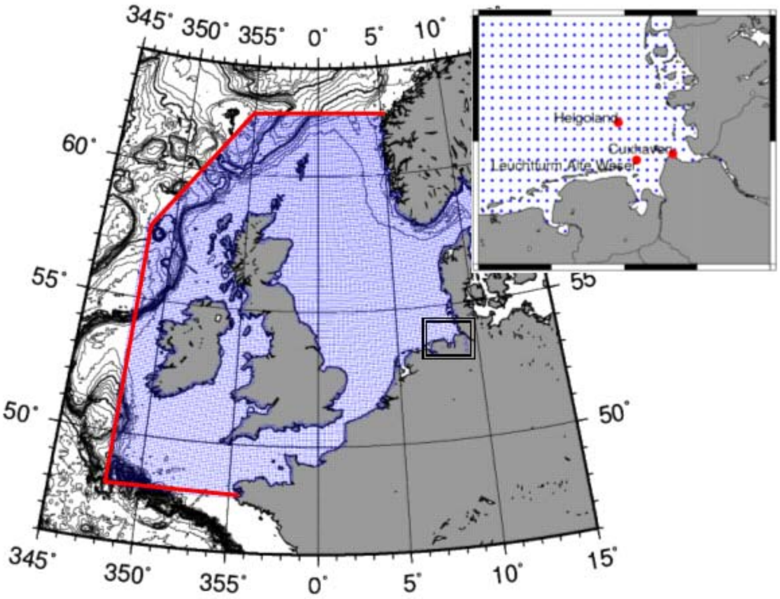


Figure 1. Domain of interest: Model grid nodes are indicated as blue dots. The red line denotes the position of open model boundaries. Tidal gauge stations are chosen for further analysis

As the real height of a possible wave cannot be defined, a range of different wave heights was tested. Simulations show the propagation of the wave across the model domain, considering uniform mean sea level as initial surface elevation condition: After entering the North Sea through the northern boundary, the wave is partly deflected towards the West, because of Coriolis force effects, and partly moves in southern direction through the Norwegian deep. The deflected wave then approaches the British East coast and partly reflects back into the North Sea. Here the primary wave and the reflected wave super-impose into complex patterns. It takes about 8.5 hours for the first wave to reach the German Bight.

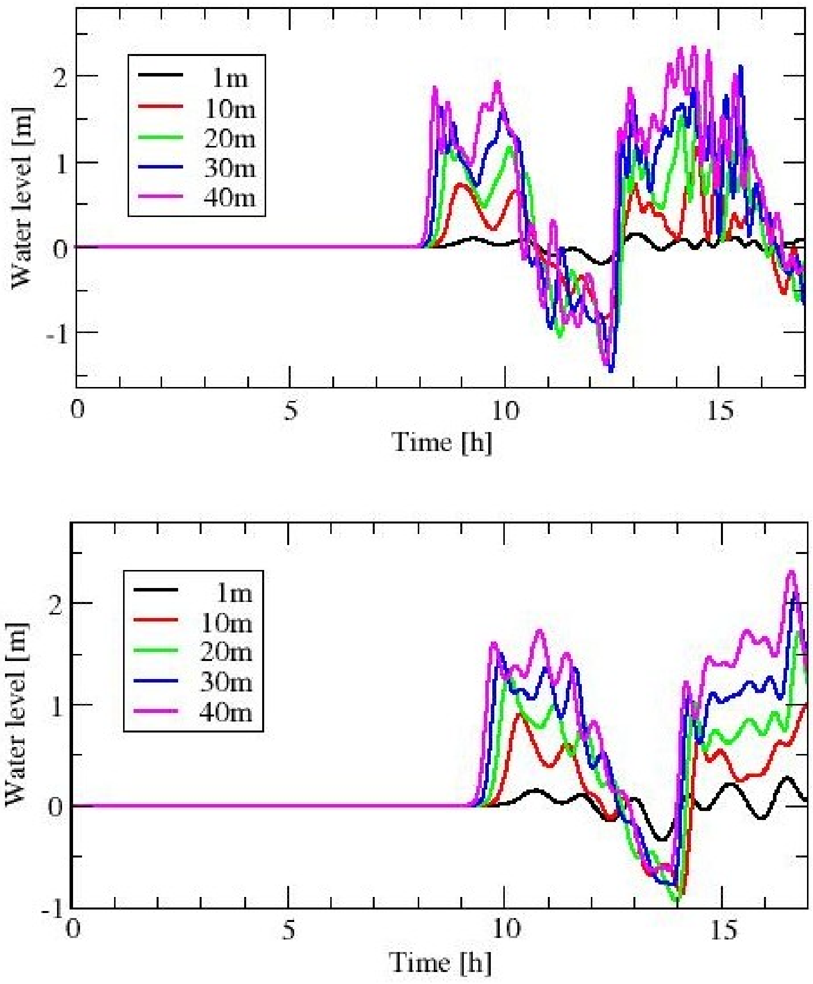


Figure 2. Extreme waves as calculated at the coastal stations featuring the first direct wave and reflected wave

The heights and characteristics of the waves at the three coastal stations are similar, all featuring the first direct wave, and about four hours later the reflected wave, which then reaches higher maximum water levels (*Figure 2*). Generally a significant reduction in wave height from the boundary to the German Bight due to bottom friction can be observed.

The characteristics of the wave triggered by the ancient Storegga event were simulated in [12]. Considering their calculated wave height of 3 meters at the Northern boundary of the model, results in maximum deviations of about 0.5 to 0.7m at the tidal gauges in the German Bight.

In contrast to the simulations described above, the natural hydrodynamics of the North Sea are driven by tidal and meteorological forcing. Thus the super-position of the extreme wave with the astronomical tidal conditions of the North Sea has been simulated (*Figure 3*). Although non-linear effects are present, generally a linear superposition of tidal elevation and extreme wave dimensions based on uniform mean sea level seem to be possible. It is noted that in the German Bight the transformed extreme wave is of much smaller height than the astronomical tidal signal: The effect of an extreme wave at the gauges Helgoland and Cuxhaven results in less than 10% of the tidal range and only one fifth of the expected surface elevation of a light storm flood, as defined by German hydrographic agencies. Similarly at gauge "Alte Weser", the extreme wave is damped to 0.55m, which is about 17 percent of the tidal range and less than one third of a light storm flood.

Considering the natural hydrodynamic conditions as tides and storm surges of the German Bight, the modelled impact of an extreme event that could be triggered by mass slide events at the northern continental margin, seems negligible.

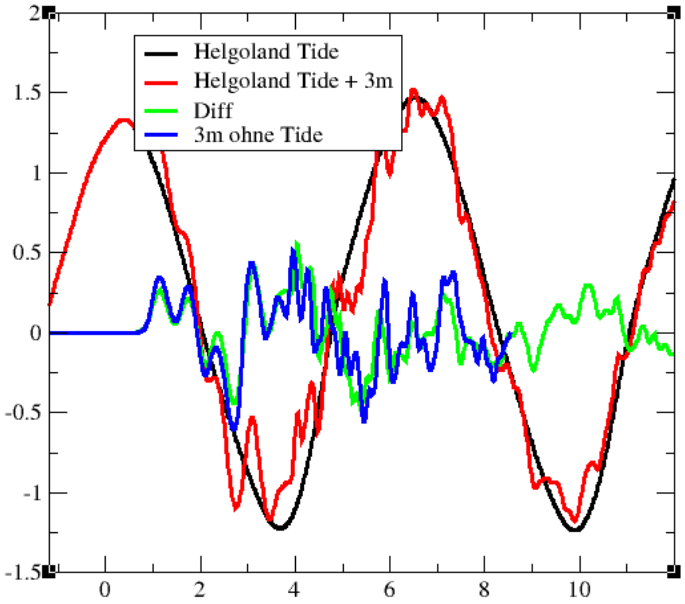


Figure 3. Superposition of tides and extreme wave signal in the German Bight

8. Concluding remarks

The approach for a probabilistic assessment of external hazards to be applied within comprehensive safety reviews of NPP in Germany starts with a screening process, which should not be too conservative so that the number of scenarios and buildings remains manageable for the detailed quantitative analysis. However, it has to be ensured that all relevant areas are investigated within the quantitative analysis. These screening procedures are specific according to the different types of hazards.

However, for those areas which have not been screened out or where a coarse meshed analysis is not sufficient it is compulsory to perform a quantitative analysis as a second step. Finally, the frequency of initiating events induced by the respective hazard, the main contributors and the calculated core damage frequency are determined.

On international level, as already mentioned earlier, there exist some standards and guidelines [1], [8], but they are on a very general level and do not allow to perform a PSA of external flooding in a comparable manner for different plants. Moreover a full scope PSA for external flooding of a nuclear power plant is not available to date.

In Germany the graded process defines only one NPP for which no analysis will be necessary because of its high-grounded level compared with the surroundings. For the other plants probabilistic considerations will be necessary with a different extent of detail.

Compared with other external events (e.g. unintended airplane crash and external pressure wave), which can have frequencies as low as 10^{-7}/a the occurrence frequency of external flooding can be expected substantially higher.

In the case of tidal-river NPPs the value will be higher than the risk of a seismic event due to the seismic situation (Intensity < 6) of the respective sites. The results of a simulation study have shown that an extreme wave in the North Sea towards to the German Bight triggered by an offshore landslide did not indicate significant impacts on the flooding risk of coastal sites. It is not expected that these conditions will be different compared to tidal-river NPP sites, this has, however, to be answered by flood hazard analyses for these sites.

For NPPs in the Southwest of Germany, the contribution of the seismic hazard to the total core damage frequency is expected to be higher compared with external flooding, but the overall core damage frequency remains dominated by internal events and internal hazards.

It should be underlined that the probabilistic assessment of external hazards, although an important part of PSA, has not yet achieved the same level of methodological maturity as being typical for other disciplines of PSA. Therefore, it is intended to conduct a kind of pilot study to get feedback from these analyses for an improvement of the German guidance documents.

However independently from NPPs and other industrial facilities floods from rivers, estuaries and the sea threaten many millions of people in Europe. Flooding is the most widely distributed of all natural hazards across Europe, causing distress and damage wherever it happens.

Previous research has improved understanding of individual factors but many complex interactions need to be addressed for flood mitigation in practice. Thus the first round of the Sixth Framework Programme of the European Commission (2002-2006) included an "Integrated Project" on flood risk management, called FLOODsite.

To achieve the goal of integrated flood risk management, the FLOODsite project has brought together managers, researchers and practitioners from a range of governmental, commercial and research organisations, all devoted to various, but complementary, aspects of flood risk management.

The FLOODsite project covers the physical, environmental, ecological and socio-economic aspects of floods from rivers, estuaries and the sea. The project is arranged into seven themes covering:

- Risk analysis – hazard sources, pathways and vulnerability of receptors.
- Risk management – pre-flood measures and flood emergency management.
- Technological integration – decision support and uncertainty.
- Pilot applications – for river, estuary and coastal sites.
- Training and knowledge uptake – guidance for professionals, public information and educational material.
- Networking, review and assessment.
- Co-ordination and management.

Within these themes there are over 30 project tasks including the pilot applications in Belgium, the Czech Republic, France, Germany (in particular for flood event measures and pilot application sites), Hungary, Italy, the Netherlands, Spain, and the UK. Published results are expected in 2007.

References

[1] ANS, American Nuclear Society (2003). *Draft of the External Events PRA Methodology Standard.* BSR/ANS 58.21-200X.

[2] Berg, H.-P. & Görtz, R. (2006). Probabilistic Safety Assessment of External Flooding of Nuclear Power Plants. *Proc. of the European Safety and Reliability Conference ESREL'06, Safety and Reliability for Managing Risk*, Estoril, Portugal, Vol. 2, Taylor & Francis, London, 1341 – 1346.

[3] Bondevik, S., Løvholt, F., Harbitz, C.B., Mangerud, J., Dawson, A.G. & Svendsen, J.I., (2005). The Storegga Slide Tsunami - Comparing Field Observations with Numerical Simulations. *Marine and Petroleum Geology 22*, 195-208.

[4] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2005). *Safety Review for NPP According to § 19a of the Atomic Energy Act - Probabilistic Safety Assessment Guide* (Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes – Leitfaden Probabilistische Sicherheitsanalyse, 31. Januar 2005, Bekanntmachung vom 30. August 2005, Bundesanzeiger Nr. 207a vom 03.

[5] Deutscher Verband für Wasserwirtschaft und Kulturbau (1999). *Statistical Analysis of Peak Level Water Runoffs* (Statistische Analyse von Hochwasserabflüssen), DVWK-Merkblatt 251.

[6] Facharbeitskreis Probabilistische Sicherheits-analyse für Kernkraftwerke (2005). *Methods for PSA for NPPs* (Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005), BfS-SCHR – 37/05, Salzgitter.

[7] Facharbeitskreis Probabilistische Sicherheits-analyse für Kernkraftwerke (2005). *Data for PSA for NPPs* (Daten zur probabilistischen Sicherheits-analyse für Kernkraftwerke, Stand: August 2005), BfS-SCHR – 38/05, Salzgitter.

[8] International Atomic Energy Agency (2003). *Flood Hazard for Nuclear Power Plants on Coastal and River Sites.* Safety Guide, No. NS-G-3.5, Vienna.

[9] Jensen, J. (2000). Probability of Occurrence of Storm Floods – Statistical View, *HANSA*, Vol 137, Nr. 12, 60 -66.

[10] Jensen, J & Frank, T. (2003). On the Determination of Water Levels from Storm-Floods with a very Small Probability Value, *Die Küste*, Spezialausgabe, Nr. 67.

[11] Jensen, J. et. al. (2003). New Procedures for the Assessment of Rare Water Levels from Storm Floods (Neue Verfahren zur Abschätzung von seltenen Sturmflutwasserständen), *HANSA*, Vol. 140, Nr. 11,68-79.

[12] Kerntechnischer Ausschuss (2004). *Flood Protection of NPP* (Schutz von Kernkraftwerken gegen Hochwasser), KTA 2207.

[13] Kleeberg, H.-B. & Schumann, A. H. (2001). Derivation of Water Runoffs with Small Exceedance Frequencies (Ableitung von Bemessungsabflüssen kleiner Überschreitungswahrscheinlichkeiten), *Wasserwirtschaft*, Vol 21, Nr. 2, 2001, 90 – 95.

[14] Løvholt, F., Harbitz, C.B. & Haugen, K.B. (2005). A Parametric Study of Tsunamis Generated by Submarine Slides in the Ormen Lange/Storegga Area off Western Norway. *Marine and Petroleum Geology 22*, 219-231.

[15] Smith, W. & Sandwell, D. (1997). Global Sea Floor Topography from Satellite Altimetry and Ship Depth Soundings. *Science 277*, 1956–1962

RECURRENT NEURAL NETWORKS FOR DYNAMIC RELIABILITY ANALYSIS

Cadini Francesco, Zio Enrico, Pedroni Nicola

Department of Nuclear Engineering,
Polytechnic of Milan, Milan, Italy

Keywords

dynamic reliability analysis, infinite impulse response-locally recurrent neural network, long-term non-linear dynamics, system state memory, simplified nuclear reactor

Abstract

A dynamic approach to the reliability analysis of realistic systems is likely to increase the computational burden, due to the need of integrating the dynamics with the system stochastic evolution. Hence, fast-running models of process evolution are sought. In this respect, empirical modelling is becoming a popular approach to system dynamics simulation since it allows identifying the underlying dynamic model by fitting system operational data through a procedure often referred to as ‘learning’. In this paper, a Locally Recurrent Neural Network (LRNN) trained according to a Recursive Back-Propagation (RBP) algorithm is investigated as an efficient tool for fast dynamic simulation. An application is performed with respect to the simulation of the non-linear dynamics of a nuclear reactor, as described by a simplified model of literature.

1. Introduction

Dynamic reliability aims at broadening the classical event tree/ fault tree methodology so as to account for the mutual interactions between the hardware components of a plant and the physical evolution of its process variables. The dynamical aspects concern the ordering and timing of events in the accident propagation, the dependence of transition rates and failure criteria on the process variable values, the human operator and control actions. Obviously, a dynamic approach to reliability analysis would not bear any significant added value to the analysis of systems undergoing slow accidental transients for which the control variables do not vary in such a way to affect the component transition rates and/or to demand the intervention of the control.

Dynamic reliability methods are based on a powerful mathematical framework capable of integrating the interactions between the components and the environment in which they function. These methods perform a more realistic modelling of the system and hence improve the quality and accuracy of risk assessment studies. A formal approach to incorporating the dynamic behaviour of systems in risk analysis was formulated under the name Probabilistic Dynamics [10]. Several methods for tackling the solution to the dynamic reliability problem have been formulated over the past ten years [1], [9], [13], [15], [16], [20]. Among these, Monte Carlo methods have demonstrated to be particularly efficient in taking up the numerical burden of such analysis, while allowing for flexibility in the assumptions and for a thorough uncertainty and sensitivity analysis [14], [16].

For realistic systems, a dynamic approach to reliability analysis is likely to require a significant increase in the computational efforts, due to the need of integrating the dynamic evolution, with its characteristic times, with the system stochastic evolution characterized by very different time constants. The fast increase in computing power has rendered, and will continue to render, more and more feasible the incorporation of dynamics in the safety and reliability models of complex engineering systems. In particular, as mentioned above, the Monte Carlo simulation framework offers a natural environment for estimating the reliability of systems with dynamic features. However, the high reliability of systems and components favours the adoption of forced transition schemes and leads, correspondingly, to an increment of the integration of physical models in each trial. Thus, the time-description of the dynamic processes may render the Monte Carlo simulation quite burdensome and it becomes mandatory to resort to fast-running models of process evolution. In these cases, one may resort to either simplified, reduced analytical models, such as those based on lumped effective parameters [2], [7], [8], or empirical models. In both cases, the model parameters have to be estimated so as to best fit to the available plant data.

In the field of empirical modelling, considerable interest is devoted to Artificial Neural Networks (ANNs) because of their capability of modelling non-linear dynamics and of automatically calibrating their parameters from representative input/output data [16]. Whereas feedforward neural networks can model static input/output mappings but do not have the capability of reproducing the behaviour of dynamic systems, dynamic Recurrent Neural Networks (RNNs) are recently attracting significant attention, because of their potentials in temporal processing. Indeed, recurrent neural networks have been proven to constitute universal approximates of non-linear dynamic systems [19].

Two main methods exist for providing a neural network with dynamic behaviour: the insertion of a buffer somewhere in the network to provide an explicit memory of the past inputs, or the implementation of feedbacks.

As for the first method, it builds on the structure of feedforward networks where all input signals flow in one direction, from input to output. Then, because a feedforward network does not have a dynamic memory, *tapped-delay-lines* (temporal buffers) of the inputs are used. The buffer can be applied at the network inputs only, keeping the network internally static as in the buffered multilayer perceptron (MLP) [11], or at the input of each neuron as in the MLP with Finite Impulse Response (FIR) filter synapses (FIR-MLP) [4]. The main disadvantage of the buffer approach is the limited past-history horizon, which needs to be used in order to keep the size of the network computationally manageable, thereby preventing modelling of arbitrary long time dependencies between inputs and outputs [12]. It is also difficult to set the length of the buffer given a certain application.

Regarding the second method, the most general example of implementation of feedbacks in a neural network is the fully recurrent neural network constituted by a single layer of neurons fully interconnected with each other or by several such layers [18]. Because of the required large structural complexity of this network, in recent years growing efforts have been propounded in developing methods for implementing temporal dynamic feedback connections into the widely used multi-layered feedforward neural networks. Recurrent connections can be added by using two main types of recurrence or feedback: *external* or *internal*. *External recurrence* is obtained for example by feeding back the outputs to the input of the network as in NARX networks [5], [17]; *internal recurrence* is obtained by feeding back the outputs of neurons of a given layer in inputs to neurons of the same layer, giving rise to the so called *Locally Recurrent Neural Networks* (*LRNNs*) [6].

The major advantages of LRNNs with respect to the buffered, tapped-delayed feedforward networks and to the fully recurrent networks are [6]: 1) the hierarchic multilayer topology which they are based on is well known and efficient; 2) the use of dynamic neurons allows to limit the number of neurons required for modelling a given dynamic system, contrary to the tapped-delayed networks; 3) the training procedures for properly adjusting the network weights are significantly simpler and faster than those for the fully recurrent networks.

In this paper, an Infinite Impulse Response-Locally Recurrent Neural Network (IIR-LRNN) is adopted together with the Recursive Back-Propagation (RBP) algorithm for its batch training [6]. In the IIR-LRNN the synapses are implemented as Infinite Impulse Response digital filters, which provide the network with system state memory.

The proposed neural approach is applied to a highly non-linear dynamic system of literature, the continuous time Chernick model of a simplified nuclear reactor [8]: the IIR-LRNN is devised to estimate the neutron flux temporal evolution only knowing the reactivity forcing function. The IIR-LRNN ability of dealing with both the short-term dynamics governed by the instantaneous variations of the reactivity and the long-term dynamics governed by *Xe* oscillations is verified by extensive simulations on training, validation and test transients.

The paper is organized as follows: in Section 2, the IIR-LRNN architecture is presented in detail together with the RBP training algorithm; in Section 3, the adopted neural approach is applied to simulate the reactor neutron flux dynamics. Finally, some conclusions are proposed in the last Section.

2. Locally Recurrent Neural Networks

2.1. The IIR-LRNN architecture and forward calculation

A LRNN is a time-discrete network consisting of a global feed-forward structure of nodes interconnected by synapses which link the nodes of the k-th layer to those of the successive (k + 1)-th layer, k = 0, 1, ..., M, layer 0 being the input and M the output. Differently from the classical static feed-forward networks, in an LRNN each synapse carries taps and feedback connections. In particular, each synapse of an IIR-LRNN contains an IIR linear filter whose characteristic transfer function can be expressed as ratio of two polynomials with poles and zeros representing the AR and MA part of the model, respectively.

For simplicity of illustration, and with no loss of generality, we start by considering a network constituted by only one hidden layer, i.e. $M = 2$, like the one in *Figure 1*. At the generic time t, the input to the LRNN consists of a pattern $x(t) \in \Re^{N^0}$, whose components feed the nodes of the input layer 0 which simply transmit in output the input received, i.e. $x^0_m(t) = x_m(t)$, m = 1, 2, ..., N^0. A bias node is also typically inserted, with the index m = 0, such that $x^0_0(t) = 1$ for all values of t. The output variable of the m-th input node at time t is tapped a number of delays L^1_{nm} - 1 (except for the bias node output which is not tapped, i.e. $L^1_{n0} - 1 = 0$) so that from each input node $m \neq 0$ actually L^1_{nm} values, $x^0_m(t)$, $x^0_m(t - 1)$, $x^0_m(t - 2)$, …, $x^0_m(t - L^1_{nm} + 1)$ are processed forward through the synapses connecting input node m to the generic hidden node n = 1, 2, … N^1. The L^1_{nm} values sent from the input node m to the hidden node n are first multiplied by the respective synaptic weights $w^1_{nm(p)}$, p = 0, 1, …, L^1_{nm} - 1 being the index of the tap delay (the synaptic weight $w^1_{n0(p)}$ connecting the bias input node $m = 0$ is the bias value itself) and then processed by a summation operator to give the MA part of the model with transfer function

$$w^1_{nm(0)} + w^1_{nm(1)}B + w^1_{nm(2)}B^2 + ... + w^1_{nm(L^1_{nm}-1)}B^{L^1_{nm}-1}, \tag{1}$$

B being the usual delay operator of unitary step. The finite set of weights $w^1_{nm(p)}$ which appear in the MA model form the so called impulse response function and represent the components of the MA part of the synaptic filter connecting input node m to hidden node n. The weighed sum thereby obtained, y^1_{nm}, is fed back, for a given number of delays I^1_{nm} ($I^1_{n0} = 0$ for the bias node) and weighed by the coefficient $v^1_{nm(p)}$ (the AR part of the synaptic filter connecting input node m to hidden node n, with the set of weights $v^1_{nm(p)}$ being the so-called AR filter's impulse response function), to the summation operator itself to give the output quantity of the synapse ARMA model:

$$y^1_{nm}(t) = \sum_{p=0}^{L^1_{nm}-1} w^1_{nm(p)} x^0_n(t-p) + \sum_{p=1}^{I^1_{nm}} v^1_{nm(p)} y^1_{nm}(t-p). \tag{2}$$

This value represents the output at time t of the IIR-filter relative to the nm-synapse, which connects the m-th input neuron to the n-th hidden neuron. The first sum in (2) is the MA part of the synaptic filter and the second is the AR part. As mentioned above, the index m = 0 usually represents the bias input node, such that $x^0_0(t)$ is equal to one for all values of t, $L^1_{n0} - 1 = I^1_{n0} = 0$ and thus, $y^1_{n0}(t) = w^1_{n0(0)}$.

The quantities $y^1_{nm}(t)$, m = 0, 1, ..., N^0, are summed to obtain the net input $s^1_n(t)$ to the non-linear activation function $f^1(\cdot)$, typically a sigmoid, Fermi function, of the n-th hidden node, n = 1, 2, ...N^1:

$$s^1_n(t) = \sum_{m=0}^{N^0} y^1_{nm}(t). \tag{3}$$

The output of the activation function gives the state of the n-th hidden neuron, $x^1_n(t)$:

$$x^1_n(t) = f^1\left[s^1_n(t)\right]. \tag{4}$$

The output values of the nodes of the hidden layer 1, $x^1_n(t)$, n = 1, 2, …, N^1, are then processed forward along the AR and MA synaptic connections linking the hidden and output nodes, in a manner which is absolutely analogous to the processing between the input and hidden layers. A bias node with index $n = 0$ is also typically inserted in the hidden layer, such that $x^1_0(t) = 1$ for all values of t.

The output variable of the n-th hidden node at time t is tapped a number of delays $L^M_{rn} - 1$ ($= 0$ for the bias node $n = 0$) so that from each hidden node n actually L^M_{rn} values, $x^1_n(t)$, $x^1_n(t-1)$, $x^1_n(t-2)$, …, $x^1_n(t - L^M_{rn} + 1)$, are processed forward through the MA-synapses connecting the hidden node n to the output node $r = 1, 2, ..., N^M$. The L^M_{rn} values sent from the hidden node n to the output node r are first multiplied by the respective synaptic weights $w^M_{rn(p)}$, $p = 0, 1, …, L^M_{rn} - 1$ being the index of the tap delay (the synaptic weight w^M_{r0} connecting the bias hidden node $n = 0$ is the bias value itself) and then processed by a summation operator to give the MA part of the model with transfer function

$$w^M_{rn(0)} + w^M_{rn(1)}B + w^M_{rn(2)}B^2 + ... + w^M_{rn(L^M_{rn}-1)}B^{L^M_{rn}-1} . \quad (5)$$

The sum of these values, y^M_{rn}, is fed back, for a given number of delays I^M_{rn} ($I^M_{r0} = 0$ for the bias node) and weighed by the coefficient $v^M_{rn(p)}$ (the AR part of the synaptic filter connecting hidden node n to output node r, with the set of weights $v^M_{rn(p)}$ being the corresponding impulse response function), to the summation operator itself to give the output quantity of the synapse ARMA model:

$$y^M_{rn}(t) = \sum_{p=0}^{L^M_{rn}-1} w^M_{rn(p)} x^1_n(t-p) + \sum_{p=1}^{I^M_{rn}} v^M_{rn(p)} y^M_{rn}(t-p) . \quad (6)$$

As mentioned before, the index $n = 0$ represents the bias hidden node, such that $x^1_0(t)$ is equal to one for all values of t, $L^M_{r0} - 1 = I^M_{r0} = 0$ and thus, $y^M_{r0}(t) = w^M_{r0(0)}$.

The quantities $y^M_{rn}(t)$, $n = 0, 1, ..., N^1$, are summed to obtain the net input $s^M_r(t)$ to the non-linear activation function $f^M(\cdot)$, also typically a sigmoid, Fermi function, of the r-th output node $r = 1, 2, ..., N^M$:

$$s^M_r(t) = \sum_{n=0}^{N^1} y^M_{rn}(t) . \quad (7)$$

The output of the activation function gives the state of the r-th output neuron, $x^M_r(t)$:

$$x^M_r(t) = f^M\left[s^M_r(t)\right]. \quad (8)$$

The extension of the above calculations to the case of multiple hidden layers ($M > 2$) is straightforward. The time evolution of the generic neuron j belonging to the generic layer $k = 1, 2, …, M$ is described by the following equations:

$$x^k_j(t) = f^k\left[s^k_j(t)\right] (= 1 \textit{ for the bias node}, j = 0) , \quad (9)$$

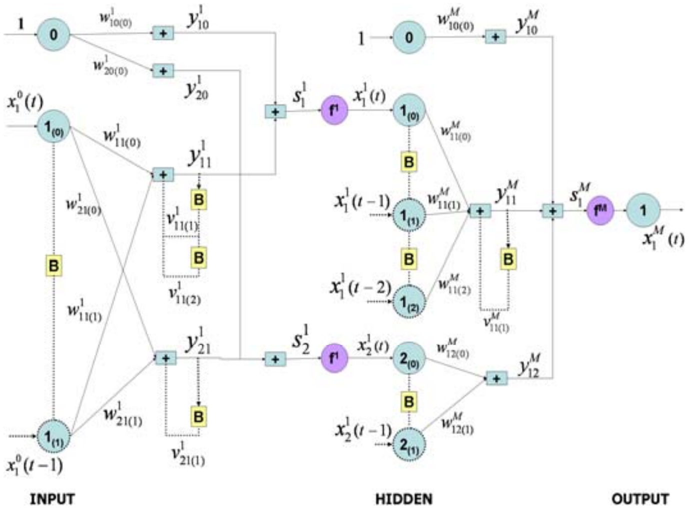
$$s^k_j(t) = \sum_{l=0}^{N^{k-1}} y^k_{jl}(t) , \quad (10)$$

$$y^k_{jl}(t) = \sum_{p=0}^{L^k_{jl}-1} w^k_{jl(p)} x^{k-1}_l(t-p) + \sum_{p=1}^{I^k_{jl}} v^k_{jl(p)} y^k_{jl}(t-p) . \quad (11)$$

Note that if all the synapses contain only the MA part (i.e., $I^k_{jl} = 0$ for all j, k, l), the architecture reduces to a FIR-MLP and if all the synaptic filters contain no memory (i.e., $L^k_{jl} - 1 = 0$ and $I^k_{jl} = 0$ for all j, k, l), the classical multilayered feed-forward static neural network is obtained.

2.2. The Recursive Back-Propagation (RBP) algorithm for batch training

The Recursive Back-Propagation (RBP) training algorithm [6] is a gradient - based minimization algorithm which makes use of a particular chain rule expansion rule expansion for the computation of the necessary derivatives. A thorough description of the RBP training algorithm is given in the Appendix at the end of the paper.



INPUT ($k = 0$)	HIDDEN ($k = 1$)	OUTPUT ($k = 2 = M$)
$N^0 = 1$	$N^1 = 2$	$N^M = 1$
	$L^1_{11} - 1 = 1$ $L^1_{21} - 1 = 1$	$L^M_{11} - 1 = 2$ $L^M_{12} - 1 = 1$
	$I^1_{11} = 2$ $I^1_{21} = 1$	$I^M_{11} = 1$ $I^M_{12} = 0$

Figure 1. Scheme of an IIR-LRNN with one hidden layer

3. Simulating reactor neutron flux dynamics by LRNN

In general, the training of an ANN to simulate the behaviour of a dynamic system can be quite a difficult task, mainly due to the fact that the values of the system output vector $\boldsymbol{y}(t)$ at time t depend on both the forcing functions vector $\boldsymbol{x}(\cdot)$ and the output $\boldsymbol{y}(\cdot)$ itself, at previous steps:

$$\boldsymbol{y}(t) = F(\boldsymbol{x}(t), \boldsymbol{x}(t-1), ..., \boldsymbol{y}(t-1), ..., \boldsymbol{\Theta}), \tag{12}$$

where $\boldsymbol{\Theta}$ is a set of adjustable parameters and $F(\cdot)$ the non-linear mapping function describing the system dynamics.

In this Section, a locally recurrent neural network is trained to simulate the dynamic evolution of the neutron flux in a nuclear reactor.

3.1. Problem formulation

The reference dynamics is described by a simple model based on a one group, point kinetics equation with non-linear power reactivity feedback, combined with Xenon and Iodine balance equations [8]:

$$\Lambda \frac{d\Phi}{dt} = \left[(\rho_0 + \Delta\rho) - \frac{\sigma_{Xe}}{c\Sigma_f} Xe - \gamma\Phi \right] \Phi$$

$$\frac{dXe}{dt} = \gamma_{Xe}\Sigma_f \Phi + \lambda_I I - \lambda_{Xe} Xe - \sigma_{Xe} Xe\Phi \tag{13}$$

$$\frac{dI}{dt} = \gamma_I \Sigma_f \Phi - \lambda_I I$$

where Φ, *Xe* and *I* are the values of flux, Xenon and Iodine concentrations, respectively.

The reactor evolution is assumed to start from an equilibrium state at a nominal flux level Φ_0= $4.66\cdot10^{12}$ *n/cm*^{2}*s*. The initial reactivity needed to keep the steady state is $\rho_0 = 0.071$ and the Xenon and Iodine concentrations are $Xe_0 = 5.73\cdot10^{15}$ *nuclei/cm*^{3} and $I_0 = 5.81\cdot10^{15}$ *nuclei/cm*^{3}, respectively. In the following, the values of flux, Xenon and Iodine concentrations are normalized with respect to these steady state values.

The objective is to design and train a LRNN to reproduce the neutron flux dynamics described by the system of differential equations (13), i.e. to estimate the evolution of the normalized neutron flux $\Phi(t)$, knowing the forcing function $\rho(t)$.

Notice that the estimation is based only on the current values of reactivity. These are fed in input to the locally recurrent model at each time step *t*: thanks to the MA and AR parts of the synaptic filters, an estimate of the neutron flux $\Phi(t)$ at time *t* is produced which recurrently accounts for past values of both the network's inputs and the estimated outputs, viz.

$$\hat{\Phi}(t) = F(\rho(t), \rho(t-1), ..., \hat{\Phi}(t-1), ..., \boldsymbol{\Theta}) \tag{14}$$

where $\boldsymbol{\Theta}$ is the set of adjustable parameters of the network model, i.e. the synaptic weights.

On the contrary, the other non-measurable system state variables, *Xe*(*t*) and *I*(*t*), are not fed in input to the LRNN: the associated information remains distributed in the hidden layers and connections. This renders the LRNN modelling task quite difficult.

3.2. Design and training of the LRNN

The LRNN used in this work is characterized by three layers: the input, with two nodes (bias included); the hidden, with six nodes (bias included); the output with one node. A sigmoid activation function has been adopted for the hidden and output nodes.

The training set has been constructed with $N_t = 250$ transients, each one lasting $T = 2000$ minutes and sampled with a time step Δt of 40 minutes, thus generating $n_p = 50$ patterns. Notice that a temporal length of 2000 minutes allows the development of the long-term dynamics, which are affected by the long-term *Xe* oscillations. All data have been normalized in the range [0.2, 0.8].

Each transient has been created varying the reactivity from its steady state value according to the following step function:

$$\rho(t) = \begin{cases} \rho_0 & t \le T_s \\ \rho_0 + \Delta\rho & t > T_s \end{cases} \tag{15}$$

where T_s is a random steady-state time interval and $\Delta\rho$ is random reactivity variation amplitude. In order to build the 250 different transients for the training, these two parameters have been randomly chosen within the ranges [0, 2000] minutes and $[-5\cdot10^{-4}, +5\cdot10^{-4}]$, respectively.

The training procedure has been carried out on the available data for $n_{epoch} = 200$ learning epochs (iterations). During each epoch, every transient is repeatedly presented to the LRNN for $n_{rep} = 10$ consecutive times. The weight updates are performed in batch at the end of each training sequence of length *T*. No momentum term nor an adaptive learning rate [6] turned out necessary for increasing the efficiency of the training, in this case.

Ten training runs have been carried out to set the number of delays (orders of the MA and AR parts of the synaptic filters) so as to obtain a satisfactory performance of the LRNN, measured in terms of a small root mean square error (RMSE) on the training set.

As a result of these training runs, the MA and AR orders of the IIR synaptic filters have been set to 12 and 10, respectively, for both the hidden and the output neurons.

3.3. Results

The trained LRNN is first verified with respect to its capability of reproducing the transients employed for the training itself. This capability is a minimum requirement, which however does not guarantee the proper general functioning of the LRNN when new transients, different from those of training, are fed into the network. The evolution of the flux, normalized with respect to the steady state value Φ_0, corresponding to one sample training transients is shown in *Figure 2*: as expected, the LRNN estimate of the output (crosses) is in satisfactory agreement with the actual transient (circles).

Notice the ability of the LRNN of dealing with both the short-term dynamics governed by the instantaneous variations of the forcing function (i.e., the reactivity step) and the long-term dynamics governed by *Xe* oscillations.

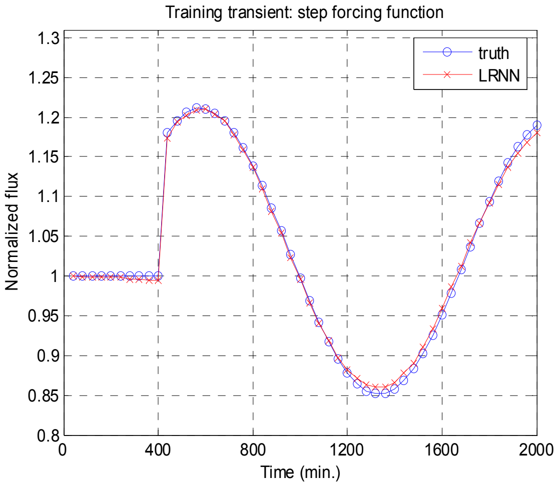


Figure 2. Comparison of the model-simulated normalized flux (circles) with the LRNN-estimated one (crosses), for two sample transients of the training set

3.3.1. Validation phase: training like dynamics

The procedure for validating the generalization capability of the LRNN to transients different from those of training is based on N_t = 80 transients of T = 2000 minutes each, initiated again by step variations in the forcing function $\rho(t)$ as in eq. (15), with timing and amplitude randomly sampled in the same ranges as in the training phase.

The results reported in *Figure 3* confirm the success of the training since the LRNN estimation errors are still small for these new transients. Furthermore, the computing time is about 5000 times lower than that required by the numerical solution of the model. This makes the LRNN model very attractive for real time applications, e.g. for control or diagnostic purposes, and for applications for which repeated evaluations are required, e.g. for uncertainty and sensitivity analyses.

3.3.2. Test phase

The generalization capabilities of the trained and validated LRNN have been then tested on a new set of transients generated by forcing functions variations quite different from those used in both the training and the validation phases. The test set consists of three

transients batches created by three functional shapes of the forcing function $\rho(t)$ never seen by the LRNN:

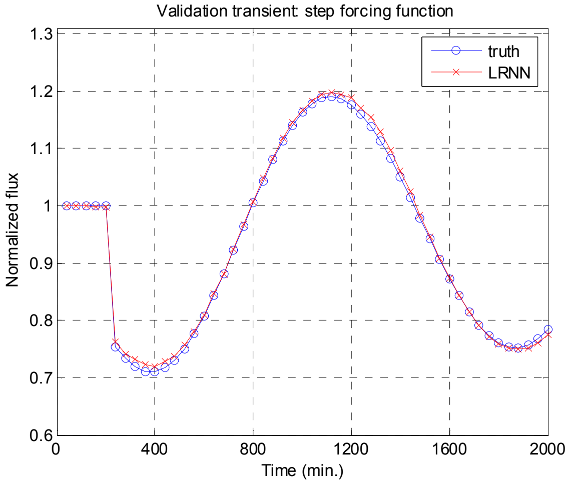


Figure 3. Comparison of the model-simulated normalized flux (circles) with the LRNN-estimated one (crosses), for one sample transient of the validation set

- A ramp function:

$$\rho(t) =$$

$$= \begin{cases} \rho_0, t \le T_s \\ \rho_0 + (\Delta\rho / T_v)t - (\Delta\rho / T_v)T_s, T_s < t \le T_s + T_v \quad (16) \\ \rho_0 + \Delta\rho, t > T_s + T_v \end{cases}$$

where the steady-state time interval T_s ($0 \le T_s \le 2000$ min), the ramp variation time interval T_v ($0 \le T_v \le 2000$ min) and the reactivity variation amplitude $\Delta\rho$ ($-5\cdot10^{-4} \le \Delta\rho \le +5\cdot10^{-4}$) are randomly extracted in their ranges of variation in order to generate the different transients;

- A sine function:

$$\rho(t) = \Delta\rho \cdot \sin(2\pi f t)\,, \qquad (17)$$

where f is the oscillation frequency ($1 \le f \le 2$ min^{-1}) and $\Delta\rho$ ($-5\cdot10^{-4} \le \Delta\rho \le +5\cdot10^{-4}$) is the reactivity variation amplitude;

- Random reactivity variation amplitude with a uniform probability density function between $-5\cdot10^{-4}$ and $+5\cdot10^{-4}$.

A total of N_t = 80 temporal sequences has been simulated for each batch, producing a total of 240 test transients. The temporal length and the sampling time steps of each transient are the same as those of the training and validation sets (2000 and 40 minutes, respectively).

Figures 4, 5 and *Figure 6* show a satisfactory agreement of the LRNN estimation with the model simulation, even for cases quite different from the dynamic evolution considered during training.

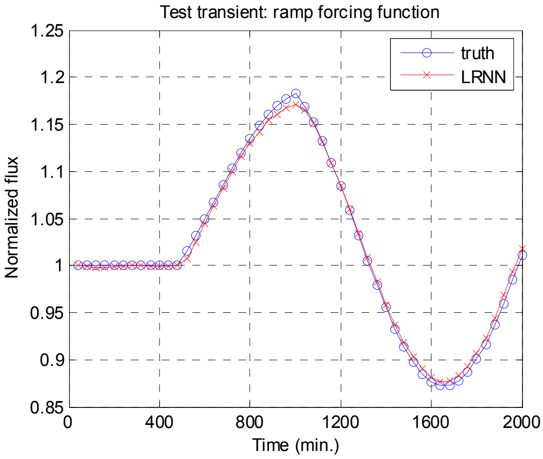


Figure 4. Comparison of the model-simulated normalized flux (circles) with the LRNN-estimated one (crosses), for one sample ramp transient of the test set

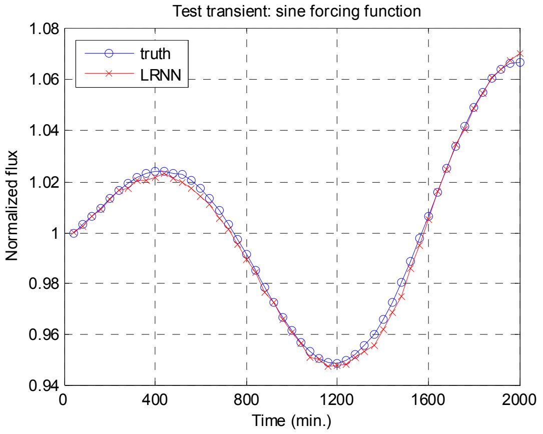


Figure 5. Comparison of the model-simulated normalized flux (circles) with the LRNN-estimated one (crosses), for one sample sinusoidal transient of the test set

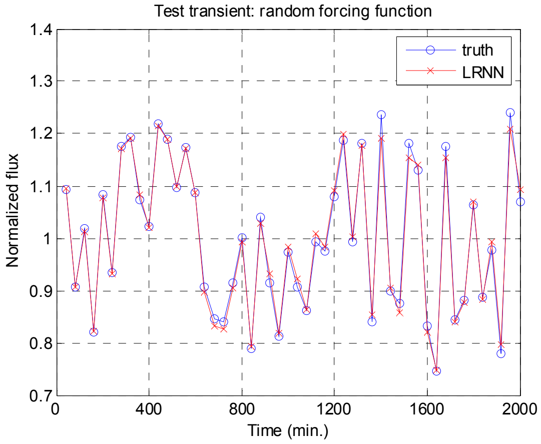


Figure 6. Comparison of the model-simulated normalized flux (circles) with the LRNN-estimated one (crosses), for one sample random transient of the test set

These results are synthesized in *Table 1*, in terms of the following performance indices: root mean square error (RMSE) and mean absolute error (MAE).

Table 1. Values of the performance indices (RMSE and MAE) calculated over the training, validation and test sets for the LRNN applied to the reactor neutron flux estimation

			ERRORS	
Set	***Forcing function***	***n. of sequences***	***RMSE***	***MAE***
Training	Step	250	0.0037	0.0028
Validation	Step	80	0.0098	0.0060
Test	Ramp	80	0.0049	0.0039
	Sine	80	0.0058	0.0051
	Random	80	0.0063	0.0054

4. Conclusion

Dynamic reliability analyses entail the rapid simulation of the system dynamics under the different scenarios and configurations, which occur during the system stochastic life evolution. However, the complexity and nonlinearities of the involved processes are such that analytical modelling becomes burdensome, if at all feasible.

In this paper, the framework of Locally Recurrent Neural Networks (LRNNs) for non-linear dynamic simulation has been presented in detail. The powerful dynamic modelling capabilities of this type of neural networks has been demonstrated on a case study concerning the evolution of the neutron flux in a nuclear reactor as described by a simple model of literature, based on a one group, point kinetics equation with non-linear power reactivity feedback, coupled with the Xenon and Iodine balance equations.

An Infinite Impulse Response-Locally Recurrent Neural Network (IIR-LRNN) has been successfully designed and trained, with a Recursive Back-Propagation (RBP) algorithm, to the difficult task of estimating the evolution of the neutron flux, only knowing the reactivity evolution, since the other non measurable system state variables, i.e. Xenon and Iodine concentrations, remain hidden.

The findings of the research seem encouraging and confirmatory of the feasibility of using recurrent neural network models for the rapid and reliable system simulations needed in dynamic reliability analysis.

References

[1] Aldemir, T., Siu, N., Mosleh, A., Cacciabue, P.C. & Goktepe, B.G. (1994). Eds.: *Reliability and Safety Assessment of Dynamic Process System NATO-ASI Series F*, Vol. 120 Springer-Verlag, Berlin.

[2] Aldemir, T., Torri, G., Marseguerra, M., Zio, E. & Borkowski, J. A. (2003). Using point reactor models and genetic algorithms for on-line global xenon estimation in nuclear reactors. *Nuclear Technology*, 143, No. 3, 247-255.

[3] Back, A. D. & Tsoi, A. C. (1993). A simplified gradient algorithm for IIR synapse multi-layer perceptron. *Neural Comput.* 5: 456-462.

[4] Back, A. D. et al. (1994). A Unifying View of Some Training Algorithms for Multilayer Perceptrons with FIR Filter Synapses. *Proc. IEEE Workshop Neural Netw. Signal Process.*: 146.

[5] Boroushaki, M. et al. (2003). Identification and control of a nuclear reactor core (VVER) using recurrent neural networks and fuzzy system. *IEEE Trans. Nucl. Sci.* 50(1): 159-174.

[6] Campolucci, P. et al. (1999). On-Line Learning Algorithms of Locally Recurrent Neural Networks. *IEEE Trans. Neural Networks* 10: 253-271.

[7] Carlos, S., Ginestar, D., Martorell, S. & Serradell, V. (2003). Parameter estimation in thermalhydraulic models using the multidirectional search method. *Annals of Nuclear Energy* 30, 133-158.

[8] Chernick, J. (1960). The dynamics of a xenon-controlled reactor. *Nuclear Science and Engineering* 8: 233-243.

[9] Cojazzi, G., Izquierdo, J.M., Melendez, E. & Sanchez-Perea, M. (1992). The Reliability and Safety Assessment of Protection Systems by the Use of Dynamic Event Trees (DET). The DYLAM-TRETA package. *Proc. XVIII annaul meeting Spanish Nuclear Society*.

[10] Devooght, J. & Smidts, C. (1992). Probabilistic Reactor Dynamics I. The Theory of Continuous Event Trees, *Nucl. Sci. and Eng.* 111, 3, pp. 229-240.

[11] Haykin, S. (1994). *Neural networks: a comprehensive foundation*. New York: IEEE Press.

[12] Hochreiter, S. & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation,* 9(8): 1735-1780.

[13] Izquierdo, J.M., Hortal, J., Sanchez-Perea, M. & Melendez, E (1994). Automatic Generation of dynamic Event Trees: A Tool for Integrated Safety Assessment (ISA), *Reliability and Safety Assessment of Dynamic Process System NATO-ASI Series F*, Vol. 120 Springer-Verlag, Berlin.

[14] Labeau, P. E. & Zio, E. (1998). The Cell-to-Boundary Method in the Frame of Memorization-Based Monte Carlo Algorithms. A New Computational Improvement in Dynamic Reliability, *Mathematics and Computers in Simulation*, Vol. 47, No. 2-5, 329-347.

[15] Labeau, P.E. (1996). Probabilistic Dynamics: Estimation of Generalized Unreliability Trhough Efficient Monte Carlo Simulation, *Annals of Nuclear Energy*, Vol. 23, No. 17, 1355-1369.

[16] Marseguerra, M. & Zio, E. (1996). Monte Carlo approach to PSA for dynamic process systems, *Reliab. Eng. & System Safety*, vol. 52, 227-241.

[17] Narendra, K. S. & Parthasarathy, K. (1990). Identification and control of dynamical systems using neural networks. *IEEE Trans. Neural Networks* 1: 4-27.

[18] Pearlmutter, B. (1995). Gradient Calculations for Dynamic Recurrent Neural networks: a Survey. *IEEE Trans. Neural Networks* 6: 1212.

[19] Siegelmann, H. & Sontag, E. (1995). On the Computational Power of Neural Nets. *J. Computers and Syst. Sci.* 50 (1): 132.

[20] Siu, N. (1994). Risk Assessment for Dynamic Systems: An Overview, Reliab. Eng. & System Safety, vol. 43, 43-74.

Appendix: the Recursive Back-Propagation (RBP) Algorithm for batch training

Consider one training temporal sequence of length T and denote by $d_r(t)$, $r = 1, 2, \ldots, N^M$, the desired output value of the training sequence at time t.

The instantaneous squared error at time t, $e^2(t)$, is defined as the sum over all N^M output nodes of the squared deviations of the network outputs $x^M{}_r(t)$ from the corresponding desired value in the training temporal sequence, $d_r(t)$:

$$e^2(t) = \sum_{r=1}^{N^M} \left[e_r(t)\right]^2 , \tag{1'}$$

where

$$e_r(t) = d_r(t) - x_r^M(t) . \tag{2'}$$

The training algorithm aims at minimizing the global squared error E^2 over the whole training sequence of length T,

$$E^2 = \sum_{t=1}^{T} e^2(t) , \tag{3'}$$

This is achieved by modifying iteratively the network weights $w^k{}_{jl(p)}$, $v^k{}_{jl(p)}$ along the gradient descent, viz.

$$\begin{aligned} \Delta w^k_{jl(p)} &= -\frac{\mu}{2}\frac{\partial E^2}{\partial w^k_{jl(p)}} , \\ \Delta v^k_{jl(p)} &= -\frac{\mu}{2}\frac{\partial E^2}{\partial v^k_{jl(p)}} , \end{aligned} \tag{4'}$$

where μ is the learning rate.

Introducing the usual *backpropagating error* and *delta* quantities with respect to the output, $x^k{}_j(t)$, and input, $s^k{}_j(t)$, of the generic node j of layer k:

$$e^k_j(t) = -\frac{1}{2}\frac{\partial E^2}{\partial x^k_j(t)} , \tag{5'}$$

$$\begin{aligned} \delta^k_j(t) &= -\frac{1}{2}\frac{\partial E^2}{\partial s^k_j(t)} = -\frac{1}{2}\frac{\partial E^2}{\partial x^k_j(t)}\frac{\partial x^k_j(t)}{\partial s^k_j(t)} \\ &= e^k_j(t) f_k^{'}\left[s^k_j(t)\right], \end{aligned} \tag{6'}$$

the chain rule for the modification (4') of the MA and AR synaptic weights $w^k{}_{jl(p)}$, $v^k{}_{jl(p)}$ can be written as

$$\begin{aligned} \Delta w^k_{jl(p)} &= -\frac{\mu}{2}\sum_{t=1}^{T}\frac{\partial E^2}{\partial s^k_j(t)}\frac{\partial s^k_j(t)}{\partial w^k_{jl(p)}} \\ &= \sum_{t=1}^{T}\mu\delta^k_j(t)\frac{\partial s^k_j(t)}{\partial w^k_{jl(p)}} , \end{aligned}$$

$$\Delta v_{jl(p)}^{k} = -\frac{\mu}{2}\sum_{t=1}^{T}\frac{\partial E^{2}}{\partial s_{j}^{k}(t)}\frac{\partial s_{j}^{k}(t)}{\partial v_{jl(p)}^{k}}$$

$$= \sum_{t=1}^{T}\mu\delta_{j}^{k}(t)\frac{\partial s_{j}^{k}(t)}{\partial v_{jl(p)}^{k}}. \tag{7'}$$

Note that the weights updates (7’) are performed in batch at the end of the training sequence of length *T*. From (10),

$$\frac{\partial s_{j}^{k}(t)}{\partial w_{jl(p)}^{k}} = \frac{\partial y_{jl}^{k}(t)}{\partial w_{jl(p)}^{k}} \quad ; \quad \frac{\partial s_{j}^{k}(t)}{\partial v_{jl(p)}^{k}} = \frac{\partial y_{jl}^{k}(t)}{\partial v_{jl(p)}^{k}}, \tag{8'}$$

so that from the differentiation of (11) one obtains

$$\frac{\partial s_{j}^{k}(t)}{\partial w_{jl(p)}^{k}} = x_{l}^{k-1}(t-p) + \sum_{\tau=1}^{I_{jl}^{k}} v_{jl(\tau)}^{k}\frac{\partial s_{j}^{k}(t-\tau)}{\partial w_{jl(p)}^{k}}, \tag{9'}$$

$$\frac{\partial s_{j}^{k}(t)}{\partial v_{jl(p)}^{k}} = y_{jl}^{k}(t-p) + \sum_{\tau=1}^{I_{jl}^{k}} v_{jl(\tau)}^{k}\frac{\partial s_{j}^{k}(t-\tau)}{\partial v_{jl(p)}^{k}}. \tag{10'}$$

To compute $\delta^{k}_{j}(t)$ from (6’), we must be able to compute $e^{k}_{j}(t)$. Applying the chain rule to (5’), one has

$$e_{j}^{k}(t) = \sum_{q=1}^{N^{k+1}}\sum_{\tau=1}^{T} -\frac{1}{2}\frac{\partial E^{2}}{\partial s_{q}^{k+1}(\tau)}\frac{\partial s_{q}^{k+1}(\tau)}{\partial x_{j}^{k}(t)},\ k < M . \tag{11'}$$

Under the hypothesis of synaptic filter temporal causality (according to which the state of a node at time *t* influences the network evolution only at successive times and not at previous ones), the summation along the time trajectory can start from $\tau = t$. Exploiting the definitions (6’) and (8’), changing the variables as $\tau - p \rightarrow t$ and considering that for the output layer, i.e. $k = M$, the derivative $\partial E^{2}/\partial x^{M}_{j}(t)$ can be computed directly from (2’), the back-propagation of the error through the layers can be derived

$$e_{j}^{k}(t) = \begin{cases} e_{j}(t)\,(eq.2'), k = M \\ \sum_{p=0}^{T-t}\sum_{q=1}^{N^{k+1}} \delta_{q}^{k+1}(t+p)\frac{\partial y_{qi}^{k+1}(t+p)}{\partial x_{j}^{k}(t)}, k < M, \end{cases} \tag{12'}$$

where from (11)

$$\frac{\partial y_{qj}^{k+1}(t+p)}{\partial x_{j}^{k}(t)} = \sum_{\tau=1}^{\min(I_{qj}^{k+1},p)} v_{qj(\tau)}^{k+1}\frac{\partial y_{qj}^{k+1}(t+p-\tau)}{\partial x_{j}^{k}(t)}$$

$$+ \begin{cases} w_{qj(p)}^{k+1}, 0 \le p \le L_{qj}^{k+1} - 1 \\ 0, otherwise. \end{cases} \tag{13'}$$

A METHODOLOGY FOR RATING AND RANKING HAZARDS IN MARITIME FORMAL SAFETY ASSESSMENT USING FUZZY LOGIC

Dourmas N. Georgios, Nikitakos V. Niñitas,
Lambrou A. Maria

University of the Aegean,
Dept. of Shipping Trade and Transport, Chios, Greece

Keywords
decision making, Formal Safety Assessment, hazard identification, marine safety, fuzzy logic

Abstract
Formal safety assessment of ships has attracted great attention over the last few years. This paper, following a brief review of the current status of marine safety assessment is focused on the hazards identification (HAZID) and prioritisation process. A multicriteria decision making framework, which is based on experts' estimation, is then proposed for hazards evaluation. Additionally in this paper many aspects of the evaluation framework are presented including the synthesis of evaluation teams, the assessment of the importance of criteria, the evaluation of the consequences of the alternative hazards and the final ranking of the hazards. The proposed methodology has the innovative feature of embodying techniques of fuzzy logic theory into the classical multicriteria decision analysis. The paper concludes by exploring the potentiality of the above methodology in providing a robust and flexible evaluation framework suitable to the characteristics of a hazard evaluation problem.

1. Introduction

Hazard identification (HAZID) is the first and in many ways the most important step in a risk assessment. This paper, following a brief review of the current status of marine safety assessment is focused on the hazards identification and prioritisation process. Hazard Identification is the process of systematically identifying hazards and associated events that have the potential to result in a significant consequence. The aim of HAZID is first to produce a list of all possible hazards and second to evaluate them in order to prioritise them. In order to support the evaluating procedure we propose as a tool the Multicriteria Decision Analysis (MCDA). The reason is that the final decision depends on criteria, which correlate the potential hazardous scenarios with different consequences.

MCDA deals with the problem of ranking various alternatives in the presence of multiple criteria. Up to now, there are a variety of methods that one can choose from solving a multicriteria decision problem, the most famous being the maximin, the weighted average, the multicriteria utility evaluation and the Analytical Hierarchical Process [13].

All the aforementioned methods assume that the decision maker is able to provide exact assessments on the importance of the importance of evaluation criteria on the impact of alternatives. However, owing to the availability and subjectivity of information, it is very difficult to obtain exact assessment data as concerns the fulfilment of the requirements of the criteria or the relative importance of each criterion. Classical decision-making methodologies are thus criticized for over-simplifying the decision-making process by "forcing" the experts to express their views on pure numeric scales. It is common evidence that assessments made by experts are mostly of subjective and qualitative nature.

Fuzzy sets theory, originally proposed by L. A. Zadeh [22], is an effective means to deal with the "vagueness" of human judgement. This theory offers us tools to handle linguistic terms as the ones mentioned above by converting them to suitable fuzzy sets and numbers. "Fuzzy" multicriteria decision analysis methods allow us to integrate linguistic assessments and weights in a multicriteria decision analysis setting [11], [14].

After fuzzy sets general methodology presentation this paper proposes an application to evaluate and rank a number hazards. We assume a multi-criteria decision making framework, where sets of general and domain-specific criteria are used to judge the relative impact of evaluating hazards. The proposed methodology has the innovative feature of embodying techniques of fuzzy logic theory into the classical multicriteria decision analysis.

2. Hazard identification

Hazard identification (HAZID) is the first and in many ways the most important step in a risk assessment. An overlooked hazard is likely to introduce more error into the overall risk estimate than an inaccurate consequence model or frequency estimate. The aim of the HAZID is to produce, therefore, a comprehensive list of all hazards. The list should include all foreseeable hazards, but it should also avoid double counting by including the same hazard under more than one heading. In order to distinguish between hazards and consequences, it is advisable to start with defining a "hazard". In formal ship safety assessment, a hazard is defined as "a physical situation with potential for human injury, damage to property, damage to the environment or some combination" [12].

Therefore, ship 'grounding' is considered as a possible consequence of hazards related, for example, to navigation error/failure, and not as a hazard itself. Similarly, 'navigation' 'ship manoeuvring', etc. are considered as hazardous operations because a component failure could lead to a chain of unwanted outcomes.

HAZID is concerned with using "brainstorming" technique involving trained and experienced personnel to determine the hazards. HAZID is, most of the time a qualitative exercise strongly based on expert judgement. Many different methods are available for hazard identification and some of them have become standard for particular applications. Experience proved that there is no need to specify which technique should be used in particular cases. Typically, the system being evaluated is divided into parts and the team leader chooses the methodology, which can be standard technique, a modification of one of these or, usually, a combination of several. In other words, the technique used is not that important since each group can follow a methodology of combined techniques. The most important thing is that the HAZID has to be creative in order to obtain comprehensive coverage of hazards skipping as fewer areas as it could practicably be. Also, it is very important that the conclusions of HAZIDs will be discussed and documented during a final session, so that they represent the views of the group rather than of an individual.

Various scientific safety assessment approaches such as Preliminary Hazards Analysis (PHA), Failure Mode, Effects and Criticality Analysis (FMECA) and Hazard and Operability (HAZOP) study can be applied in this step [21].

3. Hazard analysis

Hazard analysis approach is considered a suitable tool for ship safety assessment. In this approach it is assumed that each specific hazard can be represented by one or several threats that have the potential to lead to an incident or top (initiating) event [18]. A threat can be a specific hazard or a more detailed representation of a specific hazard. Each accidental event may lead to unwanted consequences. If a Hazard is released, the accidental event can escalate to one of the several possible consequences. To prevent escalation, the mitigation measures, emergency preparedness and escalation control measures need to be in place to stop chain of events propagation and/or to minimize the consequences of escalation [19]. At the table 1 are described some general hazards, which are analysed in more detailed hazards.

Table 1. List of hazards

General Hazard	Specific Hazard
Impacts and collision	Vessel collision
	Striking while at berth
Ship related	Flooding
	Loading/overloading
Navigation	Navigation error
	Vessel not under command
Manoeuvring	Fine manoeuvring error
	Berthing/unberthing error
Fire/explosion	Cargo tank fire/explosion
	Fire in accommodation
	Other fires
Loss of containment	Release of flammables
	Release of toxic material

4. The building blocks

The evaluation setting assumed through out the paper reflects a rather representative situation faced by hazard evaluators. This is mainly characterized by the following:

- There is a number of hazards and the objective is to evaluate the relative impact for each hazard and finally to provide an ordering from the “highest” (highest score) to the “lowest” (lowest score) of the set of the hazards. The highest hazard is that one which causes the worst consequences.
- For the evaluation process a set of criteria is used, which follows a tree-like structure. The depth of the criteria tree, which somehow reflects the depth of the analysis, is usually not constant but varies with the thematic area under consideration. The totality of evaluation criteria is divided in two clusters: the group of *general* and *thematic* criteria. As the name indicates, the criteria of the thematic class vary with the hazard domain, with the general criteria can be naturally applied to general situations according to type of effects (e.g. safety, property damage, mission interruption, environmental effects e.t.c.).
- A panel of experts is used to evaluate hazards by means of the evaluation criteria hierarchy. Generally, both thematic area and evaluation hierarchy are given in advance and experts are asked either to give their opinion using linguistic terms on the relative importance of the criteria to the overall objective or to the degree at which every hazard appeals to the requirements set by each criterion.

5. Methodology using fuzzy logic

5.1. Fuzzy numbers and arithmetic

When dealing with numeric evaluation data, finding the weighted average of individual scores and aggregating across the hierarchy is more or less a trivial task. However, when dealing with fuzzy “quantities” it is not clear at all what is the outcome of certain expressions, such as “very good” or “very important”. One needs an arithmetic that could suitably generalist basic number operations such as addition or multiplication. The theory of fuzzy sets offers a more systematic framework for handling expert linguistic assessments. This scientific area attempts to capture the “vagueness” that is an inherent characteristic of qualitative appraisals [2], [7], [11], [23].

A fuzzy number is considered as a fuzzy set over the set of all real numbers. Generally, there is much freedom in choosing between different shapes for the membership function (refers to the degree of membership for a fuzzy number, varying from no to full membership and takes rates from 0 to 1) of a fuzzy number. However, simple ones, such as a triangular or trapezoidal, are frequently more convenient to handle.

A trapezoidal (triangular) fuzzy number is a fuzzy number whose membership function forms a trapezium (triangle). Throughout this paper, trapezoidal fuzzy numbers are denoted by ($\alpha_{1,}$ α_2, α_3, α_4), where

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ correspond to the trapezium's angle points ($\alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \alpha_4$). Note that a triangular fuzzy number is a special case of trapezoidal with $\alpha_2=\alpha_3$.

Arithmetic similar to that of real numbers can be also developed by fuzzy numbers by extending the basic algebraic operations of addition, subtraction, multiplication and division. The application of the above operations to fuzzy numbers yields always a new fuzzy number [6]. In the case of trapezoidal fuzzy numbers computations are greatly simplified.

Let $\widetilde{A} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $\widetilde{B} = (b_1, b_2, b_3, b_4)$ be any two strictly positive trapezoidal fuzzy numbers (it is custom in fuzzy sets literature to use '$\sim$' above letters to discriminate fuzzy from crisp quantities). Then, it can be proven that corresponding algebraic operators $\{\oplus, \ominus, \otimes, \varnothing\}$ for fuzzy sets are as follows [3]:

$$\widetilde{A} \oplus \widetilde{B} = (\alpha_1+b_1, \alpha_2+b_2, \alpha_3+b_3, \alpha_4+b_4)$$

$$\widetilde{A} \ominus \widetilde{B} = (\alpha_1-b_1, \alpha_2-b_2, \alpha_3-b_3, \alpha_4-b_4)$$

$$\widetilde{A} \otimes \widetilde{B} = (\alpha_1 x b_1, \alpha_2 x b_2, \alpha_3 x b_3, \alpha_4 x b_4)$$

$$\widetilde{A} \varnothing \widetilde{B} = (\alpha_1/b_4, \alpha_2/b_3, \alpha_3/b_2, \alpha_4/b_1)$$

where the "circle" is used to notify that the operator applies to fuzzy and not ordinary numbers.

5.2. Defuzzification procedure

Going back to the problem of ranking e-services, we see that fuzzy numbers and their arithmetic provide us with a convenient tool for reasoning with qualitative linguistic assessments.

In particular, one could easily represent each linguistic term, such as "poor", "fair", etc., by a fuzzy number on a predefined numeric scale (e.g. 0-1, 0-10). In such a way, one gives rise to a set of *fuzzy weights* and *fuzzy rates*, upon which an assessment scheme can be based. Moreover, the algebra of fuzzy numbers, presented above and in particular the extended operations of addition $\oplus$ and multiplication $\otimes$, provide us with a tool for calculation-weighted averages of linguistic data.

As seen, the overall performance of e-services is given in terms of a fuzzy set, which is somehow expected as any algebraic operation on two arbitrary fuzzy numbers yields always a new one. This "vague" picture of the overall performances generally hinders the task of ranking alternatives, since the ordering of fuzzy numbers is not as obvious as that of real numbers. To overcome difficulties of that kind, several approaches have been proposed in the fuzzy literature, the most common being the *defuzzification*.

Defuzzification is the procedure of selecting the most representative among all members of a fuzzy set. By means of defuzzification we attempt to eliminate the "fuzziness" from a fuzzy set, providing thus a "crisp" result. Probably, the simplest defuzzification technique that one can think of is to choose among all members of a fuzzy set the one with the highest degree of membership. However, a more sophisticated method, which takes into account all the information included in the membership function, is the centre of area or centroid. This is simply the centre of area formed under the membership function. The following equation gives the general formula for calculating the centroid $\overline{x}$ of an arbitrarily shaped membership function $\mu(x)$

$$\overline{x} = \frac{\int_X x\mu(x)dx}{\int_X \mu(x)dx}. \qquad (1)$$

In the formula above, X denotes the referential of the fuzzy set, which in the case of fuzzy numbers is identified with the real line $\Re$. For the trapezoidal fuzzy number ($\alpha_1, \alpha_2, \alpha_3, \alpha_4$) the above formula reduces to [4]:

$$\overline{x} = (\alpha_1+\alpha_2+\alpha_3+\alpha_4)/4 \qquad (2)$$

6. Evaluation framework

We use two variations of the evaluation process, denoted by V.1 and V.2 whose main difference lays in the way the various rating and importance assessments are aggregated to provide a ranking of the alternative hazards.

The separation of the rating from the importance assessment is a means of making the evaluation of hazards as fair and objective as possible. In order to avoid disagreement or discrepancies among evaluation committee's members we selected to follow Delphi method. Generally speaking, the Delphi method is an iterative procedure, which aims at the convergence of various subjective opinions into a more widely acceptable view. In general, a set of assumptions form the basis of our evaluation plan:

- All people being involved in the assessment procedure agree to categorization of hazards, evaluation criteria and assessment terms.
- There are a number of hazards, which are to be ordered from the highly to the least recommended.

6.1. Assessment of criteria importance

In our hazards evaluation project a panel of experts has to evaluate the criteria importance by answering a questionnaire. Despite the numerous books and articles that have been written on the subject, questionnaire design lacks until today a coherent theory [15]. For more details about the topic the interested reader could be referred to bibliography [8], [9], [10], [17].

Evaluator's task is to debate on the linguistic weights of the general and thematic criteria, which have been predetermined. Each expert is asked to assign weights:

- To every pair of general-thematic trees and
- At each node of the hierarchical structure, moving from the lowest to the highest-level criteria.

The importance of every single criterion is evaluated by a closed-format question (or description of the criterion in general), whose answer set includes the five linguistic values: "very low (VL)", "low (L)", "medium (M)", "high (H)", "very high (VH)". From a methodological point of view, those values correspond to a suitably chosen trapezoidal (and triangular) fuzzy numbers on the numeric scale 0-1 (see *Table 2*).

After the assessment has been completed for the totality of thematic areas, a Delphi study is carried out for each thematic area separately, in order that an acceptable level of consensus is achieved.

Table 2. The linguistic rates of criteria importance

Very Low (VL)	(0.0, 0.0, 0.1, 0.3)
Low (L)	(0.1, 0.3, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.5, 0.7)
High (H)	(0.5, 0.7, 0.7, 0.9)
Very High (VH)	(0.7, 0.9, 1.0, 1.0)

6.2. Rating of hazards

Evaluators are asked to give their opinion on the impact of each hazard with respect to the criteria set by the particular evaluation problem. Rates are only given at the lowest level of the general and thematic hierarchy. Rating questionnaires could be very similar (or even the same) in design to those described in the previous section. In order to refer in a subjective attribute of hazard impact we use linguistic terms of consequence assignment (see *Table 3*). The impact for every single criterion is assessed by means of closed-format questions with the answer set: "catastrophic (CA)", "critical (CR)", "significant (SI)", "minor (MI)", "negligible (NE)".

Table 3. Linguistic terms of hazard impacts

Linguistic term	Hazard impact
Negligible	Injury not requiring first aid, no cosmetic vessel damage, no environmental impact, no missed voyages
Minor	Injury requiring first aid, cosmetic vessel damage, no environmental impact, no missed voyages
Significant	Injury requiring more than first aid, vessel damage, some environmental damage, a few missed voyages or financial loss
Critical	Severe injury, major vessel damage, major environmental damage, missed voyages
Catastrophic	Loss of life, loss of vessel, extreme environmental impact

Each of the above linguistic terms corresponds to a fuzzy number on the numeric rating scale 0-10. Details of the correspondence are given in *Table 4*.

After the assessment has been completed for the totality of evaluators, a Delphi study is carried out for each hazard separately. The information described above together with the proper criteria weights is used in the next phase of the evaluation problem: the hierarchy aggregation.

Table 4. The linguistic rates of hazards impact

Negligible (NE)	(0, 0, 1, 3)
Minor (MI)	(1, 3, 3, 5)
Significant (SI)	(3, 5, 5, 7)
Critical (CR)	(5, 7, 7, 9)
Catastrophic (CA)	(7, 9, 10, 10)

6.3. Hierarchy aggregation

All have discussed by far refer to the first stage of methodology, the acquisition data. In that part, procedures were less standardized and automated, due to the strong involvement of human expertise. From this stage onwards, tasks tend to be of more algorithmic nature, which definitely calls for the use of specially designed computer programs for performing the required computations.

The steps following the data acquisition could be summarized in two phases:

- Phase I: The evaluation of the aggregate performance of each hazard.
- Phase II: The ranking of hazards with respect to their overall rate.

Those are, according to H. J. Zimmerman, the two typical stages of a multicriteria decision-making problem in which fuzzy sets are used in the assessment process [18]. It is worth mentioning that in most classical (non-fuzzy) multicriteria methods, the results of phase I are numeric scores. Hence, phase II becomes a trivial task, as for the ranking of hazards all that is needed is the pair wise comparison of scores.

However, in fuzzy multicriteria analysis, the situation is more perplexed. Usually, the overall impact of hazards is described by a fuzzy number or a fuzzy set in general, which calls for an additional technique for "removing" the fuzziness and providing a crisp result.

Generally, many approaches have been proposed in the literature that addresses the issues of the overall rating and ranking of alternatives when fuzzy sets are involved in the decision-making process. For an overview of different approaches the reader could refer to several extensive surveys [15]. In the proposed methodology is used a technique that is based on the idea of weighted averaging, properly adjusted to fuzzy numbers [4], [5], [7], [20]. Is proposed the implementation of two variations of the weighted-average scheme (referred V.1 and V.2), whose difference mainly lies at the stage where defuzzification is applied. Those variations are described below in detail.

Variation V.1

In the first variation, is applied a fuzzy weighted averaging scheme for evaluating the aggregate impact of hazards. For each hazard we compute a weighted average of fuzzy linguistic rates, where each rate is multiplied by a suitable fuzzy linguistic weight. In variation V.1 the aggregate impact of hazards is given in terms of a fuzzy score. Therefore, defuzzification is applied to obtain a single numeric value from each fuzzy score. Those values are then used for ranking hazards.

To give a more concrete presentation of the method, let us assume that for the arbitrary thematic area (say *XYZ*), the evaluation criteria hierarchy is given, consisting of both the general and the *XYZ* criteria tree. Let the overall evaluation hierarchy comprise *K* branches in total, which is also the number of both end-criteria and rates per hazard. Then, the following algorithm is followed:

1. Form the evaluation matrix:

$$\begin{array}{c|cccc}
 & B_1 & B_2 & \cdots & B_K \\
\hline
H_1 & \tilde{r}_{11} & \tilde{r}_{12} & \cdots & \tilde{r}_{1K} \\
H_2 & \tilde{r}_{21} & \tilde{r}_{22} & \cdots & \tilde{r}_{2K} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
H_m & \tilde{r}_{m1} & \tilde{r}_{m2} & \cdots & \tilde{r}_{mK}
\end{array}$$

Where by B_K, *k*=1,2,…,*K* we denote the branches of the criteria tree and by H_i, *i*=1,2,…,*m* the hazards to be evaluated. Every element $\tilde{r}_{ik}$ of the matrix corresponds to the rate achieved by hazard H_i for the particular sub-criterion that lies at the end of branch B_k. The entries of the evaluation matrix are chosen from the set of linguistic rates (“very poor (VP)”, “poor (P)”, “fair (F)”, “good (G)”, “very good (VG)”), which correspond, to the trapezoidal fuzzy numbers presented in Table 2.

2. For obtaining the weight $\tilde{\omega}_k$ that corresponds to rate $\tilde{r}_{ik}$, trace down the evaluation criteria tree by following the *k* branch. For every node of the branch that is visited, adjust $\tilde{\omega}_k$ by multiplying with the fuzzy weight assigned to this node.
3. The aggregated fuzzy rates $\tilde{s}_i$, *i*=1,2,…,*m* are obtained by multiplying the evaluation matrix with the vector of fuzzy weights:

$$\tilde{s} = \begin{pmatrix} \tilde{s}_1 \\ \tilde{s}_2 \\ \vdots \\ \tilde{s}_m \end{pmatrix} = \begin{pmatrix} \tilde{r}_{11} & \tilde{r}_{12} & \cdots & \tilde{r}_{1K} \\ \tilde{r}_{21} & \tilde{r}_{22} & \cdots & \tilde{r}_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{r}_{m1} & \tilde{r}_{m2} & \cdots & \tilde{r}_{mK} \end{pmatrix} \otimes \begin{pmatrix} \tilde{\omega}_1 \\ \tilde{\omega}_2 \\ \vdots \\ \tilde{\omega}_{\mathrm{K}} \end{pmatrix}$$

where ⊗ denotes the product operation for fuzzy matrices, which works exactly the same as in ordinary matrix algebra. Note that every $\tilde{s}_i$, *i*=1,2,…,*m* is a trapezoidal fuzzy number.

4. In order to obtain an ordering on the set of hazards, apply the defuzzification formula for trapezoidal membership functions (eq. 2). The defuzzification values are used for ranking hazards from the highest to the lowest impacting.

Variation V.2

In the second variation, the various fuzzy linguistic assessments (rates and weights) are a priori defuzzified by using the “centre of gravity” technique. The aggregate impact of each hazard is found by computing weighted averages of defuzzified rates. The numeric scores obtained are used for ranking purposes. More precisely, let us again assume that the overall evaluation criteria tree consists of *K* branches, B_1, B_2,..., B_K. Suppose that there are also *m* hazards, H_i, *i*=1,2,…,*m* to be evaluated. Then, the procedure followed is:

1. Given the fuzzy rates of each e-service, apply the “centre of gravity” defuzzification technique to obtain a set of numeric rates r_{ik} , *i*=1,2,…,*m* and *k*=1,2,…,*K* ($\tilde{r}_{ik}$ denotes the numeric score achieved by hazard

H_i for the sub-criterion that lies at the end of branch B_k). Use these rates to form the following evaluation matrix:

$$\begin{array}{c|cccc} & B_1 & B_2 & \cdots & B_K \\ \hline H_1 & r_{11} & r_{12} & \cdots & r_{1K} \\ H_2 & r_{21} & r_{22} & \cdots & r_{2K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H_m & r_{m1} & r_{m2} & \cdots & r_{mK} \end{array}$$

2. Given the fuzzy weights, applying to the particular evaluation hierarchy, use the “centre of gravity” to obtain numeric weights for each node of the evaluation tree. Tracing down each branch *k*=1,2,…,*K* and multiplying the numeric weights assigned to each node, find the value of ω_k that multiplies each of r_{ik}, *i*=1,2,…,*m*.
3. A crisp aggregate score s_i for each hazard H_i, is obtained by computing the weighted average of r_{ik}, *k*=1,2,…,*K*. In matrix form:

$$s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_m \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1K} \\ r_{21} & r_{22} & \cdots & r_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mK} \end{pmatrix} \bullet \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_K \end{pmatrix}$$

4. Hazards H_i, *i*=1,2,…,*m* are ranked by means of their aggregate score.

7. Conclusion

In this paper we present an innovative methodological approach to the evaluation, ranking and selection of hazards. The proposed methodology introduces a hierarchical analysis of the decision-making problem, in which general and domain specific criteria compose the evaluation structure. The adopted “fuzzy” approach provides us with a suitable tool for modelling and processing linguistic assessments and subjective views in a simple and rather intuitive way.

Apart from methodological issues, this paper also discusses many practical aspects of the evaluation framework and gives multiple guidelines on how such an evaluation procedure could be implemented. Nevertheless, is obvious that the proposed framework is of more general use. Most important it gives enough flexibility in modelling an evaluation problem, since it affectively remains insensitive to changes in many individual components of the methodology.

References

[1] Baas, S. & Kwakernaak, H. (1977). Rating and ranking of multiple-aspect alternatives using fuzzy sets. *Automatica 13*, 47-58.

[2] Bellman, R. & Zadel, L. (1970). Decision-making in a fuzzy environment. *Management Science 17,* 4, 141-164.

[3] Chen, C. (1998). A study of fuzzy group decision-making method. In *1998 6th National Conference on Fuzzy Sets and Its Applications*, vol. 142, pp.174-186.

[4] Cheng, C. & Lin, Y. (2002). Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation. *European Journal of Operational Research 142*, 174-186.

[5] Dong, W., Shah, H. & Wong, F. (1985). Fuzzy computations in risk and decision analysis. *Civil Engineering Systems 2* , 201-208.

[6] Dubois, D. & Prade, H. (1978). Operations on fuzzy numbers. *Int. J. Syst. Sci.9,* 3, 613-626.

[7] Dubois, D. & Prade, H. (1980). Fuzzy Sets and Systems: Theory and Applications. Vol.144 of *Mathematics in Science and Engineering.* Academic Press Inc., U.S.

[8] Gendall, P. (1998). A framework for questionnaire design: Labaw revisited. *Marketing Bulletin 9*, 28-39.

[9] Hague, P. (1993). *Questionnaire Design.* Kogan Page, London, England.

[10] Labaw, P. J. (1980). *Advanced Questionnaire Design.* Abt Books, Cambridge, MA.

[11] Liang, G. S. & Wang, M. J. (1991). A fuzzy multi-criteria decision making method for facility site selection. *International Journal of Production Research*, 29 (11): 2313-2330.

[12] MSA. (1993). Formal Safety Assessment MSC66/14. Submitted by the United Kingdom to IMO Maritime Safety Committee.

[13] Nikitakos, G., Dounias, N. & Thomaidis, N. S. (2002). D3.1: Evaluation guidelines. Technical report, contributing to work package III *European R&D Results-Assessment and Evaluation* of DIAS.net project (project no. IST-2001-35077).

[14] Prabhu, T. S. & Vizayakumar, K. (1996). Fuzzy hierarchical decision making (FHDM): A methodology for technology choice. *International Journal of Computer Applications in Technology*, 9(5): 322-329.

[15] Ribeiro, R. (1996). Fuzzy multiple attribute decision making: A review and new preference elicitation techniques. *Fuzzy Sets and Systems 78*, 155-181.

[16] Student Researcher: Online Survey Solutions. *Questionnaire Design.* Educational Website. http:// www.studentresearcher.com.

[17] Sudman, S. & Bradburn, N. M. (1983). *Asking Questions: A Practical Guide to Questionnaire Design*. Jossey-Bass, San Francisco, CA.

[18] THESIS Version 2.02 (1998). The Health, Environment and Safety Information System, User Guide, EQE International, July.

[19] Trbojevic, V. M. & Carr, B. J. (2000). Risk based methodology for safety improvements in ports. *Journal of Hazardous Materials* 71, 467-480.

[20] Tseng, T. Y. & Klein, C. (1992). A new algorithm for fuzzy multicriteria decision making. *International Journal of Approximating Reasoning 6*, 45-66.

[21] Wang, J. (2001). The current status and future aspects in Formal Ship Safety Assessment. *Safety Science* 38, 19-30.

[22] Zadeh. L. A. (1965). Fuzzy Sets. *Information and Control 8*, 338-353.

[23] Zadeh, L. (1973). Outline of a new approach to the analysis of complex systems and decision processes. *IEEE Trans. Syst. Man Cybern. SMC-3,* 1, 28-44.

[24] Zimmermann, H. J. (1987). *Fuzzy Sets, Decision Making and Expert Systems.* International Series in Management Science/ Operations Research. Kluwer Academic, Dordrecht.

RISK PREDICTION FOR MODERN TECHNOLOGICAL SYSTEMS

Duffey Romney B.
Atomic Energy of Canada Limited,
Chalk River, ON, Canada

Saull John W.
International Federation of Airworthiness,
East Grinstead, UK

Keywords
technological systems, risk, outcome, failure, error, events, probability

Abstract
We have already examined the worldwide trends for outcomes (measured as accidents, errors and events) using data available for large complex technological systems with human involvement. That analysis was a dissection of the basic available, published data on real and measured risks, for trends and inter-comparisons of outcome rates. We found and showed how all the data agreed with the learning theory when the accumulated experience is accounted for. Here, learning includes both positive and negative feedback, directly or indirectly, as a result of prior outcomes or experience gained, in both the organizational and individual contexts. Our purpose here and now is to try to introduce some predictability and insight into the risk or occurrence of these apparently random events. In seeking such a general risk prediction we adopt a fundamental theoretical approach that is and must be testable against the world's existing data. Comparisons with outcome error data from the world's commercial airlines, the two shuttle failures, and from nuclear plant operator transient control behaviour, show a reasonable level of accord. The results demonstrate that the risk is dynamic, and that it may be predicted using the MERE learning hypothesis and the minimum failure rate, and can be utilized for predictive risk analysis purposes.

1. The risk prediction purpose

Modern technological systems fail, sometimes with catastrophic consequences, sometimes just everyday injuries and deaths. The risk is given by the probability of failure, error or more generally any outcome. Recently the crash of the NASA Space Shuttle *Columbia*, the great blackout of the North East USA and Canada, the explosion at the Texas City refinery all occurred. Other smaller but also key accidents have also occurred: the midair collision over Europe of two aircraft carrying the latest collision avoidance system; the glider landing of a jet aircraft out of fuel in the Azores; a concrete highway overpass collapsing in Laval, Quebec; the huge oil tank fire in England; more ships sinking, more trains derailing, even more cars colliding, and evermore medical errors. We have already examined the worldwide trends for outcomes (measured as accidents, errors and events) using data available for large complex technological systems with human involvement. That analysis was a dissection of the basic available, published data on real and measured risks, for trends and inter-comparisons of outcome rates. We found and showed how all the data agreed with the learning theory when the accumulated experience is accounted for. Here, learning includes both positive and negative feedback, directly or indirectly, as a result of prior outcomes or experience gained, in both the organizational and individual contexts as in [5]. Our purpose here and now is to try to introduce some predictability and insight into the risk or occurrence of these apparently random events. In seeking such a general risk prediction we adopt a fundamental theoretical approach that is and must be testable against the world's existing data.

2. What we must predict

We have shown how outcomes develop in phases from a string or confluence of factors too complex to predict but always avoidable. The bright feature is that we now know that a universal learning curve (ULC) exists and we can utilize that to predict outcome rates and track our progress as we improve. We can therefore start to manage the risk, but only if we include the human element.

We need to make it entirely clear what we do not propose. We will not use the existing idea of analysing human reliability and errors on a task-by-task, item-by-item, situation-by-situation basis. In that approach, which is commonly adopted as part of probabilistic safety analysis using event sequence "trees", the probability of a correct or incorrect action is assigned at each significant step or branch point in the hypothesized evolution of an accident sequence. The probability of any action is represented and weighted or adjusted by situational multipliers, representing stress, environment and time pressures. We suggest, at least for the present, that it is practically *impossible* to try to describe all the nuances, permutations and possibilities behind human decision-making. Instead, we treat the homo-technological system (HTS) as an integral system. We base our analysis on the Learning Hypothesis, invoking the inseparability of the human and the technological system. Using the data, we invoke and use experience as the correct measure of integrated learning and decision-making opportunity; and we demonstrate that the HTS reliability and outcome probabilities are dynamic, simply because of learning.

The basic and sole assumption that we make every time and everywhere is the "learning hypothesis" as a physical model for human behaviour when coupled to any system. Simply and directly, we postulate that humans learn from their mistakes (outcomes) as experience is gained. So, the rate of reduction of outcomes (observed in the technology or activity as accidents, errors and events) is proportional to the number of outcomes that are occurring.

That learning occurs is implicitly obvious, and the reduction in risk must affect the outcome rate directly. To set the scene, let us make it clear that the probability of error is quite universal, and can affect anyone and everyone in a homo-technological system (HTS). There are clear examples of highly skilled well-trained operators, fully equipped with warning and automated systems. So all the people involved (from maintenance, ground control, management, airline operator and the pilots) are working in an almost completely safe industry (ACSI).

Two aircraft examples are very basic to safety: loss of fuel while in flight, and mid-air collision. Given all the systems put in place to avoid these very obvious and fundamental risks, the outcomes still occurred. But despite all the effort, procedures and warnings, there is loss of control through loss of understanding, communication and information in the most modern of aircraft which were maintained to the highest standards. We need to estimate their chance of occurrence of the outcomes, and define the risk by finding the probability of the outcomes due to the human errors embedded in the HTS.

Let us start with the learning hypothesis applied and applicable to any integrated (total) HTS. Thus, the human error or technological system failure or outcome rate, λ, is equivalent to a dynamic hazard function $h(\varepsilon)$ which varies with experience, ε, as given by the Minimum Error Rate Equation (MERE):

$$d\lambda/d\varepsilon = - k (\lambda - \lambda_m) \qquad (1)$$

where k is the learning rate constant, and λ_m the minimum obtainable rate. The failure or outcome rate as a function of experience, $\lambda(\varepsilon)$, is then obtained by straightforward integration as,

$$\lambda(\varepsilon) = \lambda_m + (\lambda_0 - \lambda_m) e^{- k\varepsilon} \qquad (2)$$

where the outcome or failure rate $\lambda \equiv h(\varepsilon)$, the hazard function; λ_m is the minimum obtainable rate at large experience; and λ_0 is the initial rate at some initial experience, ε0.

Here, it will be remembered that the failure or outcome rate is the summation of all the ith rates in the technological system, so that effectively:

$$\lambda(\varepsilon) - \lambda_m = \Sigma_i (\lambda_i - \lambda_m) \qquad (3)$$

Since the MERE result describes and agrees with a wide range of actual data, we hypothesize that this is indeed the correct form for the human error or outcome rate in a HTS with learning. This form has been used to derive the ULC, validated by obtaining failure rates from the world accident, injury and event data.

In terms of the number of failures, errors or observed outcomes, N_j, then we have when sampling the j^{th} observation interval the hazard function or failure rate:

$$\lambda(\varepsilon) = \{(1/(N - N_j))\ (dN_j/d\varepsilon)\} \tag{4}$$

where N is the total number of outcomes and $A \equiv dN_j/d\varepsilon$, the instantaneous outcome rate, IR, and the number of outcomes we have observed over all prior intervals is just the summation, $n \equiv \Sigma_j N_j$.

3. The probability linked to the rate of errors

Given the outcome rate, now we need to determine the outcome (error) probability, or the chance of failure.

a. the hazard function is equivalent to the *failure or outcome rate* at any experience, $\lambda(\varepsilon)$, being the relative rate of change in the reliability with experience, $1/R(\varepsilon)\ (dR(\varepsilon)/d\varepsilon)$;
b. the *CDF or outcome fraction*, $F(\varepsilon)$, is just the observed frequency of prior outcomes, the ratio n/N, where we have recorded n, out of a total possible of N outcomes;
c. the *frequency of prior outcomes* is identical to the observed *cumulative prior probability*, $p(\varepsilon)$, and hence is the CDF, so $F(\varepsilon) = p(\varepsilon) = (n/N) = 1 - R(\varepsilon)$;
d. here $R(\varepsilon)$ is the *reliability,* 1-n/N, a probability measure of how many outcomes or failures did *not* occur out of the total;
e. the *future (or Posterior) probability*, p(P) is proportional to the Prior probability, $p(\varepsilon)$ times the Likelihood, p(L), of future outcomes;
f. the chance of an outcome in any small observation interval, is the PDF $f(\varepsilon)$, which is just the rate of change of the failure or outcome fraction with experience, $dp(\varepsilon)/d\varepsilon$;
g. the *Likelihood,* p(L) is the ratio, $f(\varepsilon)/F(\varepsilon)$, being the probability that an outcome will occur in some interval of experience, the PDF, to the total probability of occurrence, the CDF; and
h. we can write the PDF as related to the failure rate integrated between limits from the beginning with no experience up to any experience, ε,

$$f(\varepsilon) = dF/d\varepsilon = \lambda(\varepsilon) \exp - \int_0^{\varepsilon} \lambda(\varepsilon)\, d\varepsilon. \tag{5}$$

So, the probability of the outcome or error occurring in or taking less than ε, is just the CDF, $p(\varepsilon) = n/N$, conventionally written as $F(\varepsilon)$. Relating this to the failure rate, via (a) through (d) above, gives:

$$p(\varepsilon) \equiv F(\varepsilon) = 1 - e^{-\int \lambda d\varepsilon} \tag{6}$$

where, of course from the MERE,

$$\lambda(\varepsilon) = \lambda_m + (\lambda_0 - \lambda_m) \exp - k(\varepsilon - \varepsilon_0) \tag{7}$$

and $\lambda(\varepsilon_0) = \lambda_0$ at the initial experience, ε_0, accumulated up to or at the initial outcome(s). The corresponding PDF $f(\varepsilon)$, is the probability that the error or outcome occurs in the interval dε, derived from the change in the CDF failure fraction with experience, or from (f), (h) and (g) above:

$$f(\varepsilon) = dF(\varepsilon)/d\varepsilon = dp(\varepsilon)/d\varepsilon = \lambda e^{-\int \lambda d\varepsilon} = \lambda(\varepsilon) \text{ x } (1 - p(\varepsilon))$$

$$= \{(\lambda_m + (\lambda_0 - \lambda_m) \exp(-k(\varepsilon - \varepsilon_0))\} \text{ x } \{\exp((\lambda(\varepsilon)$$

$$- \lambda_0)/k - \lambda_m(\varepsilon_0 - \varepsilon))\} \tag{8}$$

The limits are clear: as experience becomes large, ε→∞, or the minimum rate is small, $\lambda_m << \lambda_0$, or the value of k varies, etc. We can also show that the uniform probability assumption for *observing* outcomes is consistent with the systematic variation of the outcome probability with experience due to *learning*.

We can also determine the maximum and minimum risk likelihood's, which are useful to know, by differentiating the probability expression. The result shows how the risk rate systematically varies with experience and that the most likely trend is indeed given by the learning curve. In other words, we learn as we gain experience, and then reach a region of essentially no decrease, in rate or in probability, and hence in likelihood. It is easy to obtain the first decrease in rates or probabilities but harder to proceed any lower. This is exactly what is observed in transport, manufacturing, medical, industrial and other accident, death and injury data [2].

4. The initial failure rate and its variation with experience

Having established the learning trend, we need to determine the actual parameters and values using data and insight. Now, in reality, the initial rate, λ_0, is *not* a constant as assumed so far since the outcomes are stochastic in experience "state space". Hence, $\lambda_0 = \lambda(\varepsilon_0)$, and it is not known when exactly in our experience we may have an error initially observed (and we might be lucky or not), and the initial value we ascribe to the initial rate observe is an arbitrary value.

To establish the initial rate, key data are available from commercial aircraft outcomes (fatal crashes) throughout the world. The major contributor is human error not equipment failure, although these latter can also be ascribed to the root cause of human failings. Fatal crashes and accidents for the thirty years between 1970 and 2000 are known [1], for 114 major airlines with ~725 million hours (Mh) of total flying experience. For each airline with its own experience, ε, the fatal accident rate per flying hour, $\lambda(\varepsilon)$, can be plotted as an open circular symbol in Figure 1 versus the accumulated experience in flying hours (adopting the FAA value of ~31/3 hours as an average flight time).

These are:

a) the crash of the supersonic *Concorde* with a rate, λ_0, of one in about 90,000 flights shown as a lozenge symbol; and

b) the explosion and disintegration of the space shuttles, *Challenger* and *Columbia,* with a rate, λ_0, of two out of 113 total missions, plotted using the triangular symbol. The typical "flight time" for the shuttle was taken as the 30-40 minutes for re-entry as reported by NASA [4] timelines, although this plot is quite insensitive to the actual value taken.

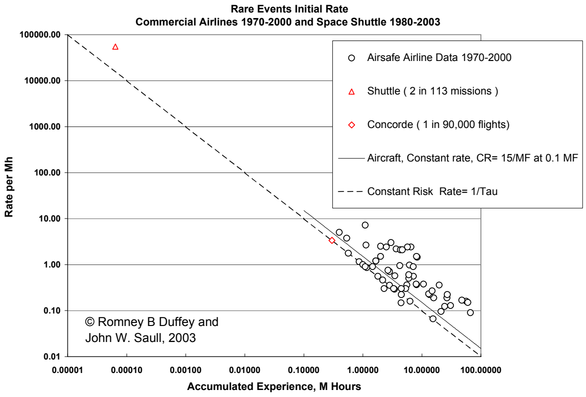


Figure 1. The initial rate based on world airline and US space shuttle accident data

For all these data and experience, there is a remarkable constancy of risk, as shown by the straight line of slope –1, which is given by the equation:

$$\lambda\varepsilon = \text{constant, n,} \tag{9}$$

where the observed rate is strictly a function of whatever experience it happened to occur at, any value being possible. Thus, in the limit for *rare events,* the initial rate should be the purely Bayesian estimate from the prior experience with n ~1 and $\lambda_0 \approx (1/\varepsilon)$. This rate varying as (1/ε) also corresponds *exactly* to the risk rate that is attainable on the basis of the minimum likelihood determined from the outcome probability. What the data are telling us is that the limiting initial rate is exactly what it is for the experience at which the first outcome occurs, no more and no less.

From the analysis of many millions of data points that include human error in the outcomes, we have been able to derive the key quantities that dominate current technological systems. These now include commercial air, road, ship and rail transport accidents; near-misses and events; chemical, nuclear and industrial injuries; mining injuries and manufacturing defects; general aviation events; medical misadministration and misdiagnoses; pressure vessel and piping component failures; and office paperwork and quality management systems [2].

From all these data, and many more, we have estimated the minimum failure rate or error interval, the typical initial error interval, and the learning rate constant for the ULC as follows:

a) minimum attainable rate, λ_m, at large experience, ε, of about one per 100,000 to 200,000 hours ($\lambda_m \sim 5.10^{-6}$ per hour of experience);
b) initial rate, λ_0, of 1/ε, at small experience (being about one per 20,000 to 30,000 hours or $\lambda_0 \sim 5.10^{-5}$ per hour of experience);
c) learning rate constant, k ~ 3, from the ULC fit of a mass of available data worldwide for accidents, injuries, events, near-misses and misadministration.

Therefore, the following numerical dynamic form for the MERE human error or outcome rate is our "best" available estimate [2]:

$$\lambda(\varepsilon) = \lambda_m + (\lambda_0 - \lambda_m)\, e^{-k\varepsilon}, \qquad (10)$$

which becomes, for $\lambda_0 = (n/\varepsilon)$, with n = 1 for the initial outcome,

$$\lambda = 5.10^{-6} + (1/\varepsilon - 5.10^{-6})\, e^{-3\varepsilon} \qquad (11)$$

The rate, λ, can be evaluated numerically, as well as the probability, p(ε), and the differential PDF, f(ε). The result of these calculations is shown in *Figure 2*, where ε ≡ τ units in order to represent the accumulated experience scale.

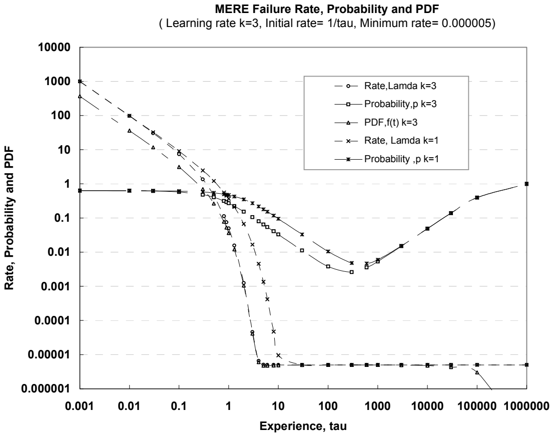


Figure 2. The best MERE values

It is evident that for k>0 the probability is a classic "bathtub" shape, being just under near unity at the start (*Figure 2*), and then falling with the lowering of error rates with increasing experience. After falling to a low of about one in a hundred "chance" due to learning, it rises when the experience is ε > 1000 tau units, and becomes a near certainty again by a million tau units of experience as failures re-accumulate, since $\lambda_m \sim 5.10^{-6}$ per experience tau unit. The importance of learning is evident, since for k<0 forgetting causes a rapid increase to unity probability with no minimum. The solution for the maximum likelihood for the outcome rate is exponential, falling with increasing experience as given by: (Rate for Maximum Likelihood)

$$\lambda_{max} = \lambda_0 \exp - \{k(\varepsilon - \varepsilon_0)/(1 + k\varepsilon_0)\} \qquad (12)$$

However, the expression that gives the minimum likelihood indicates that the *minimum risk* rate is bounded by: (Rate for Minimum Likelihood)

$$\lambda_{min} << \{ \lambda_m \}/ \{1 + k(\varepsilon - \varepsilon_0) \} \quad (13)$$

The result follows common sense. Our maximum risk is dominated by our inexperience at first, and then by lack of learning, and decreasing our risk rate largely depends on attaining experience. Our most likely risk rate is extremely sensitive to our learning rate, or k value, for a given experience.

So, as might be logically expected, the *maximum likelihood for outcomes occurs at or near the initial event rate when we are least experienced.* This is also a common sense check on our results: *we are most at risk at the very beginning.* Therefore, as could have been expected, the most likely and the least risks are reduced only by attaining increasing experience and with increased learning rates.

This approach to reduce and manage risk should come as no surprise to those in the education community, and in executive and line management positions. *A learning environment has the least risk.*

5. Future event estimates: the past predicts the future

The probability of human error, and its associated failure or error rate, we expect to be unchanged unless dramatic technology shifts occur. We can also estimate the likelihood of another event, and whether the MERE human error rate frequency gives sensible and consistent *predictions*. Using Bayesian reasoning, the posterior or future probability, p(P), of an error when we are at experience, ε, is,

$$\text{Posterior, } p(P) \propto \{\text{Prior, } p(\varepsilon)\} x \{\text{Likelihood, } p(L)\} \quad (14)$$

where p(ε) is the prior probability, and by definition both |P,L| > ε, our present accumulated experience**.** The likelihood, p(L), is also a statistical estimate, and we must make an assumption, based on our prior knowledge, and often is taken as a uniform distribution. We can show that the likelihood is formally related to the number of outcomes for a given variation of the mean.

Either:

a) the future likelihood is of the same form as experienced up to now; and/or
b) the future is an unknown statistical sample for the next increment of experience based on the differential probability, the PDF f(ε).

In the first case (a), we have that the future likelihood probability p(L) is the fraction or ratio of events remaining to occur out of the total possible number that is left. For the second case (b), the future is an unknown statistical sample for the next increment of experience based on the PDF, f(ε). This is called a "conditional probability", where the probability of the next outcome depends on the prior ones occurring, which was Bayes original premise.

The so-called generalized *conditional* probability or Likelihood, p(L), can be defined utilizing the CDF and PDF expressions. Described by [6] as the "generalized Bayes formula", the expression given is based on the prior outcome having already occurred with the prior probability p(ε). This prior probability then gives the probability or Likelihood of the next outcome, p(L), in our present experience-based notation, as:

$$p(L) = \equiv \text{PDF/CDF}\} \equiv = \lambda\{(1-p(\varepsilon))/p(\varepsilon)\} \quad (15)$$

We can evaluate this Bayesian likelihood and posterior expressions using our "best" MERE values of a learning rate constant of k=3 and a minimum failure rate of $\lambda_m = 5.10^{-6}$, obtaining the results shown in *Figure 3.*

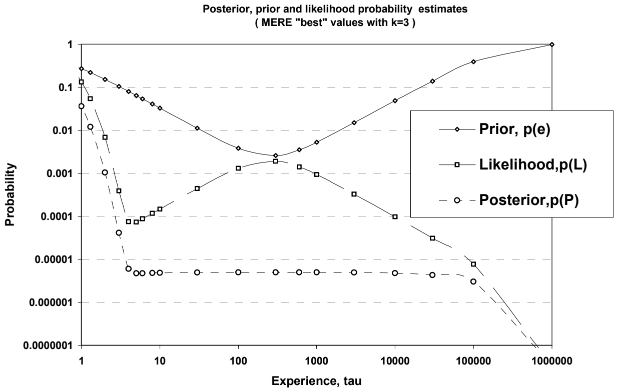


Figure 3. The estimate of the likelihood and posterior probabilities when learning

It is clear from *Figure 3* that the “human bathtub” prior probability, p(ε), causes the likelihood to fluctuate up and down with increasing experience. The likelihood tracks the learning curve, then transitions via a bump or secondary peak to the lowest values as we approach certainty (p→1) at large experience. However, the posterior probability, p(P), just mirrors and follows the MERE failure rate, as we predicted, decreasing to a minimum value of $\sim 5.10^{-6}$, our ubiquitous minimum outcome rate, before finally falling away.

Hence, since the future probability estimate, the posterior p(P), is once again derivable from its (unchanged) prior value, $f(\varepsilon) = dp(\varepsilon)/d\varepsilon \sim \lambda(\varepsilon)$, derived from learning from experience, and thus *the past predicts the future*.

For the special case of “perfect learning” when we learn from all the non-outcomes as well as the outcomes, the Poisson-type triple exponential form applies for low probabilities and small numbers of outcomes ($n<<m$). Of course, the limit of “perfect learning” is when we have an outcome, so here $p(\tau) = 1/\tau$, and is the rare event case for n = 1. The Perfect Learning limit fails as soon as we have an event, as it should. But there is also a useful simple physical interpretation, which is that:

a) we learn from non-outcomes the same way we learn from outcomes, as we have assumed;
b) the perfect learning ends as soon as we have just a single (rare) outcome; and
c) the influence of the finite minimum rate is then lost.

6. Comparison to data: the probability of failure and human error

There are three data sets for catastrophic events with defined large human error contributions that are worth re-examining further:

a) the crash rate for global commercial airlines, noting most occur during manoeuvring and approach for take-off and landing but as we have seen can also occur in flight;
b) the loss of the space shuttles, *Challenger* and *Columbia*, also on take-off and during the approach for landing; and
c) the probability of non-detection by plant operators of so-called latent (hidden) faults in the control of nuclear system transients.

Apparently disparate, these three all share the *common element of human involvement* in the management, design, safety “culture”, control and operation of a large technological system; all are subject to intense media and public interest; and the costs of failure are extremely expensive and unacceptable in many ways.

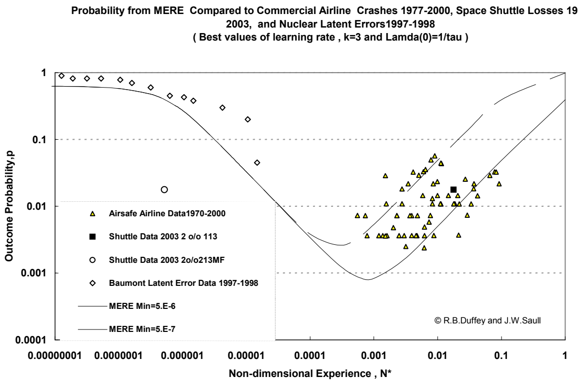


Figure 4. An outcome probability data comparison

The comparison of the data to theory is shown in *Figure 4* where the lines are the MERE calculated probability, p(ε) using the “best” values. The three lines use three bounding values for the minimum error rate to illustrate the sensitivity. Despite the scatter, a minimum rate of order ~5.10^{-6} is indeed an upper bound value, as we estimated before.

7. Implications for generalized risk prediction

The implications of using this new approach for estimating risk are profound.

This new probability estimate is based on the failure rate describing the ULC, which is derived from the Learning Hypothesis; and utilizes the validation from the outcome data of the world’s homo-technological systems. Thus, we have seamlessly linked all the way from individual human actions to the observed outcomes in entire systems. We have unified the approach to managing risk and error reduction using the Learning Hypothesis with the same values everywhere for the learning rate constant, k, and the minimum error rate, λ_m.

For the first time, we are also able to make predictions of the probability of errors and outcomes for any assumed experience interval in any homo-technological system.

Typically the probabilities for error are ~ 10^{-2}, or one in a few hundred, for any act of volition beyond the first 10% or so of the risk interval; whereas in that first increment or initial phase, the risk is much higher. Interestingly, this reduction in probability in the initial interval echoes, parallels and is consistent with the maze study results of Fang [3] showed a rapid (factor of five or so) reduction in the first 10% or so of the moves needed for success by the “treasure hunt” players. Clearly the same fundamental learning factors and success motivation is at work, and are reflected in the rapid decrease in errors down the learning curve.

Conversely, the MERE probability (the human bathtub) properly represents the data trends, such as they are, and hence can be used in PRA HEP estimation provided the correct measure is taken for experience.

In an addition the MERE results implies a finite lower bound probability of p(ε) >10^{-3}, based on the best calculations and all the available data.

8. Conclusions: the probable risk

Analysis of failure rates due to human error and the rate of learning allow a new determination of the risk due to dynamic human error in technological systems, consistent with and derived from the available world data. The basis for the analysis is the “learning hypothesis” that humans learn from experience, and consequently the accumulated experience defines the failure rate. The exponential failure rate solution of the Minimum Error Rate Equation defines the probability of human error as a function of experience.

Comparisons with outcome error data from the world’s commercial airlines, the two shuttle failures, and from nuclear plant operator transient control behaviour, show a reasonable level of accord. The results demonstrate that the risk is dynamic, and that it may be predicted using the learning hypothesis and the minimum failure rate, and can be utilized for predictive risk analysis purposes.

References

[1] Airsafe (2000). Fatal Events and Fatal Event Rates from 1970-2000, September, http://www.airsafe.com.

[2] Duffey, R.B. & Saull, J.W. (2002). *Know the Risk.* First Edition, Butterworth and Heinemann, Boston, USA.

[3] Fang, Christina. (2003). Stern School of Business, New York. Learning in the absence of feedback, unpublished MS.

[4] NASA. Implementation Plan for Return to Flight, National Aeronautics and Space Administration, http://www1.nasa.gov).

[5] Ohlsson, S. (1996). Learning from Performance Errors. *Psychological Review*, Vol. 103, No. 2, 241-262.

[6] Sveshnikov, A.A. (1968). Problems in Probability Theory, Mathematical Statistics and the Theory of Random Functions. Dover, New York.

THE SHIPS IMPACT IN GROUND OF PORT WATER AREA

Galor Wiesław

Maritime University of Szczecin, Poland

Keywords
navigational risk, ship impact in the bottom, port water area

Abstract

The existing ports are expected to handle ships bigger than those for which they were designed. The main restriction in serving these ships is the depth of port waters, which directly affects the safety of a manoeuvring ship. The under keel-clearance of a ship in the port water area should be such that a ship moves safely. In some specific conditions it happen the ship strike the sea bottom. The undesired impact against the ground can damage the ship hull. The paper presents the algorithm of ships movement parameters during contact with the ground

1. Introduction

The world fleet tends to expand in terms of total capacity, with vessels growing in size, while their number is maintained on a similar level. The building of new ports is restricted on the one hand by natural conditions of sea areas, and necessary large financial effort on the other hand. As economic and geopolitical conditions change, directions of cargo transport (bulk in particular) also change, sometimes in a cycle lasting a few years. This in turn, makes building new ports a risky enterprise for investors, as the invested capital return amounts to at least twenty years. Therefore, a need arises to use the existing ports for handling ships larger than those the ports are designed for.

This objective can be achieved through changes in operating conditions within ports and the modernization of certain components of port basins and areas. These measures should results in ports handling ships as large as possible on condition that specified safety level is maintained.

Safe manoeuvring of a ship within a given area requires that the manoeuvring area of a ship with a specific draft is comprised within available port water area having a required depth.

There are two undesired types of events [2] that can lead to a navigational accident within a port area:

- impact on the shore (or another port structure),
- contact with the area bottom.

In the former case the area depth is sufficient, whereas the horizontal dimension is too small. In the latter case the ship's draft is too deep in comparison with the basin depth. This relation is defined by the distance of the lowest point of the ship bottom to the basin bottom, usually referred to as the under keel clearance or water depth under ship's keel.

2. Under keel clearance

The under keel clearance (UKC) is used for the description of the criterion of safe manoeuvring in a port area [3]. This criterion is most often expressed in this way:

$$H - T \geq R_{min} \tag{1}$$

where:

H – water area depth,
T – ship's maximum draft,
R_{min} – safe under keel clearance.

R_{min} is the value of minimum under keel clearance of a ship manoeuvring within a given area that is to assure the ship safety that is no contact of ship's hull with the bottom should occur [5]. This clearance is also called the required or safe water clearance.

The objective function can be written as:

$$UKC = R_{min} \rightarrow min \tag{2}$$

with the restrictions

$$R \le R_{dop} \tag{3}$$

where:

R – risk of manoeuvring in an area,
R_{dop} – admissible navigational risk defined at an acceptable loss level,

where:

$$R_{dop} = P[Z_c(t) \le R_{min} \ / \ 0 \le t \le t_p] \text{ for } C \le c_{min} \tag{4}$$

where:

$Z_c(t)$ – the list distance between ships hull and bottom during manoeuvring
R_{min} – under keel clearance
C – losses,
c_{min} – acceptable level of losses.

There are cases where a ship's hull harmlessly penetrates the bottom up to 40 cm. obviously it is possible only if the bottom ground is properly loose (sand, mud etc.). Therefore, it is possible to predict the minimum value of UKC for a certain risk level. It should be emphasized here that the adoption of such assumptions can have another effect, namely certain ships will not be allowed to enter the port due to environmental conditions (mainly water level and waves). The ship will have to wait for the conditions to improve. In tidal ports whether a ship may enter or leave a port depends on the so-called tidal window with waiting time amounting to several hours. The losses arising from the fact that a ship hits the ground while moving, such as hull damage or, possibly, loss of cargo (particularly liquid cargo, which may pollute the marine environment) depend on a number of factors, which can be expressed by a variety of measures. The one of these is maximum ship hull load less than admissible value caused damage of its.

3. The probability of ship damage

As research shows [6], situations when a ship's hull touches the sea bottom do not often result in serious damage. Only incidents in which the ship's hull is damaged are regarded as accidents. The damage may be of various kinds:

- tearing of bottom plating,
- crushing of deck,
- folding of web frames,
- stretching of shell plating.

The kind and degree of hull damage depends mainly on the energy absorbed by the hull when hitting the bottom. The measure of hull damage used for the

assessment of the impact is the volume of damaged hull material. The relationship combining the absorbed energy and the degree of damage has been empirically worked out [6]:

$$E = 47.2 \cdot R_T - 37.2 \tag{5}$$

where:

E - energy absorbed by the hull during impact
R_T - degree of damage of hull material.

This empirical relation has been determined from the observations of the effects of numerous collisions and is used for the assessment of collision effects.

The relation shows that the degree of damage increases in direct proportion with the energy absorbed by the ship's hull during the impact against an obstruction. This is, undoubtedly, a simplified approach as the quantity of absorbed energy depends on a lot of factors, but mainly on the structure of the ship's hull bottom, material properties and the type of damage. Therefore, further research is carried out to determine as accurately as possible the relation between the absorbed energy and the hull material damage, which would account for the above conditions. The energy absorbed by the ship's hull hitting the bottom is equal to the work done by the ship during the impact. The energy mainly depends on the force appearing between the hull and the bottom. It is difficult to define the force and its curve as the function of time by analytical methods. Therefore, simpler methods based on empirical research data are used. The empirical equation given below presents the energy of impact dependent on ship's mass and the velocity at the moment of impact. The vertical component of ship's velocity should be taken into account in these calculations:

$$E_v = m_s V_v^{\,2} / 2 \tag{6}$$

where:

E_v - energy absorbed during impact;
m_s- ship's mass
V_v - vertical components of ships velocity.

The consequences arising from the fact that a ship hits the ground while moving, such as hull damage or, possibly, loss of cargo (particularly liquid cargo, which may pollute the marine environment) depend on a number of factors which can be expressed by a variety of measures [1].

The maximum ship hull load for such a case can be defined as:

$$P_k(t) = 1 - \exp(-t(t_c)) \tag{7}$$

where:

t_c – period in which the pre-set hull load will be exceeded during the hull impact against the bottom.

$$t_c = [P/1 - P_k(P_u)]^{-1} \tag{8}$$

where:

$P_k(P_u)$ – probability of the hull load higher than admissible during its impact against the bottom.

$$P_k(P_u) = P\lfloor Q_{sgr} \geq Z_G \rfloor \tag{9}$$

where:

Q_{sgr} – admissible pressure on ship's hull,
Z_G – passive earth pressure.

While determining the probability of ship hull damage during the impact one should take into account that not every such impact ends in a serious accident. Therefore:

$$P_{uw} = P_u \cdot P_k(P_u) \tag{10}$$

where:

P_{uw} – probability of an accident during ship's manoeuvres,

P_u – probability of a ship's touching the bottom.

The probability of ship's impact against the bottom may be assumed as a criterion for the evaluation of the safety of ship manoeuvres within port waters.

From statistical data displaying the number of damaged hulls against the number of impacts against the bottom (damage indicator), the probability of hull damage can be replaced by the hull damage indicator. Then the probability of an accident will be equal to:

$$P_{uw} = P_u \cdot w_w \tag{11}$$

where:

w_w – hull damage indicator.

Determinate the probability of accident for given number of ship transits it can used the following formula [3]:

$$P_{A(N)} = N \cdot p_A = I \cdot T \cdot p_A \tag{12}$$

where:

$P_{A(N)}$ – probability of accident for given ship transit number,
p_A – probability of accident in one transit,
N – number of transits.

This relationship is linear because implies proportional growth of probability to considered of ship number transit. More adequate manner is use the statistical models described the accident probability [4]. Because accidents are infrequent events thus it can be used recurrent models. One of them is geometrical distribution:

$$P_{A(N)} = 1 - (1 - p_A)^N \tag{13}$$

Figure 1 presents the probability of navigation accident for linear and geometrical distributions in function of ships transit numbers.

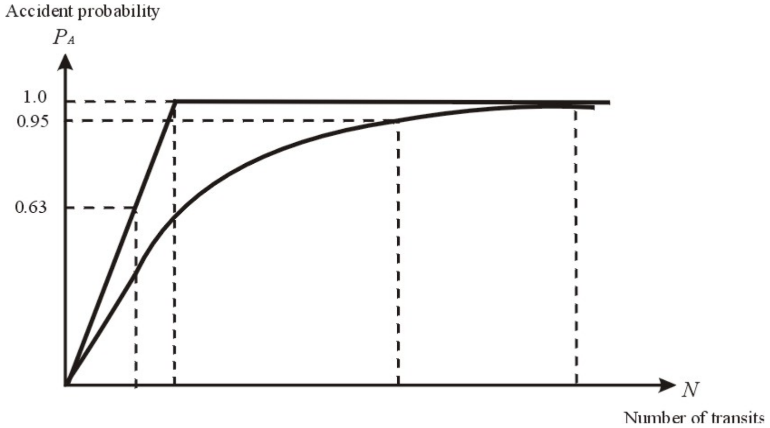


Figure 1. Probability of accident in function of transits number for linear and geometrical distributions

The probability of the ship's hull damage can be taken as an assessment criterion of safety and used to improve port functioning. The probability of arise the ship hull damage can be taken as an assessment criterion of safety and used to improve of port functioning.

4. The ship impact on the ground

When a ship hits the bottom, its hull presses on the ground, which results in the passive ground pressure. That pressure is the ground reaction to the hull pressure on the bottom. The passive ground pressure increases with the pressure of the hull. When the maximum admissible value is exceeded, the area of ground is formed and the blocks of ground begin to move aside from under the hull. An increase in the passive earth pressure (for non-cohesive grounds) along with the increase of hull pressure takes place due to structural changes in the ground [4] occur in both granular system and in particles of the ground. Initially, the elastic soil becomes elastic-plastic, then plastic. This is a state in which all the grains and particles are in the state of boundary equilibrium, which corresponds to the boundary value of passive pressure of the ground. The ship' pressure on the ground causes the hull to penetrate into the bottom ground. When the boundary passive pressure (reaction) is reached the expulsion of ground block and the ship's bottom penetrates the ground. That phenomenon takes place in both non-cohesive grounds, such as gravels and sands and their mixes, and in cohesive grounds, including clay gravels and sand-gravel mixes, clay sands, clay and silt. An analysis of the ship hull action on the ground when the bottom is hit shows that there are similarities to the action of fenders. This means that the ground is a medium absorbing the energy of the impact. The magnitude of energy absorption mainly depends on the ground properties. Ships penetrating a non-cohesive ground to a certain depth will not have their hull damaged. During a vessel's striking the bottom of an area built of sandy or argillaceous ground, for a ship in progressive movement, there occurs a gradual sinking of the hull into the ground (until the vessel stops). The mechanism of the vessel's striking the area's bottom depends on the vessel's draft, namely whether the ship is trimmed by the bows, the stern or if it is loaded on an even keel.

During a ship's striking the bottom of an area of fragmented ground, for a vessel in progressive movement, there occurs gradual sinking of the hull into the ground (until the vessel's stoppage). During this process there can be distinguished the plough-in phase bound with longitudinal motion and the penetration (sinking) in a vertical direction. A similar phenomenon will occur in the case of being trimmed by the stern.

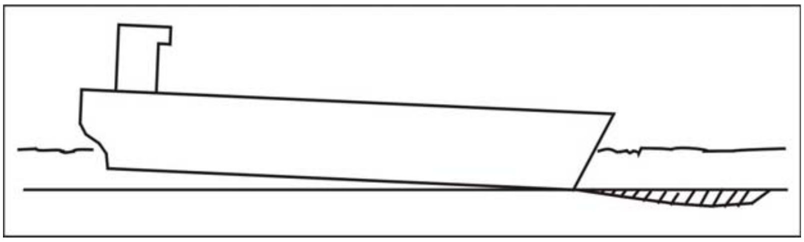


Figure 2. Penetration of the ships hull into the bottom

The penetration of the vessel into the ground depends on the relation between the horizontal and vertical components of the ship's speed. The ship will stop in a certain distance from the point of the hull's first contact with the bottom and the penetration to a particular depth. In the initial stage of the vessel's penetration into the ground, the ship's movement is mainly affected by horizontal forces. Stopping of the vessel takes place on a horizontal plane until the vessel stops, which is described as stopping distance from the first contact point to the stopping of the ship. During plough-in there are also vertical forces causing penetration of the ground. Exceeding the permissible value of hull strength may cause damage to the hull. These stages are affected by the kind of ground of the area bottom.

On the basis of considerations presented there has been prepared an algorithm of calculating vessel movement parameters when striking the port water area ground and of forces impacting on the ship's hull. It has been applied in a computer simulation model of the vessel's movement in the area. The model works in real time and serves the purpose of preparing navigational analyses. This permits risk determination of the vessel striking the area bottom and its results (likelihood of hull damage). In successive steps ship movement parameters during contact with the ground are calculated, which permits the determination of its results. There are the following steps of calculating of:

- initial kinetic energy.
- pressure of the ship on the area bottom, to decrease the water level or the vessel's draft.
- checking whether passive earth pressure (the ground's reaction) does not exceed the permissible value.

- the friction force of the bottom part of the ship's hull against the ground, taking into account the friction coefficient.
- the depth of the ship's penetration into the ground.
- work performed for overcoming friction force of the hull's bottom part.
- work performed for overcoming the resistance of friction of the lateral parts of the hull for a specified depth of the ship's penetration into the ground.
- work performed for overcoming soil wedge.
- the decrease of the ship's kinetic energy caused by contact with the ground.
- the decrease of the ship's speed components.

5. Conclusion

The keel clearance should warrant the safe manoeuvring of a ship in the port water area. Its value depends on many elements, in the midst of which the sea water level is very important. If keel clearance is great then the safety of ship is major but the admissible ship draft is less. It can cause:

- limited quantities of cargo loaded and unloaded, which means lower earnings for the port and stevedoring companies;
- lower ship-owners' profits as the ship's capacity is not used to the full or longer turnaround time due to necessary lighter age at the roads, before the ship's entrance. port charges are smaller as they depend on the ship's tonnage (berthing, towage etc.);
- in many cases large ships resign from using services of a port where they are not able to use their total cargo capacity.

It is possible to predict of maximum sailing draft for entering ships into the port by proper method of calculation. Such predictions enabled increases in maximum drafts in relation to UKC defined by port low as a fix value. It can translate into cargo increases ranging up to several thousands tonnes per ship. In particular it refers to the Polish ports (Gdańsk, Gdynia, Świnoujście). UKC requirements should be determined with a much higher degree of certainty allowing the manoeuvring of ship to be made more safely. A ship can touch the bottom of a navigable area due to the reduction of its keel clearance. The mechanism of ship's impact against the bottom basically differs from grounding or hitting a port structure (berth) and is not sufficiently described in the literature on the subject. Phenomena such as ship's pressure on the bottom ground and its reaction (passive earth pressure) are essential in the assessment of the impact effects. The kind and degree of hull damage mainly depend on the energy absorbed by the hull during its impact against the sea bottom. The results of the research permits to assess of navigational risk and thus to improve the safety of ship manoeuvring in port water areas.

References

[1] Galor, W. (2005). *The managing of the navigational safety of ships in port water areas.* Editors C.A. Brebbia At all. WITPRESS Southampton, Boston.

[2] Galor, W. (2005). The movement of ship in water areas limited by port structures. *Annual of Navigation no 10*, Gdynia.

[3] Galor, W. (2005). Analiza określania zapasu wody pod stępką. *Materiały XI Międzynarodowej Konferencji Naukowo –Technicznej „Inżynieria Ruchu Morskiego". Szczecin, 2005.*

[4] Galor, W. (2005). Wybrane problemy bezpieczeństwa żeglugi na akwenach portowych. *TRANSPORT* pod redakcją Z. Strzyżakowskiego, Prace Naukowe nr 3(23) 2005 Politechniki Radomskiej, Radom.

[5] Mazurkiewicz, B. (2006). *Morskie budowle hydrotechniczne. Zalecenia do projektowania i wykonania Z1-Z41.* Wyd. FPPOiGM, Gdańsk.

[6] Pedersen, T.P. & Zhang, S. (2000). Absorbed energy in ship collision and grounding, Revision Minorsky's Empirical Method, *Journal of Ship Research,* Vol.44, No.2.

METHODS FOR RISK ANALYSIS IN DISASTER REDUCTION

Van Gelder, P.H.A.J.M.

TU Delft, Delft, The Netherlands

Keywords
risk analysis, disaster reduction, natural hazards

Abstract
This paper discusses a proposal for a risk management tool for applications to risk reduction of natural hazards.

1. Natural Hazards

It is always a difficult dilemma with research projects on natural hazards if it should focus on certain aspects of the hazard (its probability of occurrence, its damage potential, the effectiveness of mitigation measures and building codes, its human behaviour and injury causation during the catastrophe, etc), or if the project should be addressed as a complete entity which involves physical, technological, economic and social realities. In this paper the first option is chosen, although now and then parts of the second option are presented.

Many books on natural hazards too often fall to an anecdotal level of 'horror stories' lacking a serious academic treatment of the subject. This is in contrast with one of the first complete treatises on natural hazards by White et al. [16]. Since the book is over 30 years old, many of the issues in this book are outdated unfortunately. It describes the status of natural hazards research in the USA in the 70s, and it gives recommendation for future research. The main message in their book is that research in the 1970s concentrated largely on technologically oriented solutions to problems of natural hazards, instead of focusing equally on the social, economic and political factors which lead to non adoption of technological findings, or which indicate that proposed technological steps would not work or only tend to perpetuate the problem (according to the authors). For floods the authors propose five major lines of new research: Improving control and prediction, Warnings and flood proofing, Land Management, Insurance, relief and rehabilitation, basic data and methods. For other natural hazards, 15 in total, similar lines are outlined. Interesting is that the authors already present methods of estimating research results within an evaluation framework, including economic efficiency, trade-offs and values.

Natural hazards considered under climate change have been studied by McGuire et al [12] and is heavily based on the results of the 3rd assessment report of 2001 by the IPCC (Intergovernmental Panel on Climate Change), who upgraded their temperature rise forecasts to 8 degrees Celsius by the end of the century. The natural hazards in McGuire [12] are described in the light of IPCC's forecasts. Windstorms are described to anthropogenic climate change and are shown to have the potential for large changes for relatively small changes in the general climate. Its natural patterns of climate variability are discussed by McGuire, amongst which ENSO, NAO, and PNA (Pacific North American tele-connection). Studies are presented which try to observe and predict the frequency and severity of extreme windstorms on a spatial and temporal scale. Also river and coastal floods under global warming are examined. Most research on river floods has concentrated on changes in observed precipitation and prediction methods, but the authors also present non-climatic factors involving human influences on the river basin. Coastal flooding from tropical and extra tropical storms under sea level change is investigated, as well as sea temperature changes (heat - and cold waves). The 1999 Venezuela landslides, causing 50 000 fatalities, have put this undervalued natural hazard on the agenda again. The authors concentrate on the water accumulation below the surface of unstable slopes. The landslide's theological properties (which resist the movement) are studied under environmental change.

Sea level change is discussed under the uncertainties of response to warming of the Greenland and Antarctic ice sheets and the effect of CO2 gas mitigation in the coming decades. The effect of sea level rise on submarine landslides and as a consequence ocean-wide tsunami is analysed. Coastal erosion and other geomorphologic effects of sea level rise are left out here.

Also asteroid and comet impacts as initiators of environmental change are included in McGuire [12]. Time domain simulations of a 20km/s impact in a 4 km deep ocean are presented.

McGuire [12] ends with some results from a recent paper in Science (v 289, p 2068-74, DR Easter ling et al) on different forecasts of climate extremes. The authors plead for political will from industrialized countries such as USA, Japan and Australia to invert their increase in gas emissions before the hazardous aspects of climatic shift make themselves felt.

Bryant [5] gives a complete overview on natural hazards, as well as its social impacts. Apart from how natural hazards occur, the author also presents (controversial) methods how to predict hazards from occurring again (on short and long term). The author claims that there is sound scientific evidence that cosmic / planetary links exist with the occurrence of earthquakes and floods. The 11-year sunspot cycle and the 18.6-year lunar cycle (caused by the moon's orbit fluctuation) are used to show a correlation with the ENSO index, occurrences of floods and droughts in North America, Northern China, Australia, Patagonia, amongst others. Very surprising Bryant [5] shows that in some parts of the world (such as the Mediterranean) the sunspot frequency and the seismic activity are correlated, via fluctuations in the Earth's rotation (in the order of milliseconds). However, if earthquake occurrence is dominated by some force external to the Earth (as mentioned by the author), then one would expect clustering to be taking place at the same time worldwide, which is not supported by the data.

Cannon et al [7] claim that natural disasters are not only caused by the natural environment, but also (or maybe even more) by the social, political and economic environment. This is shown throughout their work when they concentrate on the various hazard types: floods, coastal storms, earthquakes, landslides, volcanoes, biological hazards and famine. The authors consistently use a flow diagram describing the framework of the root causes, dynamic pressures, unsafe conditions (on the one side), the hazard (on the other side), and the disaster (in the middle).

Cannon et al [7] describe 12 principles towards a safer environment. It cannot be made by technical measures alone. It should address the root causes by challenging any ideology, political or economic system that causes or increases vulnerability. It should reduce pressures by developing by macro forces such as urbanization, re-forestation, a.o. It should achieve safe conditions by protected environment, resilient local economy and public actions, such as disaster preparedness. Together with technical measures to reduce certain hazards (such as flood defences, shelter breaks, etc), it should all lead to a substantial reduction in disaster risk.

The authors illustrate natural hazards from a social studies point of view, with striking observations, such as the bureaucratic blindness and biased relief assistance in South Carolina following hurricane Hugo in 1989 to the needs of many African Americans who lacked insurance and other support systems. The huge North Vietnam floods in 1971 only resulted in a few hundred deaths, largely because of a highly efficient wartime village-level organization that allowed rapid evacuation and provision of first aid, whereas the similar 1970 Bangladesh floods killed a record 300,000 people.

2. Ten steps for a structured approach of risk analysis and risk reduction of natural hazards

In recent years probabilistic and statistical approaches and procedures are finding wider and wider applications in all fields of engineering science, starting from nuclear power aeronautic applications down to structural mechanics and engineering, offshore and coastal engineering, and in more or less sophisticated forms are the base of many of the most recent versions of Structural Codes of Practice throughout the world. Detailed commentaries of these codes have been written as CIRIA (1977) or ISO (1973) reports. Applications to civil engineering are described by the comprehensive text of Benjamin & Cornell [3]. More recent similar comprehensive texts are Augusti & al. [1] and Thoft-Christensen & Baker [15]. A general application to structures in a coastal environment is provided by Burcharth [6].

Risk analysis is usually structured in:

1. analysis of hazard (risk source, natural processes causing damages),
2. analysis of failure (risk pathway, mechanisms through which hazard causes damages).
3. analysis of vulnerability (behaviour of the risk receptors).

For the first analysis, extreme events and joint probabilities of natural processes making up the hazards should be statistically described. In the second analysis, components of the defence systems should be identified, characterized and processes leading to failure are deterministically described. In the third analysis, understanding and assessment of direct and indirect damages and intangible losses including risk perception and acceptance from population, social and ecological reaction (resilience). The second step is process specific and will be described below, separately for each considered hazard. This step structured however in identification and prediction of failure modes, reliability analysis of defence structure or systems (combination of hazard statistics and structure behaviour) and modelling of post failure scenarios aiming to identify damages.

Damages caused by natural disasters can be distinguished as economical and non-economical, depending on whether or not a monetary value can be assigned to a specific damage. In addition, these damages are distinguished as direct and indirect, depending on whether the damage is the results of direct contact with the natural hazard or whether it results from disruption of economic activity consequent upon the hazard [13]. The economic approaches on the valuation of disaster generally pursue an objective of public policy: Given a set of courses of action to take to alleviate damages from hazardous events, what is the one with highest economic value? To answer that question, the literature has followed two approaches.

The first approach is that in which the value of a given public policy comes from the avoided damage. There is a series of damages associated with hazardous events, some of those that come to mind are loss of property, injury and loss of human life, or natural habitat disruption. Farber [9] and Yohe et al. [17] illustrate complex cases of valuation of property loss and disruption of economic activity caused by potential storm and flooding events. A qualitative list of potential losses can be found in Penning-Rowsell and Fordham [14]. A benefit transfer exercise consists in a statistical estimation of a function based on existing evidence in order to transfer value ("benefit") from the various study sites to the policy site, see Brouwer [4] and Bateman et al. [2]. On the basis of the evidence gathered to estimate the transfer function, it is possible to assess the risk of error in transferring values. End-users may then decide what risk they are willing to run for a particular application. The trade-off is between administering an expensive valuation survey (with low risk of error) and an inexpensive transfer of values with a potentially high risk of error depending on the particular site analysed.

The second approach is more direct in the sense that the researcher directly asks the relevant public to value the public policy itself, including its effects on flooding risk and potential physical damage. This approach has been illustrated in Penning-Rowsell and Fordham [14] and relies on "stated preferences" methods such as the contingent valuation or choice experiments; see Carson [8] and Haab and McConnell [10] for recent reviews on the former and Louviere et al. [11] on the latter. Contingent Valuation surveys consisted of the following steps: survey design, whose aim is to draw up a questionnaire suitable for the specific situation considered; sample design, to provide guidelines to obtain a random sample; pre-test of 30/50 interviews to check the wording of the questionnaire; main survey on the field of at least 600 interviews. As regards sites under risk of flooding, in general it is possible to carry out: site specific surveys to obtain data about property damages and to estimate damages from flooding, and post-flood household surveys to identify the immediate needs of the flood victims and to assess the intangible or non-economical flood effects [13].

Historically human civilizations have striven to protect themselves against natural and man-made hazards. The degree of protection is a matter of political choice. Today this choice should be expressed in terms of risk and acceptable probability of failure to form the basis of the probabilistic design of the protection. It is additionally argued that the choice for a certain technology and the connected risk is made in a cost-benefit framework. The benefits and the costs including risk are weighed in the decision process. Engineering is a multi-disciplinary subject, which also involves interaction with many stakeholders (individuals or organizations who have an interest in a project). This paper addresses the specific issue of how numerical occurrence probability levels of natural hazards are both formulated and achieved within the context of engineering design and how these relate to risk consequence.

A proposal for a common framework for risk assessment of any type of natural hazard is given by adapting the general theoretical approaches to the specific aspects of natural hazards, such as mass movements, and extreme waves. The specific features of each case will be presented in this paper and it will be shown that the common procedure proposed is able to deal appropriately with the specifics of each of the natural hazards considered.

Statistical methods are abundantly available to quantify the probability distributions of the occurrences of different hazards with special topics such as treating very seldom events, dealing with spatial and temporal variability of data, as well as with joint occurrences of different types of data. The two cases will demonstrate the applicability of the general methods to the specific aspects of the data from mass movements, and extreme waves. The 1st step in a structured risk analysis of natural hazards is:

Step 1. Statistical analysis of observations

Data is collected from mass movements, flooding, extreme waves and earthquakes and analysed with statistical methods. Proper tools are used in order to harmonies data, which comes from different sources (for instance instrumental or historical observations of natural hazards).

Step 2. Integration of mathematical-physical models in probabilistic models

The possible progress of a natural hazard from phase I to phase I+1 is described with transition probabilities in Markov models. Mathematical-physical models are used to generate data to be combined with observations and measurements for statistical analysis.

Step 3. Estimation of dependencies between natural hazards

Collected data from mass movements, flooding, extreme waves and earthquakes in some instances are analysed with respect to linear correlations and non-linear dependencies. Mathematical-physical-based reasons can be investigated to explain the existence of correlations and dependencies between the occurrences of hazards at the same time.

Step 4. Use of multivariate statistical models

Joint probability distribution functions (JPDFs) describe the probability that a number of extreme events happen simultaneously. Dependencies between events cause difficulties in deriving these JPDFs.

Elements characterizing the degree of the past and future hazards can be combined with indicators for the vulnerability of the inhabited areas or of infrastructure installations. In databases, the damage is expressed in terms of fatalities and damage costs for private buildings, infrastructure installations and agricultural land. In the next steps it is necessary to relate the expected physical damage to the expected economic losses and expected losses of life.

Step 5. Economic models to derive (in)direct consequences of hazards: FD-curves

Risk is considered as the product of probability and consequences. All natural hazards are analysed with respect to their economic impacts on society. This leads to so-called FD-curves (the cumulative distribution function of the amount of damage D). Economic expertise is an important part in this step.

Step 6. Models to estimate loss of human lives: FN curves.

Apart from economic damage, natural hazards can also lead to human casualties. Estimates are derived and covariates are found of the possible number of casualties caused by natural hazards.

Step 7. Cost-Benefit transfer

The aim of step 7 is to examine whether or not it possible to transfer values from natural disasters mitigation, and in case it is, to extract a transfer function. First the different methodologies used to value hazardous events are compared and whether and how they can be aggregated. Then, the construction of the actual value database can be carried out. Finally, if sufficient data quality criteria are met, a statistical analysis is performed in order to extract a benefit transfer function for one or several categories of values of hazardous events.

The methods presently accepted to set the acceptable risk levels related to industrial risks can be considered and their applicability to set acceptable risk levels of natural hazards can be studied. An approach is proposed to determine risk acceptance levels for different types of natural hazards, discussing in particular the specific aspects of mass movements, flooding, extreme waves and earthquakes.

Step 8. Acceptable risk framework development

Decisions to provide protection against natural hazards are the outcome of risk analyses and probabilistic computations as an objective basis. Development of concepts and methods to achieve this are available from literature. It covers both multi-attribute design and setting of acceptable risk levels. The research reinforces the concept that efficient design not only requires good technical analysis, but also needs to consider the social aspects of design as well and incorporate the concerns and aspirations of stakeholders.

Each stakeholder has a different perspective on the objectives of a particular project and it is the designer's challenge to manage these multiple concerns and aspirations efficiently. If the efficiency of decision-making can be improved then it is quite possible that a 5% saving or larger can be achieved.

The main approaches to assess costs and benefits of different risk reduction measures can be analysed dealing in particular with the approaches to deal with multiple risk and to take in consideration their interaction. An approach is proposed to determine actions leading to as low as reasonably possible (ALARP) levels of risk for different types of natural hazards, discussing in particular the specific aspects of mass movements, flooding, extreme waves and earthquakes. For cost benefit analysis it is necessary to have models of the costs and of the benefits. Rough estimates on these numbers for the two cases will be shown in Sec. 3 and 4.

Step 9. Cost analysis of mitigation measures

In order to reduce the risks of natural hazards, mitigation strategies are applied. To answer the question if more mitigation is necessary (or in general the question "how safe is safe enough"), insight is developed in the costs of mitigation measures of natural hazards.

Step 10. Effectively analysis of mitigation measures

Apart from insight in the costs of mitigation measures, it is also necessary to quantify the effectively of these measures, in other words, how much can they reduce the consequences of natural hazards or reduce the probability of occurrence of these negative impacts.

3. Conclusion

The above 10 steps are proposed as an overall integrated and structured way to analyse risks from natural hazards and are identified as 'best practice'.

References

[1] Augusti, G., Baratta, A. & Casciati, F. (1984). *Probabilistic methods in Structural Engineering.* Chapman and Hall, London.

[2] Bateman, I.J., Jones, A.P., Nishikawa, N., & Brouwer, R. (2000). *Benefits transfer in theory and practice: A review and some new studies.* CSERGE and School of Environmental Sciences, University of East Anglia.

[3] Benjamin, J.R. & Cornell, C.A. (1970). *Probability, Statistics and Decision for Civil Engineers*. McGraw-Hill, New York.

[4] Brouwer, R. (2000). Environmental value transfer: state of the art and future prospects. *Ecological Economics*, 32:1, 137 - 52.

[5] Bryant, E. (1991). *Natural Hazards*. Paperback: 312 pages , Publisher: Cambridge University Press, ISBN: 0521378893.

[6] Burcharth, H.F. (1997). *Reliability-based designed coastal structures.* In Advances in coastal and ocean engineering, Vol 3, Philip L.-F. Liu Ed., World Scientific, 145-214.

[7] Cannon, T., Davis, I., Wisner, B. & Blaikie, P. (1994). *At Risk: Natural Hazards, People's Vulnerability, and Disasters*. Hardcover: 284 pages, Publisher: Routledge , ISBN: 0415084768.

[8] Carson, R. (2000). Contingent Valuation: A User's Guide. *Environmental Science & Technology,* 34(8): 1413-18.

[9] Farber, S. (2001). *The Economic Value of Coastal Barrier Islands: A Case Study of the Louisiana Barrier Island System.* University of Pittsburgh: 26: Pittsburgh.

[10] Haab, T. & McConnell, K. E. (2002). *Valuing Environmental and Natural Resources*: The Econometrics of Non-Market Valuation Cheltenham, UK: Edward Elgar.

[11] Louviere, J. J., Hensher, D. A., & Swait, J.D. (2000). *Stated Choice Methods*. Cambridge University Press, Cambridge.

[12] McGuire, B., Mason, I. & Killburn, Ch. (2002). *Natural Hazards and Environmental Change.* Hardcover: 202 pages, Publisher: A Hodder Arnold Publication, ISBN: 0340742194.

[13] Penning-Rowsell et al. (1992). *The Economics of Coastal Management.* Belhaven Press, London.

[14] Penning-Rowsell, E. C. & Fordham, M. (1994). *Floods across Europe*. Middlesex University Press, London.

[15] Thoft-Christensen, P., & Baker, M. J. (1982). *Structural reliability Theory and its Application.* Springer Verlag, Berlin

[16] White, G. & Eugene Haas, J. (1975). Assessment of Research on Natural Hazards. Hardcover: 487

[17] Yohe, G., Neumann, J. E. & Marshall, P. (1999). *The economic damage induced by sea level rise in the United States, in The impact of climate change on the United States economy*. Robert Mendelsohn and James- E. Neumann eds. Cambridge; New York and Melbourne: Cambridge University Press, 331.

STATISTICAL ANALYSIS OF INTERVAL AND IMPRECISE DATA - APPLICATIONS IN THE ANALYSIS OF RELIABILITY FIELD DATA

Hryniewicz Olgierd

Systems Research Institute,
Warszawa, Poland

Keywords
reliability, statistical analysis, field data, interval data, fuzzy data

Abstract

The analysis of field lifetime data is much more complicated than the analysis of the results of reliability laboratory tests. In the paper we present an overview of the most important problems of the statistical analysis of field lifetime data, and present their solutions known from literature. When the input information is partial or imprecise, we propose to use interval arithmetics for the calculation of bounds on reliability characteristics of interest. When this information can be described in a more informative fuzzy form, we can generalize our interval-valued results to their fuzzy equivalents.

1. Introduction

Statistical analysis of results of lifetime tests has its over 50 years lasting history. In contrast to methods usually applied for the analysis of ordinary statistical data, in case of lifetime data we have to take into account such specific features like censoring of observations or the existence of covariates. First applications of this methodology were designed for the analysis of reliability data. However, starting from the 1970's their main field of applications is the survival analysis applied not only to technical objects, but to human beings as well.

In classical textbooks on reliability it is always assumed that *n* independent objects (systems or components) are put on test, and in the ideal case of no censoring we observe the realizations of *n* independent and identically distributed (*iid*) random variables $T_1,\ldots,T_n$. When the lifetime test is terminated after the *r*-th observed failure, e.g. when we observe a predetermined number of failures *r* at times $t_{(1)} < \ldots < t_{(r)}$, and the remaining *n-r* objects survive a random censoring time $t_{(r)}$, we have the case of the type-II censoring. On the other hand, when the lifetime test is terminated at the predetermined time t_B, and the number of observed failures is a random variable, we have the case of the type-I censoring. In more general models, we may also assume the cases of individual random censoring (when we observe random variables $X_i = min(T_i, C_i)\, i = 1,\ldots,n$, where $C_i, i = 1,\ldots,n$ are random, and independent from $T_i, i = 1,\ldots,n$ censoring times), multiple censoring (when for each subgroup of tested objects there exists a predetermined censoring time), or progressive censoring (when a predetermined number of objects are withdrawn from the test after each observed failure). The detailed description of these censoring schemes may be found in classical textbooks on the analysis of lifetime data, such as the book of Lawless [16].

Unfortunately, the practical applicability of well known methods is often limited to the case of precisely designed laboratory tests, when all important assumptions made by statisticians are at least approximately fulfilled. These tests provide precise information about lifetimes and censoring times, but due to the restricted (usually low) number of observed failures and/or the restricted test times, the accuracy of reliability estimation is rather low. Moreover, some types of possible failures may not be observed in such tests (e.g. due to their limited duration), and the obtained estimates of reliability may be overestimated.

It is beyond any discussion that the most informative reliability data may come only from field experiments, i.e. from the exploitation of considered objects in real conditions. Unfortunately, we have very seldom statistical data that are obtained under field conditions and fit exactly to the well known theoretical models. For example, test conditions are usually not exactly the same for all considered objects. Therefore, the random variables that describe their lifetimes are not identically distributed. Another serious practical problem is related to the lack of precision in reported lifetime data. Individual lifetimes are often imprecisely recorded. For example, they are presented in a grouped form, when only the number of failures which occurred during a certain time interval is recorded. Sometimes, times to failures are reported as calendar times, and this does not necessarily mean the same as if they were reported as times of actual operation. Finally, reliability data that come from warranty and other service programs are not appropriately balanced; there exists more information related to a relatively short warranty time, and significantly less information about the objects, which survived that time.

Statisticians who work with lifetime data have tried to build models that are useful for the analysis of field data. The majority of papers devoted to this problem are related to the methodology of dealing with data from warranty programs. These programs should be considered as the main source of reliability field data. Therefore, the presentation of the statistical problems of the analysis of warranty data shall be an important part of this paper. Some important mathematical models related to the analysis of warranty data are presented in the second section of this paper. In all these models it is assumed that all observations are described more or less precisely, and all necessary probability distributions are either known or evaluated using precisely defined statistical data. In many cases this approach is fully justified. However, close examination of real practical problems shows that in many cases available statistical data are reported imprecisely. We claim that making these data precise by force may introduce unnecessary errors. Therefore, we believe that in case of really imprecise data this fact should be taken into account in an appropriate way. In the third section of the paper we present the solution of some chosen practical problems when the input information is given in an interval form. These results are generalized in the fourth section to the case of fuzzy input data. Some conclusions and proposals for future investigations are presented in the last section of the paper.

2. Mathematical models of reliability field data coming from warranty programs

Lifetime data collected during precisely controlled laboratory test provide important, albeit limited, information about reliability of tested equipment. This limitation has different reasons. First, the number of tested units and/or the duration of a lifetime test are usually very limited due to economic constraints. Second, controlled laboratory conditions do not reflect real usage conditions. For this reason, for example, some of important types of failures cannot be revealed during the test. Finally, only field data can provide useful information about dependencies between reliability characteristics of tested units and specific conditions of exploitation. In contrast to laboratory lifetime data, reliability field data may yield much more interesting information to a manufacturer. Unfortunately, the information that is characteristic for laboratory data is seldom available in case of field data. First of all, warranty programs that serve as the main source of reliability field data are not designed to collect precise data. For example, reliability data are collected only from those items that have failed during the warranty period. Moreover, this period may not be uniquely defined. It is a common practice to define the warranty period both in calendar (for example, one year) and operational (for example, in terms of mileage) time. Therefore, in many practical cases reliability data are intrinsically imprecise. Also exploitation conditions, important for the correct assessment of reliability, are not precisely reported. All those problems, and many others, make the statistical analysis of reliability field data a difficult problem. Therefore, despite its practical importance, the number of statistical papers devoted to the analysis of reliability field data is surprisingly low.

Statistical analysis of reliability field data coming from warranty programs can be roughly divided into two related, but distinct, parts: analysis of claims processes and the analysis of lifetime probability distributions. From the point of view of a manufacturer the most important information is contained in the description of the process of warranty claims. Comprehensive description of this type of analysis can be found in the papers by Lawless [17] and Kalbfleisch et al. [14]. In the analysis of claims processes statistical data are discrete, and are described by stochastic count processes like the Poisson process or its generalizations. By analysing count reliability data we can estimate such important characteristics as, e.g., the expected number of warranty claims during a specific period of time, the expected costs of such claims, etc. This type of information is extremely important for designing of warranty programs, planning of the supply of spare parts, and the evaluation of the efficiency of service activities, but does not yield precisely enough information about the intrinsic reliability characteristics of investigated units. Information of this type is much more useful for improving the quality on the design stage of a product, especially for the comparison of different solutions, etc.

In this paper we limit the scope of our investigations to the statistical analysis of probability distributions of lifetimes. Throughout the paper we will denote by *T* the continuous random lifetime whose probability density function is denoted by $f(t\,|\,\mathbf{x};\boldsymbol{\theta})$, where $\mathbf{x}$ is a vector of parameters (covariates) that describe exploitation conditions, and $\boldsymbol{\theta}$ is a vector of parameters that describe the lifetime distribution.

2.1. Estimation from truncated lifetime data

In case of the analysis of warranty data we often face situations when we observe both failure times $t_i, i=1,...$ and corresponding vectors of covariates $\mathbf{x}_i$, $i=1,...$ are observed only for failed units. Let T_c be a certain prespecified censoring time such that failures are observed only when $T_i \le T_c$, where $T_i, i=1,...$ denote random variables describing lifetimes of failed units. If only lifetimes of failed units are available, and the form of the lifetime probability distribution is known, the statistical inference about parameters $\boldsymbol{\theta}$ can be based on a truncated conditional likelihood function

$$L_T(\theta) = \prod_{i:t_i \le T_c} \frac{f(t_i\,|\,\mathbf{x}_i;\boldsymbol{\theta})}{F(T_c\,|\,\mathbf{x}_i;\boldsymbol{\theta})}, \tag{1}$$

where $F(t\,|\,\mathbf{x};\boldsymbol{\theta}) = P\{T \le t\,|\,\mathbf{x};\boldsymbol{\theta}\}$. This likelihood function arises from the conditional (truncated at time T_c) probability distribution of the random lifetime *T*. It is interesting to note, that the likelihood function (1) does not depend upon the number *N* of units in the considered population of tested items. Therefore, (1) is suitable for the estimation of $\boldsymbol{\theta}$ when this number is unknown. Moreover, in case of a low proportion of failed items, this likelihood function can be quite uninformative, as it was noticed by Kalbfleisch and Lawless [13]. They showed using computer simulations that the variance of the estimators of unknown parameters is substantially larger than in the case when some information about non-failed units is available.

Estimation of $\boldsymbol{\theta}$ using the likelihood function (1) is rather complicated, even in simple cases. A comprehensive presentation of this problem can be found in the book by Cohen [2]. A relatively simple solution was proposed by Cohen [1] for the lognormal probability distribution of lifetimes, i.e. when logarithms of observed lifetimes are distributed according to the normal distribution. In this case the maximum likelihood estimators based on (1), and the moment estimators based on the first two moments coincide, but computation requires either special tables or the usage of numerical procedures. Cohen [1] considered a single left truncation at X_0. In this case the *k*th sample moment is calculated from

$$\nu_k = \sum_{i=1}^{n} \frac{(x_i - X_0)^k}{n}. \tag{2}$$

For the estimation of the unknown parameters □ and □□ Cohen [1] proposed to use three first moments defined by (2). The obtained estimators can be calculated from the following simple formulae:

$$\left(\sigma^2\right)^* = \frac{\nu_2^2 - \nu_1\nu_3}{\nu_2 - 2\nu_1^2}, \tag{3}$$

and

$$\mu^* = X_0 + \frac{\nu_3 - 2\nu_1\nu_2}{\nu_2 - 2\nu_1^2}. \tag{4}$$

These formulae are derived for the left truncated sample. However, they can be applied in case of right truncated samples, in which case the odd moments are negative. The solution given by (3) and (4) is theoretically less efficient than the maximum likelihood estimators obtained from (1). However, Rai and

Singh [21] have shown using extensive Monte Carlo simulations that there is no significant difference between these two methods. However, the efficiency of these estimators decreases, as expected, significantly when the percentage of truncated (i.e. not observed) lifetimes is larger than 30%.

2.2. Estimation from censored lifetime data with full information about censored lifetimes

In the previous subsection we considered the case when only the data from units failed prior to a certain time T_c are available. The situation when the information about non-failed units is available is well known as "censoring". Following Hu and Lawless [9] let us present the general mathematical model of lifetime data. We consider population **P** consisting of *n* units described by their lifetimes, $t_i, i=1,\dots.n$, random censoring times, $\tau_i, i=1,\dots.n$, and vectors of covariates $\mathbf{z}_i, i=1,\dots.n$, respectively. Triplets (t_i, τ_i, z_i) are the realizations of a random sample from a distribution with joint probability function

$$f(t \mid \theta; \tau, \mathbf{z})dG(\tau, \mathbf{z}), t>0, \tau>0, \mathbf{z}\in R^q, \tag{5}$$

where lifetimes and censoring times are usually considered independent given fixed z, and $G(\tau, z)$ is an arbitrary cumulative distribution function. Let *O* be the set of *m* units for whom the lifetimes are observed, i.e. for whom $t_i \le \tau_i, i=1,\dots,n$. The remaining *n-m* units belong to the set *C* of censored lifetimes for whom only their censoring times τ_i and covariates $\mathbf{z}_i$ are known. The function $S(t \mid \theta; \tau, \mathbf{z}) = 1 - F(t \mid \theta; \tau, \mathbf{z})$, where $F(t \mid \theta; \tau, \mathbf{z})$ is the cumulative distribution function of the lifetime, is called in the literature the survivor function or the survival function. The likelihood function that describes the lifetime data is now given by [9]

$$L(\boldsymbol{\theta}) = \prod_{i\in O} f(t_i \mid \boldsymbol{\theta}; \tau_i, \mathbf{z}_i)dG(\tau_i, \mathbf{z}_i)\times \\ \times \prod_{i\in C} S(t_i \mid \boldsymbol{\theta}; \tau_i, \mathbf{z}_i)dG(\tau_i, \mathbf{z}_i) \tag{6}$$

The special cases of (6) are well known, and comprehensively described in many reliability textbooks, such as an excellent book by Lawless [16]. However, they are rather well suited for the description of laboratory life tests, where all censoring times are known, and the values of covariates that describe test conditions are under control. In this paper we recall only those results, which in our opinion are pertinent to the analysis of field lifetime data.

One of the features that distinguish reliability field tests from laboratory tests is the variety of test conditions. In the laboratory test these conditions are usually the same for all tested units. Only in case of accelerated lifetime these test conditions are different for different groups of tested units. In contrast to this situation, in reliability field tests usage conditions may be different for all tested units. Therefore, statistical methods that allow taking into account different test conditions are especially useful for the analysis of reliability field data.

There exist two general mathematical models that link lifetimes to test conditions and are frequently used in practice: proportional hazard models, and location-scale regression models. In the proportional hazard models the hazard function, defined as $h(t; \boldsymbol{\theta}, \mathbf{z}) = f(t; \boldsymbol{\theta}, \mathbf{z}) / S(t; \boldsymbol{\theta}, \mathbf{z})$, is linked to the test conditions by the following equation

$$h(t \mid \mathbf{z}) = h_0(t)g(\mathbf{z}), \tag{7}$$

where functions $h_0(.)$ and $g(.)$ may have unknown parameters which have to be estimated from statistical data. Another representation of the proportional hazard model is the following:

$$S(t \mid \mathbf{z}) = S_0(t)^{g(\mathbf{z})}. \tag{8}$$

The most frequently used model is given by the following expression

$$h(t \mid \mathbf{z}) = h_0(t)e^{\mathbf{z\beta}}, \tag{9}$$

where $\mathbf{z\beta} = z_1\beta_1 + \cdots + z_q\beta_q$, and □□'s are unknown regression coefficients. This model was investigated by many authors. To give an illustration of its application let us recall the results given in Lawless [16] for the case of the Weibull distribution of lifetimes.

The Weibull probability distribution is the most frequently used mathematical model of lifetime data. In the considered case of the proportional hazard model its survivor function is given by the following expression

$$S(t \mid \mathbf{z}) = exp\left[-\left(te^{-\mathbf{z\beta}}\right)^{\delta}\right], \tag{10}$$

where □>0 is the shape parameter, responsible for the description of the type of failure processes. If we use the transformation $Y = log\,T$, the logarithms of lifetimes are described by simple linear model

$$Y = \mathbf{z\beta} + \sigma W, \tag{11}$$

where □□□□□, and the random variable W has a standard extreme value distribution with the probability density function $exp[w - exp(w)]$.

Suppose that n units are tested, and independent observations $(x_i, \mathbf{z}_i), i = 1, \ldots, n$ are available, where x_i is either a logarithm of lifetime or logarithm of censoring time of the ith tested unit. Additionally suppose that exactly r failures are observed. If we apply the maximum likelihood methodology to this model, we arrive at the following set of equations [16]:

$$-\frac{1}{\sigma}\sum_{i \in o} z_{il} + \frac{1}{\sigma}\sum_{i=1}^{n} z_{il}e^{x_i} = 0, l = 1, \ldots, q \tag{12}$$

$$-\frac{r}{\sigma} - \frac{1}{\sigma}\sum_{i \in O} x_i + \frac{1}{\sigma}\sum_{i=1}^{n} x_i e^{x_i} = 0, \tag{13}$$

where $x_i = (y_i - z_i\mathbf{\beta})/\sigma$. The solution of q+1 equations given by (12) and (13) yields the maximum likelihood estimators of □ (and hence for the shape parameter □), and regression coefficients $\beta_1, \ldots, \beta_q$. The formulae for the calculation of the asymptotic covariance matrix of these estimators can be found in [16].

A second regression model commonly used for the analysis of lifetimes is the location-scale model for the logarithm of lifetime T. In this model the random variable $Y = log\,T$ has a distribution with the location parameter $\mu(\mathbf{z})$, and a scale parameter □, which does not depend upon the covariates z. This model can be written as follows:

$$Y = \mu(\mathbf{z}) + \sigma\xi, \tag{14}$$

where $\sigma > 0$ and ξ is a random variable with a distribution that is independent on z. Alternative representation of this model can be written as

$$S(t \mid \mathbf{z}) = S_0\left(\frac{t}{\alpha(\mathbf{z})}\right). \tag{15}$$

Both models, i.e. proportional hazard model and location-scale model, have been applied for different probability distributions of lifetimes. The detailed description of those results can be found, for example, in

[16]. However, it is worth to note, that only in the case of the Weibull distribution (and the exponential distribution, which is a special case of the Weibull distribution) both models coincide.

When the type of the lifetime probability distribution is not known and the proportional hazards model seems to be appropriate we can apply distribution-free methods for the analysis of lifetimes. Let (8) be of the form

$$S(t \mid \mathbf{z}) = S_0(t)^{\mathbf{z}\boldsymbol{\beta}} . \tag{16}$$

Cox [5] proposed a method for the separation of the estimation of the vector of regression coefficients □ from the estimation of the survivor function $S_0(t)$. Suppose that the observed lifetimes are ordered as follows: $t_{(1)} < \cdots < t_{(m)}$. Let $R_i = R\left(t_{(i)}\right)$ be the set of all units being at risk at time $t_{(i)}$, that is the set of all non-failed and uncensored units just prior to $t_{(i)}$. Note, that in this model censoring times of the remaining *n* – *m* units may take arbitrary values. For the estimation of □□Cox [5] proposed to use a pseudo-likelihood function given by

$$L(\boldsymbol{\beta}) = \prod_{i=1}^{m} \left(e^{\mathbf{z}_{(i)}\boldsymbol{\beta}} \Big/ \sum_{l \in R_i} e^{\mathbf{z}_{(i)}\boldsymbol{\beta}} \right) \tag{17}$$

Slight modification of (17) has been proposed in Lawless [16]. This modification allows for few multiple failures at times $t_{(i)}, i = 1, \ldots, m$. Let D_i be the set of units that fail at $t_{(i)}$, d_i be the number of those units, i.e $d_i = \mid D_i \mid$, and $\boldsymbol{\Xi}_i = \sum_{l \in D_i} \mathbf{z}_l$. The likelihood function is now given by [16]

$$L(\boldsymbol{\beta}) = \prod_{i=1}^{m} \left[e^{\boldsymbol{\Xi}_i \boldsymbol{\beta}} \Big/ \left(\sum_{l \in R_i} e^{\mathbf{z}_{(i)}\boldsymbol{\beta}} \right)^{d_i} \right] . \tag{18}$$

The maximum likelihood estimators of the regression coefficients □ are found from the following equations:

$$\sum_{i=1}^{m} \left(\Xi_{ir} - d_i \sum_{l \in D_i} z_{lr} e^{\mathbf{z}_l \boldsymbol{\beta}} \Big/ \sum_{l \in D_i} e^{\mathbf{z}_l \boldsymbol{\beta}} \right) = 0, r = 1, \ldots, q , \tag{19}$$

where Ξ_{ir} is the *r*th component in $\boldsymbol{\Xi}_i = \left(\Xi_{i1}, \ldots, \Xi_{iq} \right)$. Formulae for the calculation of the asymptotic covariance matrix of these estimators are given in [16]. When the vector of the regression coefficients □□has been estimated, we can use a distribution-free method, such as the Kaplan-Meier estimator [15], for the estimation of $S_0(t)$.

2.3. Estimation from censored lifetime data with incomplete information about censored lifetimes

In case of real field lifetime data the full information about the non-failed units is often unavailable, even in the case when there exists full and precise information about all failed units. Consider, for example, the data from warranty programs. Suppose that we do our analysis at a certain moment of time using the data (lifetimes and values of covariates) on all units that have failed by that moment. As we usually do not have information about the units which have not failed, we neither know their censoring times nor the values of their corresponding covariates. Moreover, we may also not know even the total number of units *n*. However, if even partial information about these units is available, it can be used for the improvement of the efficiency of estimation. This information may come, for example, from the follow-ups of certain units during the warranty period or monitoring of some units after their warranty has been expired.

Suzuki [22], [23] was one of the first researchers who considered the case of incomplete information coming from field reliability data. In [23] he considered the case when a certain fraction p^* of units is additionally monitored during their warranty period. Thus, we have lifetimes of all units that have failed during the warranty period and all censoring times that do not failed during the warranty period but have been monitored. Under the assumption of random censoring times independent from random times to failure Suzuki [23] derived the maximum likelihood estimator of the survivor function *S*(*t*) that generalizes the estimator proposed by Kaplan – Meier [15]. In [22] Suzuki applied his methodology to find estimators of the parameters of such lifetime distributions like the exponential distribution or the Weibull distribution. Consider, for example, the exponential distribution with the survivor function $S(t) = exp(-\lambda t), \lambda > 0, t > 0$. Let $t_1,\ldots,t_m$ be the observed lifetimes of *m* failed units, and $t_1^*,\ldots,t_k^*$ be the known censoring times of those *k* monitored units that have not failed during the warranty period. The censoring times of the remaining $n_l = n - m - k$ units that have not failed during the warranty period are unknown. The maximum likelihood estimator of the hazard rate □□is given as [22]

$$\lambda^* = \frac{m}{\sum_{i=1}^{m} t_i + \left(1 + \frac{n_l}{k}\right)\sum_{i=1}^{k} t_i^*} \tag{20}$$

In the similar case of the Weibull distribution Suzuki [22] derived modified maximum likelihood equations.

In [22] Suzuki considered also another problem related to the analysis of warranty data. In modern warranty systems the warranty "time" is often bi-dimensional. For example, for newly sold cars warranties are defined both in terms of calendar time and mileage. Thus, failures that occurred during the calendar-time warranty period but after the moment when the maximum mileage had been exceeded are not reported. Formulae used for the calculation of respective estimators are more complicated in this case. A more general model, when the additional information about covariates is available, was considered by Kalbfleisch and Lawless [13].

The results of Suzuki [22], [23] originated the paper by Oh and Bai [20] who considered the case when monitoring of certain units taken randomly from the whole population of considered objects is monitored not only during a warranty period, but also during some after-warranty period. They assumed that: (i) each failure that occurs during a warranty period $(0,T_1]$ is reported with probability 1; (ii) each failure that occurs during an after-warranty period $(T_1,T_2]$ is reported with probability *p*, and (iii) each unreported unit either fails during the after-warranty period but is not reported with probability 1-*p* or survives time T_2. Let $f(t;\boldsymbol{\theta})$ be the probability density function of the lifetime, and $S(t;\boldsymbol{\theta})$ be the corresponding survivor function of the considered objects. We assume that the vector of parameters □ is unknown, but we know probability *p*. In this case the log-likelihood function is given by [20]

$$\log L(\boldsymbol{\theta}) =$$

$$\sum_{i \in D_1} \log\{f(t_i;\boldsymbol{\theta})\} + \sum_{i \in D_2} [\log p + \log\{f(t_i;\boldsymbol{\theta})\}] \tag{21}$$

$$+ n_3 \log[(1-p)S(T_1;\boldsymbol{\theta}) + pS(T_2;\boldsymbol{\theta})],$$

where D_1 is the set of units which failed during the warranty period $(0,T_1]$, D_2 is the set of units failed and reported during the after-warranty period $(T_1,T_2]$, and n_3 is the number of units (both failed and not failed) not reported during $(0,T_2]$. Maximum likelihood estimators of □ can be found, as usual, by the maximization of (21). Oh and Bai [20] considered also a more difficult problem when the probability of revealing failures during the after-warranty period is unknown. To solve this problem they applied the EM maximum likelihood algorithm and proposed an iterative procedure for finding the estimators of □. For both cases of known and unknown *p* Oh and Bai [20] calculated the asymptotic covariance matrix of the obtained estimators. Another approach was used by Hu et al. [11] who have found non-parametric estimators of the probability distribution of the time to failure *f*(*t*) when the additional information about the probability distribution of censoring times is available. Hu et al. [11] assumed that times to failure and censoring times are described by mutually independent discrete random variables and found moment and maximum likelihood estimators of *f*(*t*).

The problem of two time scales mentioned in the paper by Suzuki [22] has attracted many researchers. The general discussion of the alternative time scales in modelling lifetimes is considered in the paper by Duchesne and Lawless [7]. In the considered in this paper context of the analysis of field reliability data this problem was considered by several authors. For example, Lawless et al. [18] considered the following linear transformation of the original calendar time *t* to an operational (usage) time *u*

$$u_i(t) = \alpha_i t, \quad t \geq 0 \ , \qquad (22)$$

where α_i is a random usage rate described by the cumulative probability function $G(\alpha)$. Jung and Bai [12] have used this approach for the analysis of lifetime data coming from warranty programs when warranty periods were defined in two time scales (e.g. calendar time and mileage). The results of their computations are rather difficult for real applications, and cannot be applied without a specialized software. Moreover, this model requires the knowledge of $G(\alpha)$, and this probability distribution is rarely known for practitioners.

Another approach for solving this problem was proposed by Jung and Bai [12] who described lifetime data by a bivariate Weibull distribution. They calculated a very complicated log-likelihood function that can be used for the estimation of the parameters of this distribution when the data are reported both in calendar time and operational time. They showed an example where this approach may be more appropriate than the linear transformation model proposed by Lawless et al. [18].

Reliability field data may be collected and stored also in other forms that are far from those known in classical textbooks. Coit and Dey [3], and Coit and Jin [4] consider the case, typical for the collection of real reliability data, when data from different test programs are available in a form (r, T_r), where *r* is the number of observed failures, and T_r is the cumulative time on test for the data record with *r* failures. Coit and Dey [3] considered the case when lifetimes are distributed according to the exponential distribution. They proposed the test for the verification of this assumption.

Coit and Jin [4] considered a case when lifetimes are distributed according to the gamma distribution

$$f(t)\lambda^k t^{k-1} e^{-\lambda t} \big/ \Gamma(k), \quad t > 0, k > 0, \lambda > 0 \qquad (23)$$

They considered the case typical for the analysis of field data for repairable objects, where a single data record consists of the number of observed failures and total time between those failures. Let T_{rj} be the *j*th cumulative operating time for the data record with exactly *r* failures (Note, that no censoring is considered in this case); n_r be the number of data records with exactly *r* failures; *m* be the maximum number of failures for any considered data record; *M* be the total number of observed failures, i.e. $M = \sum_{r=1}^{m} r n_r$; and $\bar{t} = \sum_{r=1}^{m} \sum_{j=1}^{n_r} T_{rj} \big/ M$ be the average time to failure. The maximum likelihood estimator of the shape parameter *k* can be found from the equation [4]

$$\sum_{r=1}^{m} r n_r \psi(rk) - M \, ln \, k = K' , \qquad (24)$$

where

$$K' = \sum_{r=1}^{m} \sum_{j=1}^{n_r} r \, ln \, T_{rj} - M \, ln \, \bar{t} , \qquad (25)$$

and

$$\psi(rk) = ln(rk) - \frac{1}{2rk} - \frac{1}{12(rk)^2} + \frac{1}{120(rk)^4} - \cdots \tag{26}$$

is the digamma function. The estimator of the parameter □ is simply given by $\hat{\lambda} = \hat{k} / \bar{t}$.

Another type of reliability field data was considered in papers by Usher [24] and Lin et al. [19]. These authors considered the case of so-called masked data. This type of data is observed when lifetimes of whole systems are observed, but the exact cause of failure (i.e. a component that failed) can be isolated only to some subset of components. Unfortunately, the problem of estimation of lifetime characteristics has been solved only either in the case of two-component systems [24] or in the case when there exists additional prior information about reliability of considered components.

2.4. Estimation of the failure rate from field data

Hu and Lawless [10] considered the case when reliability data sets contain information not only on times to first failures, but also on times to consecutive failures if the observed units failed several times during a warranty period. In such cases, which are typical for the reliability analysis of repairable objects, the most frequently used model that describes the process of failures is a Poisson process characterized by a failure rate □. When the failure rate varies in time the process of failures is called the non-homogeneous Poisson process, and the reliability characteristic of interest is the time-dependent failure rate $\lambda(t)$. Hu and Lawless [10] considered parametric and non-parametric estimation of $\lambda(t)$ in two cases: when only data on failed units are reported (i.e. in case of data truncation, when the number of non-failed units is unknown), and when the population's size and the distribution of individual censoring times are known. In the first case the estimator of the failure rate $\lambda(t)$ can be found iteratively. In the second case the complexity of computations depends on the amount of knowledge about the population size and the distribution of censoring times.

3. Statistical analysis of reliability field data with incomplete interval-type information

In the previous section we have presented different mathematical models that can be used for the analysis of reliability field data. This type of lifetime data is in general more difficult to analyse using classical statistical methods. What is typical to field data is the existence of missing, unobserved or imprecisely reported data. If we want to analyse such data using a thorough statistical approach we immediately are in troubles. First of all, additional statistical information is needed which is necessary for the description of missing or imprecisely reported data in terms of the theory of probability. For example, if lifetime data are imprecisely reported due to the unknown delay time, see [17] for the description of the problem, the probability distribution of the delay time has to be identified using independent investigation. The same problem arises when we need to know the usage rate. The probability distribution of α_i in (22) has to be estimated even in the case when there exist doubts whether such unique distribution ever exists. Another group of problems arises even in those cases when the additional information is available. Mathematical models used for the estimation of reliability characteristics become very complicated, and in many cases are rather intractable for an average user. Specialized software is needed, and this software is rarely commercially available. In all these and similar cases there exists, however, additional imprecise information about *possible* values of the quantities of interest. This information may be expressed in a form of *intervals* of possible values of model parameters or values of imprecisely reported observations. It has to be noted that this type of the representation of imprecision is *not* equivalent to the assumption that quantities with unknown or imprecisely reported values are *uniformly* distributed on those intervals. The interpretation of these intervals should be rather made in the spirit of the classical theory of measurement. If such unknown or imprecisely reported quantity is represented by the interval of its possible values it may be understood as if that value could be represented by *any* probability distribution defined over such interval. Thus, the application of interval data yields both pessimistic and optimistic *bounds* for the reliability characteristics of interest. In this section we present some examples of the usage of this approach in dealing with reliability field data.

Let us begin with the simplest model of life data. Suppose that *M* units are tested during a fixed time period T_0. Let $t_1,\ldots,t_m$ be the observed times of *m* reported failures. The failures of the remaining *M-m* units have not been reported by the time T_0, and we assume that for these units T_0 is their censoring time. As usual, we assume that $f(t;\boldsymbol{\theta})$ is the density function of the time to failure, and □ is a vector of its unknown parameters. The maximum likelihood estimators of □ can be found by the maximization of the log-likelihood function

$$L(\boldsymbol{\theta})=\sum_{i=1}^{m} log\, f(t_i;\boldsymbol{\theta})+(M-m)S(T_0;\boldsymbol{\theta}), \tag{27}$$

where $S(T_0;\boldsymbol{\theta})=P(T>T_0)$ is the survivor function. The problem stated above is a classical statistical problem extensively investigated for numerous probability distributions of lifetimes. Consider now its more realistic version. First of all let us assume that the reported failure times T_i do not represent real failure times due to some random delay. For example, a transmission leakage in a car may be reported after a visit to a service centre, and not after observing its first signs on a garage floor [21]. Let D_i be a random delay time. Hence, the real time to failure is described by an unobserved random variable. Note however, that even if observed lifetimes T_i are distributed according to a well known probability distribution, e.g. the Weibull distribution, then the distribution of X_i may be completely different, even when the distribution of delays D_i is known. In real situation the distribution of D_i is usually very difficult to estimate, so the derivation of a more or less precise probabilistic model for the description of X_i is usually hardly possible. The existence of delays in the reporting of failures may cause additional complication. As a matter of fact we may not be sure if all failures have been reported by the censoring time T_0. We do not consider this possibility in our model, as its thorough description seems to be very complicated. Now, let us consider another serious problem with the analysis of reliability field data. In the majority of practical cases reliability engineers are rather not interested in the description of reliability in terms of calendar time, but in terms of operational or usage time. In the previous section we discussed some basic problems that arise when we want to model this situation. Even in the simplest case of a linear transformation of a calendar time to a usage time we have to know the daily usage rate U_i that is a random variable whose distribution is very difficult to estimate. In practice this can be done only for products like cars when the usage time is continuously monitored in an automatic way. In all other practical situations the usage rate may be only estimated from imprecise statements of users. Let Z_i be the lifetime in terms of usage time. Then we have $Z_i=(T_i-D_i)U_i$. In face of all difficulties mentioned above the derivation of the probability distribution of Z_i seems to be hardly possible. Finally, let us notice that different usage rates influence the values of censoring times of non-failed units. These censoring times are now the realizations of a random variable $Z_0=T_0U$, where *U* represents a random usage rate for non-failed units. It is quite obvious that this distribution can be estimated either using expert opinions or from a specially designed statistical experiment.

The discussion presented above shows quite clearly that even in the simplest case of the analysis of real field data the precise mathematical description of the problem becomes very difficult or even mathematically intractable. However, we still have to analyse the data in the form they are available to us. Therefore, there is a need to propose approximate methods that should be simple enough in order to be applied in practice. In this section of the paper we propose to represent our lack of knowledge in terms of intervals representing the values of considered characteristics or quantities.

In order to simplify further notation let us denote by □*x* a compact interval $[x_{min},x_{max}]$. The lack of knowledge about the precise value of the time to a real failure let us describe by assuming that the real time to failure takes place in the interval □t_i, where $t_{i,max}$ is equal to the reported failure time t_i. Similarly, we assume that the usage rate for each observed failed unit is described by the interval □u_i, and the usage rate for all censored unit belongs to the interval □*u*. Hence, we can calculate the interval the usage time to a failure belongs to. This can be done using the rules of simple interval arithmetics; the lower bound of the interval □z_i is equal to $z_{i,min}=t_{i,min}u_{i,min}$, and the upper bound is given by $z_{i,max}=t_{i,max}u_{i,max}$. Similarly, the lower bound for the usage censoring time is given by $Z_{0,min}=T_0u_{min}$, and the upper bound by $Z_{0,max}=T_0u_{max}$. We should also make the assumption that the probability distribution of lifetimes belongs to a certain class of probability distributions. This assumption is a crucial one, as strictly speaking this distribution is different from that which describes observed times to failures measured in the calendar time. However, when the intervals of interest are not very wide this assumption seems to be practically acceptable.

In the next step of our analysis we calculate a multivariate interval $\Delta\boldsymbol{\theta} = [\boldsymbol{\theta}_{min}, \boldsymbol{\theta}_{max}]$ that describes the estimated values of □. Lower and upper bounds of □ can be found by solving two optimisation **problems.**

$$\boldsymbol{\theta}_{min} = \inf_{z_i \in \Delta z_i, Z_0 \in \Delta Z_0} \arg\max_{\boldsymbol{\theta}} L(\boldsymbol{\theta}) \tag{28}$$

$$\boldsymbol{\theta}_{max} = \sup_{z_i \in \Delta z_i, Z_0 \in \Delta Z_0} \arg\max_{\boldsymbol{\theta}} L(\boldsymbol{\theta}), \tag{29}$$

where $L(\boldsymbol{\theta})$ is the log-likelihood function given by

$$L(\boldsymbol{\theta}) = \sum_{i=1}^{m} \log f(z_i; \boldsymbol{\theta}) + (M - m) S(Z_0; \boldsymbol{\theta}). \tag{30}$$

The optimisation problem defined by (28) – (29) may be, in a general case, difficult, as the interval computations for non-linear functions are usually time consuming. However, in some practical cases the optimisation problem may be significantly simplified. In the case of the exponential distribution the lower and upper bound for the hazard rate □ are given by simple formulae

$$\lambda_{min} = \frac{m}{\sum_{i=1}^{m} z_{i,max} + (M - m) Z_{0,max}} \tag{31}$$

$$\lambda_{max} = \frac{m}{\sum_{i=1}^{m} z_{i,min} + (M - m) Z_{0,min}}. \tag{32}$$

Unfortunately, in the case of the Weibull distribution the interval for the possible estimated values of the shape parameter □ cannot be calculated using separately lower and upper bounds for observed lifetimes and censoring times. Only the bounds for the scale parameter (or its reciprocal) can be calculated in such a way. In general, simple computations are possible only then if a lifetime distribution is of a location-scale type. In such a case, the bounds for a location parameter can be calculated using lower and upper bounds for lifetimes and censoring times separately.

Let us consider now another relatively simple example of a practical application of the interval approach in the analysis of reliability field data. In section 2.2 of this paper we presented a mathematical model of lifetimes when the probability distribution of these random variables depends also on certain covariates, which describe usage conditions. These conditions may be described by a vector of covariates z, and the dependence of lifetimes on these covariates may be described by different mathematical models. Assume now, that this dependence is described by the proportional hazard model defined by equations (7) – (9). In this model probability distribution of lifetimes depends on the values of covariates via $\mathbf{z}\boldsymbol{\beta} = z_1\beta_1 + \cdots + z_q\beta_q$, where □□'s are unknown regression coefficients. Estimation of these coefficients in the proportional hazard model was proposed by Cox [5], and is briefly presented in section 2.2.

In case of reliability field experiments each investigated unit may be used in different conditions. Theoretically, these conditions may be defined quite precisely, and described by real numbers. However, in practice it is much more convenient to describe usage conditions by categorical variables. In such a case each covariate $z_j, j = 1, \ldots, p$ may adopt only a finite number of possible values $z_{j,l}, j = 1, \ldots, p; l = 1, \ldots, n_j$. If the set of these values can be identified for each of *k* failed units we can find the estimators of □ by solving equations (19). However, in certain circumstances the users may face difficulties with a precise identification of the values of covariates z. Let us suppose, for example, that exploitation conditions vary in time, and it is not obvious whether these conditions should be labelled as moderate or severe. In such situation the necessity to choose only one value of the covariate that describes the severity of exploitation conditions may distort a final reliability analysis. Introduction of another probabilistic model for the description of this situation may be too difficult from a practical point of view. Therefore, it seems to be much more convenient to use a set-valued description of the considered covariates. In case of covariates described by real numbers we can directly use the notation introduced previously, i.e. $\Delta z_j = \lfloor z_{j,min}, z_{j,max} \rfloor, j = 1,\ldots,p$. However, we also can use this notation in case of ordered categorical data. Let □□□be a multivariate interval that describes the estimated values of the regression coefficients □□in the presence of interval data $\Delta \mathbf{z}_i, i = 1,\ldots,m$, where *m* is the number of observed failures. The lower and upper bounds for □□can be found by solving the optimisation problems

$$\boldsymbol{\beta}_{min} = \inf_{z_i \in \Delta z_i} \arg\max_{\boldsymbol{\beta}} L(\boldsymbol{\beta}) \tag{33}$$

$$\boldsymbol{\beta}_{max} = \sup_{z_i \in \Delta z_i} \arg\max_{\boldsymbol{\beta}} L(\boldsymbol{\beta}) \ , \tag{34}$$

where $L(\boldsymbol{\beta})$ is the log-likelihood function given by (18).

The solution of (33) – (34) is, in general, difficult. However, in many cases the dependence of reliability upon covariates has a monotonic nature. In this case the lower and upper bounds of □ defined by (33) – (34) may be found using appropriately chosen (depending on the direction of the dependence) boundary values of $\Delta \mathbf{z}_i, i = 1,\ldots,m$.

The limited volume of this paper allows us to present only a general description of relatively simple models for the analysis of reliability field data. These models are more complicated than the simplest lifetime models, but are applicable in such cases when a proper probabilistic analysis of reliability field data is either very difficult or even impossible. In order to overcome these problems we have to deal with some information of subjective nature. This is the price we have to pay if we want to solve more realistic problems.

4. Statistical analysis of reliability field data with imprecise fuzzy information

In the previous section we considered the case when the information which is necessary for a proper evaluation of reliability in terms of the theory of probability and mathematical statistics may be incomplete and imprecise. Our lack of full information we represented in terms of intervals describing the quantities of interest. Representation of uncertainty by intervals has its origins in the theory of measurement. If no additional information is present, this methodology allows the calculation of the bounds for reliability characteristics of interest. These bounds may be interpreted as “the worse” and “the best” possible values which take into account any type of variability of imprecisely or partially known values of field lifetime data. However, one can argue that this type of representation of uncertainty may not reflect the complexity of available information. For example, let us suppose that the daily usage rate of certain equipment is reported by its user as “about five hours a day”. From further inquiry one may get information that it means “between four and six hours a day”. Note, that this information does not tell anything about the way the usage rate varies in time. Therefore, the representation of uncertainty in a form of an interval seems to be quite appropriate. On the other hand, it is easy to note that the original information, “about five hours a day”, carries additional information. One may believe that the real usage rate is more often closer to five hours than to any other number of hours. This still vague information, which does not allow building any probability distribution, may be described formally using the theory of fuzzy sets introduced by Lotfi A. Zadeh[25].

Fuzzy sets are the generalization of ordinary sets. In order to define a fuzzy set we have to specify a so called *universe of discourse X*, i.e. an ordinary set that contains all elements that are relevant for the description of a vaguely defined (or described) object. In the considered in this paper reliability context it might be a set (or a subset) of positive real numbers, when we describe the usage rate, a set of integers, when we describe a partially known number of units on test, or a set of labels, when we describe the severity of working conditions. A *membership function* $\mu_A : X \to [0,1]$ such that $\mu_A(x)$ tells us to which degree an element $x \in X$ belongs to the fuzzy set *A,* is the second part of the definition of a fuzzy set. Thus, a fuzzy set *A* in a universe of discourse *X* is a set of pairs

$$A = \{\mu_A(x), x\} \tag{35}$$

This formalism is very useful for the description of vague and imprecise concepts, as the value of the membership function $\mu_A(x) \in [0,1]$ describes our degree of belief that the value *x* describes the considered concept.

Each fuzzy set has a unique representation in terms of so called □-cuts, or □-level sets. The ordinary (non-fuzzy) set $A_\alpha = \{x \in X : \mu_A(x) \geq \alpha\}$, for each $\alpha \in (0,1]$, is called the □-cut of the fuzzy set *A*, and the set of all □-cuts uniquely defines this fuzzy sets.

When the universe of discourse is represented by the set of real numbers we can generalize the concept of a real number and define a *fuzzy number*. The fuzzy subset *A* of the real line *R*, with the membership function $\mu_A : R \to [0,1]$ is a fuzzy number iff

a) *A* is normal, i.e. there exists an element x_0 such that $\mu(x_0) = 1$;

b) *A* is fuzzy convex, i.e. $\mu_A(\lambda x_1 + (1-\lambda)x_2) \geq \mu_A(x_1) \wedge \mu_A(x_2)$, $\forall x_1, x_2 \in \boldsymbol{R}, \forall \lambda \in [0,1]$;

c) μ_A is upper semi-continous;

d) supp *A* is bounded.

From the definition given above one can easily find that for any fuzzy number *A* there exist four real numbers a_1, a_2, a_{13}, a_4 and two functions: non-decreasing function $\eta_A : \mathbf{R} \to [0,1]$, and non-increasing function $\xi_A : \mathbf{R} \to [0,1]$, such that the membership function μ_A is given by

$$\mu_A(x) = \begin{cases} 0 & \text{if} \quad x < a_1 \\ \eta_A(x) & \text{if} \quad a_1 \leq x < a_2 \\ 1 & \text{if} \quad a_2 \leq x < a_3 \\ \xi_A(x) & \text{if} \quad a_3 \leq x < a_4 \\ 0 & \text{if} \quad a_4 < x \end{cases} \tag{36}$$

Functions η_A and ξ_A are called the left side and the right side of a fuzzy number *A*, respectively. A special, and very useful in practice, case of a general fuzzy number is a trapezoidal fuzzy number defined by the following membership function

$$\mu_X(x) = \begin{cases} 0 & \text{if} \quad x < x_1 \\ (x - x_1)/(x_2 - x_1) & \text{if} \quad x_1 \leq x < x_2 \\ 1 & \text{if} \quad x_2 \leq x < x_3 \\ (x_4 - x)/(x_4 - x_3) & \text{if} \quad x_3 \leq x < x_4 \\ 0 & \text{if} \quad x_4 \leq x \end{cases} \tag{37}$$

Note, that real-valued intervals considered in the previous section of this paper can be looked upon as trapezoidal fuzzy numbers for which $x_1 = x_2 = x_{min}$, and $x_3 = x_4 = x_{max}$.

Membership functions of fuzzy numbers that are defined as functions of other fuzzy numbers may be calculated using the following *extension principle* introduced by Zadeh, and described in Dubois and Prade [6] as follows:

Let *X* be a Cartesian product of universe $X = X_1 \times X_2 \times \cdots \times X_r$, and $A_1, \ldots, A_r$ be *r* fuzzy sets in $X_1, \ldots, X_r$, respectively. Let *f* be a mapping from $X = X_1 \times X_2 \times \cdots \times X_r$ to a universe *Y* such that $y = f(x_1, \ldots, x_r)$. The extension principle allows us to induce from *r* fuzzy sets A_i a fuzzy set *B* on *Y* through *f* such that

$$\mu_B(y) = \sup_{x_1,\dots,x_r;\, y=f(x_1,\dots,x_r)} \min\left[\mu_{A_1}(x_1),\dots,\mu_{A_r}(x_r)\right] \tag{38}$$

$$\mu_B(y) = 0 \text{ if } f^{-1}(y) = \varnothing \tag{39}$$

One can prove, see e.g. books by Dubois and Prade [6] or by Zimmermann [27], that the application of the extension principle is equivalent to the application of the interval arithmetics on □-cuts.

Fuzzy sets, and their special instances – fuzzy numbers, have been applied in solving different reliability problems. An extensive overview of these applications can be found in Hryniewicz [8]. If we want to apply this approach to the analysis of field lifetime tests we can directly apply the results presented in the previous section. In order to do so let us notice that the calculations presented in that section are exactly the same as the calculations that should be done for given □-cuts representing fuzzy data.

5. Conclusion

Probabilistic models that have been proposed for the description of field lifetime data, and are relatively easy to be applied in practice, usually do not describe all the aspects of this type of data. If we want to build models, which better describe reality, then immediately these models become very complicated. Moreover, additional assumptions have to be made in order to describe complex phenomena characteristic for this problem. In this paper we have proposed an alternative but only approximate approach where unknown values of model parameters are represented in terms of intervals. By applying the interval arithmetics we can calculate the bounds on the values of respective reliability characteristics. If additional but still imprecise information is available we propose to generalize the interval-valued calculations to fuzzy-valued ones. The results of these calculations can be interpreted as *possibility distributions* in the sense of Zadeh [26], defined on sets of possible values of vague quantities. It has to be stressed, however, that if appropriate probabilistic information is available it should not be replaced with the fuzzy one. Fuzziness in our models does not replace randomness, but supplements it if we have to use imprecisely perceived notions or vague statistical data.

References

[1] Cohen, C. A. (1959). Simplified estimators for the normal distribution when samples are singly censored or truncated. *Technometrics*, 1, 217 – 237.

[2] Cohen, C. A. (1991). *Truncated and censored samples: theory and applications*. Marcel Dekker, New York.

[3] Coit, D. W. & Dey, K. A. (1999). Analysis of grouped data from field-failure reporting systems. *Reliability Engineering and System Safety*, 65, 95 – 101.

[4] Coit, D. W. & Jin, T. (2000). Gamma distribution parameter estimation for field reliability data with missing failure times. *IEE Transactions*, 32, 1161 – 1166.

[5] Cox, D. R. (1972). Regression models and life tables (with discussion). *Journal of the Royal Statistical Society, ser.B*, 34, 187 – 202.

[6] Dubois, D. & Prade, H. (1980). *Fuzzy Sets and Systems. Theory and Applications*. Academic Press, New York.

[7] Duchesne, T. & Lawless, J. F. (2000). Alternative time scales and failure time models. *Lifetime Data Analysis*, 6, 157-179.

[8] Hryniewicz, O. (2007). Fuzzy sets in the evaluation of reliability. In: *Computational Intelligence in Reliability Engineering. New Metaheuristcs, Neural and Fuzzy Terchniques in Reliability*, Levitin, G. (Ed.), Springer, Berlin., 363 – 386.

[9] Hu, J. X. & Lawless, J. F. (1996a). Estimation from truncated lifetime data with supplementary information on covariates and censoring times. *Biometrika*, 83(4), 747-761.

[10] Hu, J. X. & Lawless, J. F. (1996b). Estimation of rate and mean functions from truncated recurrent event data. *Journal of the American Statistical Association*, 91, 300-310.

[11] Hu, J. X., Lawless, J. F. & Suzuki, K. (1998). Nonparametric estimation of a lifetime distribution when censoring times are missing. *Technometrics*, 40, 3-13.

[12] Jung, M. & Bai, D. S. (2007). Analysis of field data under two-dimensional warranty. *Reliability Engineering and System Safety*, 92, 135-143.

[13] Kalbfleisch, J. D. & Lawless, J. F. (1988). Estimation of reliability in field-performance studies. *Technometrics*. 30, 365-388.

[14] Kalbfleisch, J. D., Lawless, J. F. & Robinson, J.A. (1991). Methods for the analysis and prediction of warranty claims. *Technometrics,* 33, 273-285.

[15] Kaplan, E. L. & Meier, P. (1958). Nonparametric estimation from incomplete observations. *Journal of the American Statistical Association*, 53, 457 – 481.

[16] Lawless, J. F. (1982). *Statistical Models and Methods for Lifetime Data*. John Wiley and Sons, New York.

[17] Lawless, J. F. (1998). Statistical analysis of product warranty data. *International Statistical Review*, 66, 41-60.

[18] Lawless, J. F., Hu, J. & Cao, J. (1995). Methods for the estimation of a lifetime distributions and rates from automotive warranty data. *Lifetime Data Analysis*, 1, 227-240.

[19] Lin, D. K. J., Usher, J. S. & Guess, F.M (1996). Bayes estimation of component-reliability from masked system-life data. *IEEE Transactions on Reliability*, 45, 233 – 237.

[20] Oh, Y. S. & Bai, D. S. (2001). Field data analyses with after-warranty failure data. *Reliability Engineering and System Safety*, 72, 1-8.

[21] Rai, B. & Singh, N. (2003). Hazard rate estimation from incomplete and unclean warranty data. *Reliability Engineering and System Safety*, 81, 79 – 82.

[22] Suzuki, K. (1985). Estimation of lifetime parameters from incomplete field data. *Technometrics*, 27, 263-272.

[23] Suzuki, K. (1985). Nonparametric estimation of lifetime distributions from a record of failures and follow-ups. *Journal of the American Statistical Association*, 80, 68-72.

[24] Usher, J. S. (1996). Weibull component reliability-prediction in the presence of masked data. *IEEE Transactions on Reliability*, 45, 229-232.

[25] Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8, 338 – 353.

[26] Zadeh, L.A. (1978). Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, 1, 3 – 28.

[27] Zimmermann, H. J. (1996). *Fuzzy Set Theory and its Applications* (Third Edition), Kluwer, Boston.

A SHORT NOTE ON RELIABILITY OF SECURITY SYSTEMS

Jóźwiak Ireneusz J., Laskowski Wojciech

Wroclaw University of Technology,
Wroclaw, Poland

Keywords
computer security, reliability, computer incidents

Abstract

Telecommunication systems become a key component of critical infrastructure. One of the main elements of such systems is computer system. The organizations which can be involved in crisis management (e.g. government agencies, etc.) need to know results of security drawbacks in their systems. Moreover, they should have a tool for analysing the results of decision made in security context. And often the following question is raised: why do security systems fail? To answer it in this paper the aspects of reliability are discussed. From this point of view the security systems are analysed. We hope that thanks to such approach we will be able to reach some characteristics of security incidents occurrence. Moreover, we hope to use our results to build security attributes metrics. In addition, we present thesis that predictions of occurrence of incidents is impossible, so we should focus on registration of incidents type. On such a foundation we can formulate conclusions about drawbacks in configurations or administration of information systems. In our research we have observed that in case of some class of information systems, the availability incidents are the most dangerous. And we conclude that only using technologies with good reliability characteristics can lead to solving this problem.

1. Introduction

The problem of reliability of security systems were discussed by Anderson in several publications e.g. [1] or [2]. Another example is paper [11] where system reliability is viewed from game theoretical perspective and this work can be easily applied to security domain. One of the most popularised practical models of security systems is so called ‘defence-in-depth’ model [3]. Taking into consideration such a model it can direct our attention into basic models of system reliability: serial or parallel systems [4], [7]. Many components of security systems can be characterized by one of the above-mentioned structures. For example, access control subsystem, firewall, IDS and antivirus software can be considered as a mixed structure (*Figure 1*) with three serial elements and one element parallel to this structure.

Using reliability techniques influence security systems. A good example is a problem of placing IDS in redundant networks [10]. Another example is operating systems. Very large number of modules, software

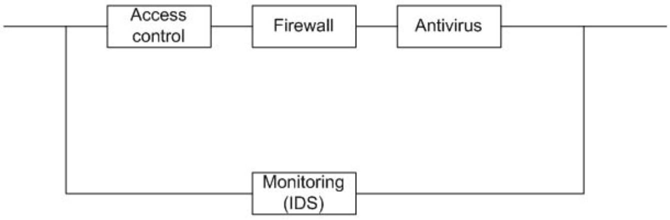


Figure 1. The scheme of a typical security system – an example

applications or services induce many security problems. There are many areas when security vulnerabilities are present, e.g. authorization subsystem, remote services etc. There is a set of security holes, which can be viewed as a serial or parallel structure (in basic reliability models sense). In this paper we present some empirical data from our research connected with analysing incidents connected with security of information systems.

2. Security incidents

In some period of the time (approximately 2 years) we have focused on observation of tree kinds of security systems. These systems (the models are presented in fig. 2) can be characterized as follows:

1. System A – a stand-alone system, not connected to any network, an access to this system is limited to a small number of users.
2. System B – specialized networked system, separated from public networks (several workstations)
3. System C – system networked, connected to public operators network (dozen workstations)

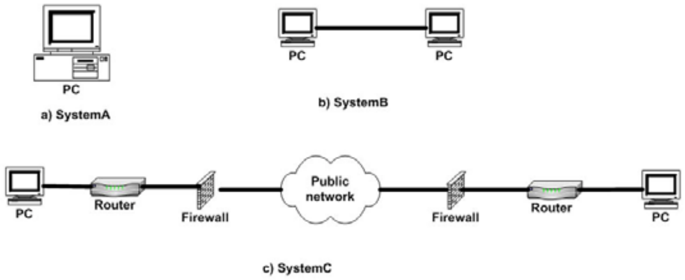


Figure 2. The models of observed information systems

The physical structures of these systems are less important for our research. Moreover, the size, role and localization of these systems are intended not to be mentioned at this time. Taking into consideration of three attributes of information: confidentiality, integrity and availability these systems were observed in order to notice specific incidents: virus incidents in System A and System C and availability incidents in case of System B. The availability incidents we understand as the breaks in proper working the system, e.g. lack of communications or servicing the elements of network infrastructure. The preliminary results are presented in *Table 1*.

Table 1. The number of observed incidents

Type of system	Number of virus incidents	Number of availability incidents	Period of observations
System A	2	----	1 year
System B	----	137	2 years
System C	41	----	1,5 year

In case of System A we noticed two different kinds of macro viruses [12]. The virus incidents in System C were connected with worms (mainly from Sasser 'family'), trojans or loggers [12]. The most interesting observations are connected with System B. Over 130 incidents were noticed. So some kind of reliability analysing methodology was used in order to describe the characteristics of events in this system. We are interested in mean time between incidents and frequencies of incidents.

3. Analysis of incidents

The preliminary results are presented in *Table 2* and in the *Figures 3,4,5*.

These pictures present number of incidents and its length and time periods between incidents. In case of System B we are focused on general number of incidents and time between incidents (*Figure*.)

Table 2. A comparison of mean values and standard deviations of data about incidents

Type of system	Mean time between incidents [day]	Standard dev.of time between incidents [day]	Mean time of incident [min]	Standard dev.of time of incident [min]
System B	5,25	7,30	129,48	184,77
System C	11,90	16,54	---	---

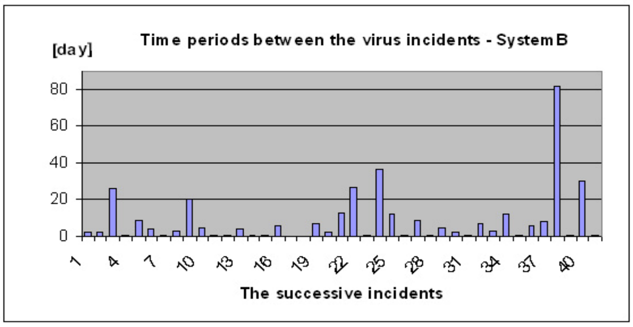


Figure 3. Graphical representation of observed length of time periods between incidents. System C.

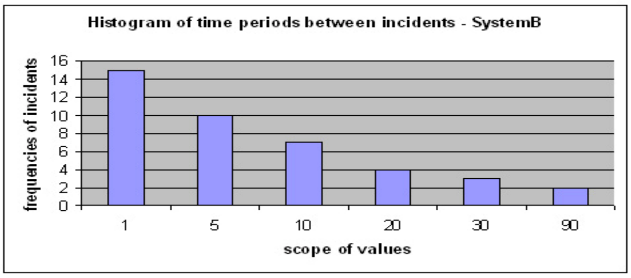


Figure 4. Histogram of observed time between the virus incidents. System C.

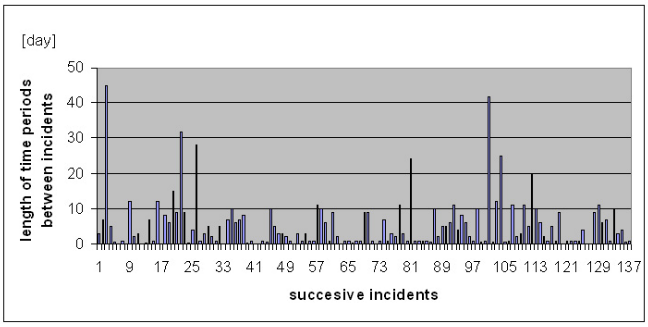


Figure 5. Graphical representation of observed length of time periods between incidents. System B.

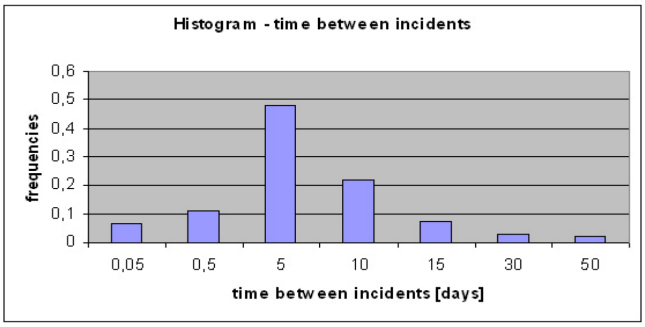


Figure 6. Histogram of observed time between the availability incidents. System B.

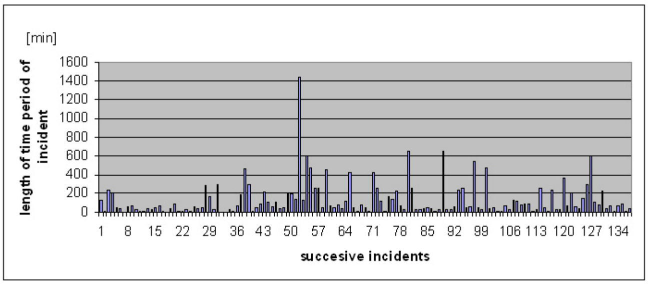


Figure 7. Graphical representation of observed length of time periods of availability incidents. System B.

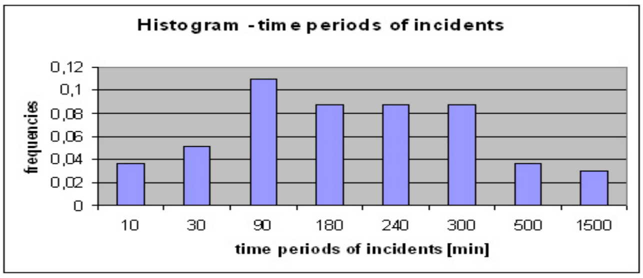


Figure 8. Histogram of observed time periods of availability incidents. System B.

The basic statistical analyses were done in order to notice the frequencies of incidents and derive empirical distributions.

In case of SystemB and virus incidents, the occurring the events has characteristic presented in figure 4.

In case of System C and availability incidents, the characteristics presented in fig. 6 and 7 were derived.

4. Reliability of security systems

When security of information systems is considered it is needed to analyse three attributes: confidentiality, availability and integrity. According to reliability theory, one of the key measures is probability of failures or time between failures. When it comes to security systems there is a lack of such metrics. In general security can be seen as a subjective category. So it is very difficult to find adequate metrics or measures of security attributes. But it seems that reliability context and analogies should be helpful. Another problem is if such metrics can be helpful in decision taking during ensuring security process. It seems that measuring security is impossible or at least possible in very limited scope. In authors' opinion every techniques which can be utilized to limit uncertainty during decision taking (in computer security domain) is worth considering.

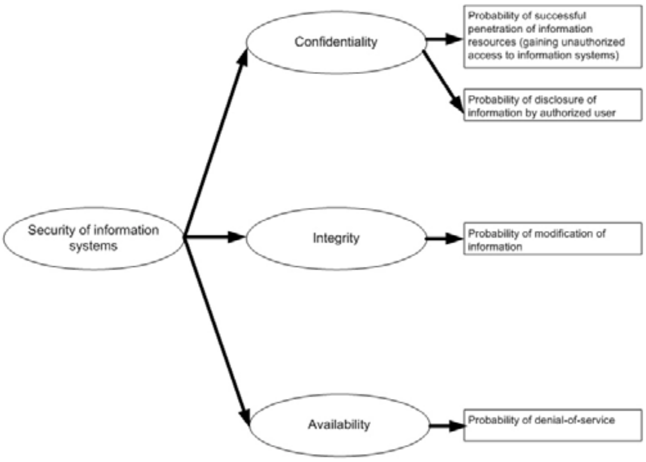

Security of information systems
Confidentiality
Integrity
Availability
Probability of successful penetration of information resources (gaining unauthorized access to information systems)
Probability of disclosure of information by authorized user
Probability of modification of information
Probability of denial-of-service

Figure 9 . Metrics for security attributes analysing

The observation done by authors can be helpful in analysing first of all aspects of availability. Looking for the distribution of probability of occurring incidents we can observe shape the distribution presented in *Figure 10* and *Figure 11*.

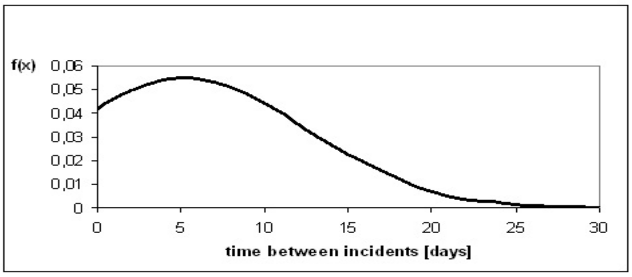


Figure 10. Probability distribution of observed time between the availability incidents. System B.

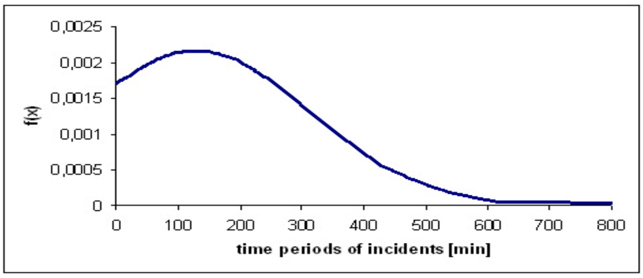


Figure 11. Probability distribution of observed time periods of availability incidents. System B.

The main conclusion from this preliminary analysis is that the most probable time between incidents is from range 0,01 to 1 day. It means that in the case of this system, the attention of operators should be focused first of all on control transmission links and devices. When it comes to virus incidents our observation proves that supervising the system should be done every day (the shape of characteristic in

Figure 4 shows that occurrence of incidents more often than one incident per 5 days period is possible with high probability).

The availability incidents' distributions were presented in fig. 10 and *Figure 11*. Expected time period of availability incidents is approximately 2 hours.

The reliability of security systems is connected with proper implementation of software and hardware components of security systems. The flexible and easy in realization reconfigurable hardware elements can be used. This problem was discussed and presented e.g. in [8] or [6]. Using reconfigurable hardware can significantly increase reliability e.g. cryptographic systems. What is more the speed of transmitting data are very important parameters. For example, the results of implementation of cryptographic device CRYPTON [12] is presented in *Table 3*.

5. Conclusion

Our observations proof the thesis that collecting data for analysing security is a very complex practical problem.

Table 3. The chosen parameters of reconfigurable device CRYPTON [12]

Device	Reconfigurable device CRYPTON
Clock period [ns]	52
Frequency [MHz]	19,2
Encryption (decryption) speed [Mb/s]	203,2
Time to encrypt (decrypt) one data block [ns]	630
Number of encryption (decryption) per second	1 587 301

What is more, the analysing of these data needs new more accurate methods. This is a general problem of IDS systems. Many methods of artificial intelligence are used in this domain, e.g. machine learning, data mining or neural networks. Exploring the data for discovering dependencies connected with incidents is a real and still open problem. We face some kind of paradox: we either a huge number of data and have problems with its exploring or we suffer from lack of accurate data. This problem can be noticed when a need for a fast assessing of security incidents takes place. In such a situation very often fast decision is needed: is this an incident or not? We still do researches connected with developing a new method for security assessment. Our method is based on preliminary preparation of data for scaling early intrusion detection systems using simulation. And in this method we need some characteristic connected with frequencies of incidents presented in the paper. In many elements our analysis is very similar to reliability analysis. We are focused on answering the questions: why do the security systems fail? And this is the key direction of constructing our method: finding the cause – effect dependencies in incident analysis in order to induce the rules for IDS systems. The first element of these observations is to notice how often the incidents take place.

As far as reliability of security system is concerned it is worth underline the wide spectrum of threads, which should be considered. One of these subjects is implementing hardware devices using high speed and characterized by good reliability characteristic technology.

The occurrence of computer incidents is rather unpredictable. It is very hard to reach characteristics like probability distributions. Institutions do not publish data about incidents. We can only collect own data or gather data from other sources, like CERT (Computer Emergency Response Team). Other solution is preparing data using simulation.

To conclude we can say that only implementing heterogeneous environments with combination of software and hardware, commercial and open source components can lead to ensuring a good level of reliability. And consequently in such a way we can increase level of security of information systems.

References

[1] Anderson, R. (1993). Why Cryptosystems Fail. *1st Conference on Computer and Communication Security*. VA, USA.

[2] Anderson, R. (2001). Security engineering. *A Guide to Building Dependable Distributed Systems.* John Wiley & Sons Inc.

[3] Hazlewood, V. (2007). Defense-in-depth. An Information Assurance Strategy for the Enterprise, San Diego 2006, (http://security.sdsc.edu/DefenseInDepthWhitePaper.pdf, February 2007)

[4] Jóźwiak, I.J. (1992). The reliability and functional model of computer network with branched structure. *Microelectronics and Reliabilit.* Vol. 32, nr 3, 345-349.

[5] Jóźwiak, I.J. (1996). The failure time random variable modeling. *Microelectronics and Reliability*. vol. 36, 10, 1525-1529.

[6] Jóźwiak, I. & Laskowski, W. (2003). Reconfigurable hardware and safety and reliability of computer systems. *Risk Decision and Policy Journal*. Philadelphia.

[7] Kołowrocki, K. (2004). *Reliability of Large Systems.* Amsterdam-Boston-Heidelberg-London-New York-Oxford-Paris-San Diego-San Francisco-Singapore-Sydney-Tokyo, Elsevier.

[8] Laskowski, W. (2001). Układy programowalne jako narzędzia wspomagające kryptograficzną ochronę danych. *Przegląd Telekomunikacyjny* 3, 178-183.

[9] Liderman, K. (2003). *A guide for security administrators.* Warszawa (in Polish).

[10] SANS Institute, Intrusion detection FAQ. (2007). (on line: http://www.sans.org/resources/idfaq).

[11] Varian, H. (2002). *System reliability and free riding*. Workshops on Economics and Information Security. Berkeley, (on line: http://citeseer.ist.psu.edu/527418.html).

Virus Encyclopedia, CA. (2007). (http://www3.ca.com/securityadvisor/virusinfo/browse.aspx).

STABILITY AND SAFETY OF SHIPS: HOLISTIC AND RISK APPROACH

Kobyliński Lech

Foundation for Safety of Navigation,
Gdansk, Poland

Keywords
maritime safety, risk analysis, ships' stability, ice accretion on ship

Abstract
Present stability regulations developed over the years by IMO reached definite conclusion with the adoption of the Revised Draft of the Intact Stability Code. The criteria included there are design criteria of the prescriptive nature, based mainly on statistics of stability casualties. Currently IMO is considering development of criteria based on ship performance. Concept of such criteria is, however, at present not agreed. The criteria are working comparatively well with regard to the majority of conventional ships, however advent of very large and sophisticated ships of non-conventional features caused that those criteria may be inadequate. The author advances the idea consisting of application of safety assessment and risk analysis using holistic and system approach to stability. Safety against capsizing (or LOSA accident) is a complex system where design, operational, environmental and human factors have to be taken into account. Although this seems to be a very complex task, in the opinion of the author it may be manageable and could be applied for safety assessment of highly sophisticated and costly ships.

1. Introduction

One of the most important aspects of safety is safety against capsizing. In modern times capsizing is an accident that is not happening often, but if it happens, the consequences are usually catastrophic and ship is lost, quite often with all hands on board. When the number of lost lives is large, the public opinion reacts to such accidents acutely, almost hysterically, as for example in the case of ESTONIA disaster, and the consequences of the accident to the maritime world may be rather serious. That is why safety against capsizing is an important issue.

In order to avoid possibility of capsizing, criteria for ship stability were developed. Some simple criteria were proposed quite long time ago, in the middle of nineteenth century, but the most recent criteria were developed and recommended by the International Maritime Organisation (United Nations Agency) in late sixties and early seventies of the last century. Those criteria are used until this day in some countries; recently they were included in the Code of Intact Stability for All Types of Ships developed by IMO and they will become compulsory under the provisions of the SOLAS Convention in 2009.

The existing criteria are design oriented and their essence consists of specification of critical values of some stability parameters. In spite of the fact, that some ships satisfying those criteria capsized, the general opinion is that the great majority of ships are reasonably safe.

The existing criteria may be, however, not applicable to some types of modern ships incorporating novel design features. There is no previous experience in relation to safety and stability of those ships and to satisfy existing criteria may not assure required level of safety. Because of this, Marine Safety Committee of IMO recently included in its work programme the item requiring development of performance-oriented criteria for ships of novel ship type.

Performance oriented criteria according to this definition, but also according to the understanding of the majority of members of the IMO SLF Sub-committee, are criteria that take into account scenarios of capsizing of the ship in a seaway. However, forces of the sea are not the main hazard posed to the ship. Analysis of causes of stability accidents reveals that in more than 80% of casualties human factor is the principal cause, in the remaining accidents factors such as cargo shift, icing or other heeling moments are often initiating events. Therefore, the author proposed that instead of developing additional prescriptive criteria provision may be used, already included in the SOLAS Convention (Chapter II-1, Part B-1, regulation 25-1.3) allowing the Administration to apply, under certain conditions, alternative methods if it is satisfied that it least the same degree of safety as represented by the existing requirements is achieved.

If the formulation of this provision (rather often used in IMO instruments) is understood as such, that the objectives are specified, it opens the way to application of the holistic and risk-based approach. Chantelave [3] discussed this problem. Obviously, as the application of risk analysis is not an easy task, the provision should be supplemented by guidance to the Administration.

Full risk analysis for the particular ship or group of ships requires large resources that were not available to the author. Therefore risk analysis was executed on a limited scale, and in particular group of experts consisted of few persons. The purpose of the exercise was to investigate the possibilities of application holistic and risk approach to stability problems and create some basis for possible content of guidance such as mentioned above. In the paper only some parts of the analysis are referred; the other parts of the exercise will be published in other places.

2. Holistic and system approach

As mentioned above, existing criteria are design criteria intended to be applied during the design stage of a ship. However, even the preliminary analysis of stability casualties shows, that design features of the ship are not the most important nor most often cause of casualty. Casualty – it will be in the following called LOSA –(loss of stability accident) [16], is usually the result of a sequence of events that involve environmental conditions, ship loading condition, ship handling aspects and human factor in general. Therefore in order to make safety assessment holistic approach is needed to the ship stability system.

Ship stability system is rather complicated. However, in most cases it could be considered as consisting of four basic elements: ship, environment, cargo and operation (See *Figure 1*). The Venn diagram in this figure stresses strong interactions between the four elements. The use of the system approach to stability criteria was proposed by the author quite long time ago and it was partly applied in development of the Intact Stability Code [12], but in general until this day stability requirement remain basically design oriented. Analysis of LOSA casualties reveals that the causes of casualty may be attributed to:

- functional aspects resulting from reliability characteristics of the technical system, therefore stability characteristics of the ship
- operational aspects resulting from action of the personnel handling the system, therefore crew members but also ship management, cargo handling, marine administration and owners company organisation
- external causes resulting from factors independent from designers, builders and operators of the technical system therefore ship environment and climatology [4], [5].

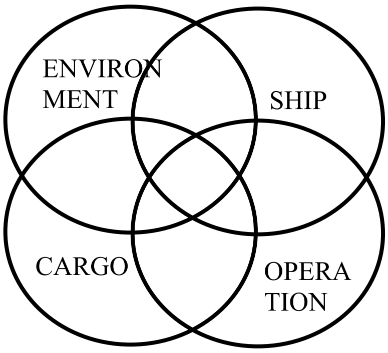


Figure 1. Four-fold Venn diagram for ship stability system

Human factor plays important part in all four elements of the system. Human and organisational errors, HOE, according to some authors, are responsible for approximately 80% of all marine casualties [17], other sources definitely stated that this percentage is 80% [23]. In order to achieve sufficient level of safety with respect of stability, all elements creating stability system have to be taken into account. Taking into account the fact, that less than 20% of all casualties are caused by faulty or bad design of the ship, the existing safety requirements that refer mainly to design features of the ship can not insure sufficient level of safety, in particular with regard to ships having novel design features. The only way out of this would be to use risk-based approach.

3. Prescriptive versus risk-based approach

In many fields of technology when planning highly sensitive and costly enterprises risk analysis is performed nowadays. The Marine Safety Committee of IMO recommended using this approach in IMO rule making process [11]. In spite of this recommendation, and in spite of the fact that risk analysis is performed, for example, as a rule in offshore industry experts on stability are hesitant to use this approach, still preferring development of prescriptive criteria.

Conventional prescriptive approach to the problem of safety that is used for a very long time is in the form of a recipe defining maximum or minimum values of some parameters. This approach is now substituted by safety assessment and analysis of risk. In place of rigid formulae, the disadvantage of which is insufficient flexibility to innovative of the system and that may be changed only using small steps, new risk based requirements are oriented on attainment of the target that is safety of the system.

Traditional regulations related to stability are of prescriptive nature and usually are based on deterministic calculations. They are formulated in the way where a ship dimension or other characteristic (e.g. metacentric height) must be greater (or smaller) than certain prescribed quantity. Prescriptive regulations could be developed on the basis of statistics, model tests and full-scale trials. In some cases probabilistic calculations might be also used as a basis of prescriptive regulations

The basic dichotomy in the conception of safety requirements consists of prescriptive approach versus risk-based approach. The main shortcoming of prescriptive regulations is that they are bounding designers and they do not allow introduction of novel design solutions. They are based on experience gained with existing objects and they are not suitable to novel types. Usually they were amended after serious casualties had been happened. The risk involved and the level of safety with the application of prescriptive regulations is not known [15].

At the opposite to the prescriptive regulations there is risk-based approach. In the risk-based approach the regulations specify objectives to be reached that is safe performance of an object. Risk-based approach could be described as a goal-oriented performance based approach utilizing, usually, probabilistic calculations. However, it is possible to imagine. The advantages of risk-based approach are obvious. They give free hand to the designers to develop new solutions, they actually allow taking optimal decisions from the point of view of economy and the risk to the public and to the environment is assessed and accepted.

All existing stability regulations are of the prescriptive nature. At present, however, the need to apply risk-based approach is recognized and actually recommended. However, up to now there are very few attempts to apply, at least partially, this approach to stability problems.

Risk-based approach according to IMO recommendation is formalized and includes the following steps:

1. Identification of hazards
2. Risk assessment
3. Risk control options
4. Cost-benefit assessment, and
5. Recommendations for decision making

4. Hazard identification

The first step of a risk analysis is to carry out hazard identification and ranking procedure (HAZID). Hazards could be identified using several different methods.

IMO resolution included general guidance on the methodology of hazard identification. With respect to stability, hazard identification could be achieved using standard methods involving evaluation of available data in the context of functions and systems relevant to the type of ship and mode of its operation. Stability is considered assuming that the ship is intact and accident evaluated is called LOSA (loss of stability accident) that is covering capsizing, that means taking position upside down, but also a situation where amplitudes of rolling motion or heel exceed a limit that makes operation or handling the ship impossible for various reasons -loss of power, loss of manoeuvrability, necessity to abandon the ship. In the last situation the ship may be salvaged [16].

According to general recommendation the method of hazard identification comprises mixture of creative and analytical techniques. Creative element is necessary in order to ascertain that the process is proactive and is not limited to hazards that happened in past. For this purpose a group of experts should be created consisting of specialists in design, operation, management and human factor.

Hazards identification was based on

1. Analysis of historical data on LOSA accidents.
2. Statistical analyses of cause of accidents available in various sources, *inter allia* in [1], [8], [9], [10]
3. Detailed description of LOSA accidents. For this purpose accidents of 20 described in detail casualties were analysed,
4. Analysis of the few accidents using TRIPOD methodology [22]
5. Evaluation by experts using DELPFIC method
6. Analysis by the group of experts

The group of experts was requested to evaluate the results of all the above analyses and to propose a list and ranking of hazards. Because of available resources to conduct engineering analysis was preferred in opposite to expert analysis as defined in [7].

The expert group recognized that the number of hazards defined as a potential situation to threaten the ship stability when considering all elements of the stability system is large and because of that decided to consider on the first level the following hazards

1. critical stability
2. forces of the sea
3. cargo shift
4. icing
5. human factor- management
6. external heeling moments
7. cargo and ballast operations
8. fire and explosion

Figure 2 shows fault tree for the first level. It shows all eight groups of hazards connected by “OR” gate; this however, does not preclude that two or more hazards may be present at the same time. The system is rather complex, because in further down levels of the fault trees there are strong interconnections between different factors. This is shown in the example of the fault tree (*Figure 4*).

In the above list, insufficient stability is defined as stability characteristics that do not meet IMO current requirements. Cargo shifting was singled out because in more than 300 LOSA casualties cargo shift occurred in about 40% cases. Fire is important because fire fighting water can reduce stability and cause capsizing (example: NORMANDIE in New York harbour in 1942). Forces of the sea include action of waves and wind. This may be the most difficult hazard to evaluate because of the complex hydrodynamic structural model of behaviour of the ship in a seaway. External heeling moments comprise different heeling moments apart of heeling moments caused by forces of the sea and shifting of cargo. In this category are heeling moment caused by water on deck, by centrifugal force when turning, fishing gear pull, tow rope forces etc.

Ranking for the frequency of hazards adopted in the application of Delphic method consisted of five groups (1 to 5) as proposed in [6]: (frequent, probable, occasional, remote and unlikely) that is different from the IMO recommendation [11]. Different ranking indexes are related to probabilities, but this was not revealed to participants of the exercise, because it seems that assessment of probability is very subjective and does not lead to reliable results. This is shown in *Table 1*.

Ranking, as proposed by the group of experts, that took into consideration all the above-mentioned results, differs in rather wide limits. That is understandable, because hazards probability is obviously different for different types of ships and for different modes of operation. For example, icing need not to be considered as hazard for ships operating in Mediterranean, and requires high ranking for ship s operating at high latitudes. The same applies to shifting of cargo, because in some ships there is no cargo that can shift. Therefore no probabilities were attached to hazards at the first level. However an example of averaged ranking estimated by the group of nine experts is shown in *Table 2*.

Probabilities could be attached to different hazards when second and further down levels in fault trees are identified. Therefore the next step in the identification of hazards and estimation of their probabilities is construction of fault trees and event trees.

Table 1. Hazards classification

R	Description	Frequency per ship	Frequency per fleet	Probability (hourly)
1	Frequent	Likely to occur frequently – one or more times per year	Continuously	Greater than 10^{-3} do 10^{-4}
2	Probable	Several times per ship's lifetime – once every few years	Once or more times in a year	10^{-4} do 10^{-5}
3	Occasional	Likely to occur once during the lifetime of the ship	Several times during fleet's lifetime – once every few tears	10^{-5} do 10^{-7}
4	Remote	Unlikely, but possible during lifetime of the ship	Probable once during lifetime of the fleet	$<10^{-7}$
5	Extremely improbable	So extremely remote that it does not to be considered as possible to occur		Substantially less than 10^{-7}

Table 2. Averaged ranking of hazards as assessed by the group of experts

Hazard	Ranking			
	Ferry	Passenger ship	Container	Bulk carrier
Insufficient stability	1	4	2	2
Forces of the sea	4	4	3	4
Cargo shifting	4	1	3	3
Icing		4	4	
HOE	3	5	2	4
External heeling moments	2	3	3	2
Cargo and ballast operations	3		4	3
Fire and explosion	4	4	3	4

5. Risk evaluation

Risk is defined as a product of hazard probability and hazard severity (consequences):

$$\mathbf{R = P \cdot S}$$

To facilitate the ranking and validation of ranking IMO [11] recommended to define consequence and probability indices on a logarithmic scale. A risk index may therefore be established by adding the probability (frequency) and consequence indices. We have then:

$$\text{Log (risk)} = \text{Log (frequency)} + \text{Log (consequence)}$$

In order to assess risk, both quantities in the above equation should be evaluated. IMO recommended for the maritime safety uses–for the frequency of accidents ranking from FI=7 (frequent) to FI=1 (extremely improbable) and for consequences scale SI=1(negligible), SI=2 (marginal), SI=3(critical) and SI=4 (catastrophic). This classification is useful for the safety assessment in particular for the evaluation of risk control options.

With regard to safety against capsizing obviously we may consider only levels of frequency 1 to 4 and hazard severity of the category SI=3 (critical) and SI = 4 (catastrophic) because capsizing or loss of stability accident has always catastrophic or critical consequences and, on the other hand, probability of capsizing must be kept low. Catastrophic effect (Category SI = 4) would mean capsizing and loss of the ship, whether critical hazardous effect (Category SI =3) would mean dangerous list and loss of ability to sailing further, which, according to definition would mean loss of stability accident (LOSA).

Based on the above risk index matrix could be constructed (*Table 3*). The risk indexes applicable to stability (safety against capsizing or against LOSA accident) are grouped in the lower right corner of the matrix.

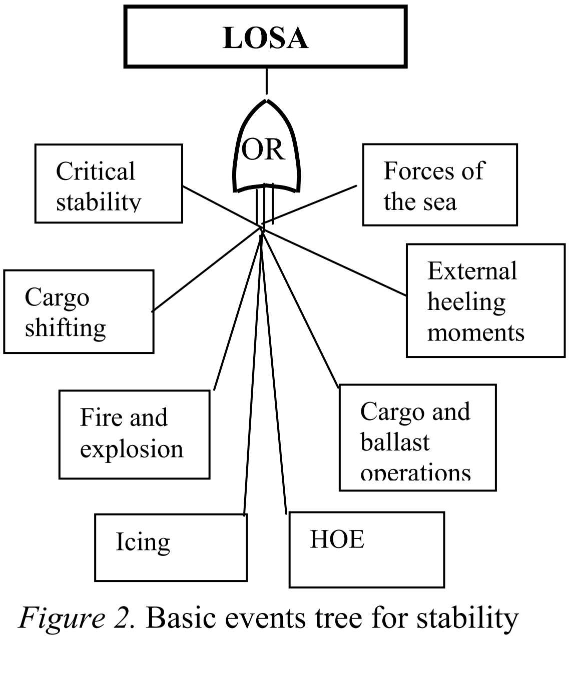


Figure 2. Basic events tree for stability

For assessment of risk index and in order to construct risk matrix, IMO resolution recommended using hazards and operability study (HAZOP). Frequencies of hazards could be assessed on the basis of risk contribution trees (RCT) being a set and combination of all fault trees and event trees as defined below [11].

A fault tree is a logic diagram showing the casual relationship between events, which singly or in combination occur to cause the occurrence of higher level event. It is used to determine the probability of the top event. Fault tree is to-down procedure systematically considering the causes and events at levels below the top event. The top events are events shown in the *Figure 2.*

Table 3. Risk matrix

Risk Index (RI)					
FI	FREQUENCY	SEVERITY			
		1	2	3	4
		Minor	Significant	Severe	Catastrophic
7	Frequent	**8**	**9**	**10**	**11**
6		**7**	**8**	**9**	**10**
5	Reasonably probable	**6**	**7**	**8**	**9**
4		**5**	**6**	**7**	**8**
3	Remote	**4**	**5**	**6**	**7**
2		**3**	**4**	**5**	**6**
1	Extremely remote	**2**	**3**	**4**	**5**

An event tree is logic diagram used to analyse the effect of an accident, a failure or an unintended event. The diagram shows the probability or frequency of the accident linked to those safeguard actions required to be taken after occurrence of the event to mitigate or prevent escalation. An event tree is down-top procedure starting from the undesired event and leading to possible consequences.

In the risk analysis of stability safety a number of risk contribution trees (RCT) have to be constructed, for each of the undesired event (hazard) in the first level hazard identification tree (*Figure 2*). Moreover, for some hazards require more than one fault and event tree to be constructed, because of possibility of different capsizing scenarios. Therefore, before RCT are constructed, different modes or scenarios of capsizing must be identified. This is particularly important with regard to forces of the sea, where more than twenty different capsizing scenarios could be identified.

Generally it appears that within risk analysis the system of RCT's may be quite complex, but in cases of risk analysis for concrete design it may by considerably simplified, because some of the hazards identified may be not applicable. As an example of this method risk contribution trees in the case of icing is shown.

6. A case study - icing

Icing was considered by the group of experts as one of the most serious hazards that may cause LOSA. Generally icing is considered dangerous for small ships and in particular for ships operating in high latitudes. However experts were of the opinion that icing is also dangerous for larger ships and not necessary operating in arctic water. As an example it was shown the photograph of icing that happened onboard M/S STEFAN BATORY in North Atlantic (*Figure 3*).

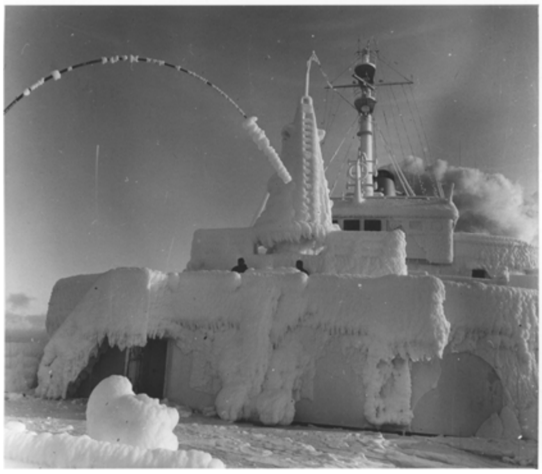


Figure 3. Example of icing in North Atlantic.(Photo: Kpt. Ż.W. Hieronim Majek)

Requirements concerning icing are currently included in the recommendatory part of the IS Code [12]. They are limited to the specification of amount of ice that has to be taken when calculating stability of ships sailing in certain areas. Those are general recommendations, the Administrations are encouraged to use different values of accrued ice if they have their own experience.

Te ice accretion is, however, o complex process. Not entering into details, it can be stated that ice accretion depends on several factors, of which the sea state, air and sea temperatures, wind velocity, ship speed and heading with regard to wind direction are of importance. In many cases ice accrued may exceed several times values recommended by IMO IS Code. Analysis of LOSA accidents reveals several casualties caused by ice accretion, some of them even in Black Sea [21].

The structural model for calculating effect of ice accretion is simple and it is identical to putting additional load onboard, but as the ice is accrued mostly on exposed decks, superstructures and rigging, the centre of gravity of ice accrued is positioned high. Therefore stability of the ship is impaired and the ship might be in dangerous situation.

The branch of fault tree for the case of dangerous icing must take into account

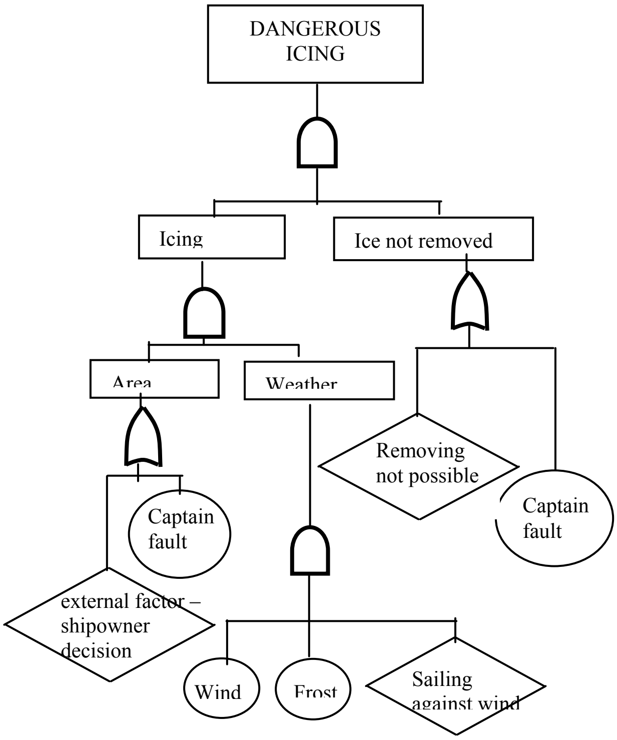


Figure 4. Branch fault tree for dangerous ice accretion

The branch of fault tree for the case of dangerous icing must take into account scenarios that may lead to LOSA accident. In all cases of icing the metacentric height and stability lever arms are reduced.

The simplest scenario is when the amount of accrued ice is so large, that the metacentric height becomes negative and the initial part of the stability lever arms curve is also negative. With the reduction of the stability characteristics probability of LOSA may increase even by two to three orders.

More complex scenarios, where human factor must be considered, are also possible. Accrued ice should be removed by the crewmembers. However it is not always possible. If the ship is sailing against the wind and waves in severe storm, when the conditions are most favourable for ice accretion in the bow quarters, it is not possible to send crew towards the bow in order to remove ice. It would be necessary to turn the ship to sail with the wind. Such manoeuvre is, however, dangerous and it may cause ship capsize, in particular if the removal of ice was started to late when the stability of the ship was already low.

Examples of fault tree and event tree for the case of dangerous icing are shown in *Figure 4* and *Figure 5*. It is obvious that two conditions are necessary for ice accretion: the ship must be in the area where icing is possible, and also weather conditions must allow that (negative temperatures, wind). Situation, where the ship is in the area where icing is possible and there are unfavourable weather conditions depends on sailing route, then on ship owner request or on decision of master who ignored the danger and makes no attempt to avoid the dangerous area.

Attaching probabilities to various events that appear in the fault tree and estimating on this basis probability of the top event should be accomplished mainly using expert's opinions. In some cases statistical data may be available in ship owners data bank. Review of the literature reveals that in case of icing such data were collected by some research institutes, but generally they refer to the amount of accrued ice in various conditions. Statistical data on effect of operational measures in case of icing are not available and probabilities could only be assessed o upon studying as many as possible real situations and accidents.

7. Risk control options and acceptability of risk

Considering risk control options three levels of action may be necessary if the risk index is over, say, grade 3.

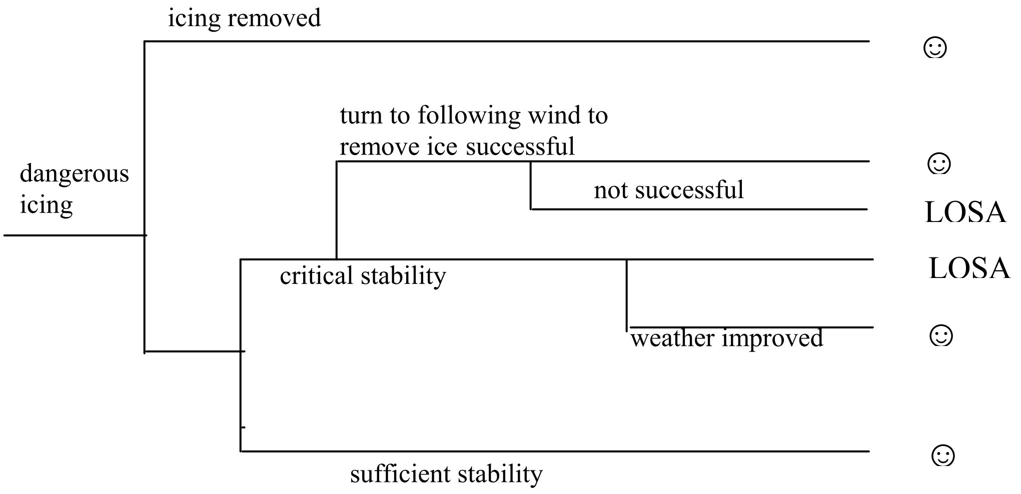


Figure 5. Event tree for severe icing consequences

Grade 8-9 – action to eliminate the hazard or hazardous situation (intolerable region)
Grade 6-7 – action to control or reduce the probability of the hazardous situation (tolerable region)
Grade 4-6 – action control the hazard, desirable, if cost effective

This problem is not elaborated because lack of space. Reference is made to [14] where risk acceptability and risk control options are discussed more widely.

8. Conclusion

Application of risk analysis may be quite complex task, requiring employment of large group of experts and analysts, nevertheless, is realistic. Risk analysis would reveal weak points in ship design, but also, which is more important, in management and operational procedures. It can also show where barriers have to be put in order to control risk. Risk analysis must be viewed as advantageous in comparison with the traditional prescriptive approach, although the last being much simpler, will certainly be used in majority of cases. Obviously, because of high effort and cost of performing risk analysis, in practice it could only be applied in cases of highly sophisticated large ships or ships with novel design features.

References

[1] Aksiutin, L. P. & Bliagoveschensky, S. N. (1975). *Avarii sudov ot potieri ostoichivisti,* Sudostroenye, Leningrad.

[2] Alman, P. R., Minnicck, P. V., Sheinberg, R. & Thomas III, W. L. (1999). *Dynamic capsize vulnerability: reducing the hidden operational risk.* SNAME Annual Meeting, paper No.10.

[3] Chantelauve, G. (2005). *On the use of risk analysis in maritime certification and classification.* Advances in Safety and Reliability ESREL 2005, Vol. I p. 329.

[4] Cleary, W. A. (1975). *Marine stability criteria*. Proceedings of the 1st International Conference on Stability of Ships and Ocean Vehicles, Glasgow.

[5] Ericson, A., Persson, J. & Rutgerson, O. (1997). *On the use of Formal Safety Assessment when analyzing the risk for cargo shift in rough seas.* RINA International Conference Design and Operation for Abnormal Conditions, Glasgow.

[6] Halebsky, M. (1989). *System safety engineering as applied to ship design*, Marine Technology, Vol. 26.

[7] Hokstad, P., Øien, K. & Reinertsen, R. (1998). *Recommendations on the use of expert judgement in safety and reliability engineering studies. Two offshore case studies.* Reliability Engineering & System Safety, Vol. 61, No.1/2.

[8] IMO (1966). *Analysis of intact stability casualty records of cargo and passenger vessels.* Joint report submitted by the Federal Republic of Germany and Poland. Doc. IS VI/3.

[9] IMO (1966a). *Analysis of intact stability records of fishing vessels.* Joint report submitted by the Federal Republic of Germany and Poland. Doc. PFV IV/2.

[10] IMO (1985). *Analysis of intact stability casualty records.* Submitted by Poland. Doc. 30/4/4 and SLF/38.

[11] IMO (2002). *Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process*. Doc. MSC/Circ.1023; MEPC/Circ.392.

[12] IMO (2006). *Revised Intact Stability Code Prepared by the Intersessional Correspondence Group.* Submitted by Germany. Doc. SLF 49/5.

[13] Kobyliński, L. (1984). *Philosophishe und Hydrodynamische Probleme der Internationalen Kenterkriterien von Sciffen.* Intern. Schiffstechnische Symposium, Rostock.

[14] Kobyliński, L. (2004). *Application of the FSA methodology to intact stability criteria.* Marine Technology Transactions, Vol. 15, pp 319-329.

[15] Kobyliński, L. (2005). *Appraisal of risk assessment approach to stability of ships.* International Workshop on Ship Stability, Istambul.

[16] Kobyliński, L. (2006). Alternative stability requirements based on system and risk approach. Rio de Janeiro.

[17] Manum, I. A. (1990). *What have guided international activities on intact stability so far?* Proceedings of the 4th International Conference on Stability of Ships and Ocean Vehicles, Naples.

[18] McTaggart, K. & de Kat, J. O. (2000). *Capsize risk of intact frigates in irregular seas.* SNAME Annual Meeting, No. 8.

[19] Schauer, T., Romberg, B., Jiang, Ch. & Treasch, A. W. (1995). *Risk assessment of small fishing vessel trap net operations.* Marine Technology, Vol. 32. No. 4.

[20] Spouge, J. (1996). *Safety assessment of passenger/ro-ro vessels.* RINA Intern. Conference on the safety of passengers in ro-ro vessels. London.

[21] Sukhanov, S. I., Panov, V. V. & Lavrenov, I. V. (2003). *Extreme ship's icing in the Black Sea.* Arctic and Antarctic Research Institute, Russia No. 04-05-64306.

[22] Bekke, E. C. A., van Daalen, E. F. G., Willeboordse, E. J., Boonstra, H., Keizer, E. W. H. & Ale, B. (2006). *Integrated safety assessment of small container ships.* 8th Intern. Conference on Probabilistic Safety Assessment and Management, New Orleans.

[23] U. S. Coast Guard (1995). *Prevention through people.* Quality Action Team Report.

RELIABILITY WAVE IN LIGHT OF THE NANO DEVELOPMENT

Kuo Way

The University of Tennessee,
Knoxville, TN, USA

Keywords
stress test, nano technology

Abstract
This talk is based on the Editorial of *IEEE Transactions on Reliability*, December, 2006 and discusses a framework for applying reliability principles and practices to the emerging nano technology fields.

1. Introduction

To Build for the Future, we must achieve major advances related to reliability in addition to exploring and discovering interdisciplinary connections in important cutting-edge research areas. The technologies for today's design and manufacturing have for some time been steadily moving from the realm of the micro- to the nano-scale, but advancements in reliability have not kept up with the pace!

2. Reliability and nano technologies

New ideas and connections stimulated by modern advancements are appearing in the bio, energy, and computing fields while design, manufacturing, and reliability modelling are being left behind. For example, fabrication technologies for integrated circuits are on the edge of the nano scale, with a gate length of less than 100 nm in the most advanced microprocessors [1], [2], and some capacitors are already available on a scale of 1-2 nm equivalent oxide thickness [3]. In particular, micro-electromechanical (MEM) devices are integrating mechanical motion with electronics on the micro-scale, and thereby, generating novel approaches to applications and new industries. Furthermore, we are already developing the scientific base – nano theory, fabrication science, materials sophistication, and manufacturing capabilities – for a full-scale assault on nanotechnology. But we must ask if the manufacturing community is ready for producing nano devices, and whether the reliability community is ready to certify proper use of these nano devices-based systems.

Even more fundamentally, we must ask: what is the meaning of reliability for systems that use nano or new technologies, and how do we interpret this meaning in practice? For example, are consumers likely to be satisfied with high cost plasma TVs with an estimated 5-7 year expected life? As reliability engineers, we must not only bridge multiple cutting-edge disciplines to complement the technology-rich industries, but also be leaders in guaranteeing that high tech products and systems perform to acceptable modern standards.

The activities associated with nano development are expected to enhance international understanding and collaboration for a bright, fast-moving future in design, manufacturing, and industrial innovation. Reliability research and development work in the past has contributed to the industrial world by enhancing the quality of the products. The academic community has also played a critical role in the process by making fundamental discoveries that have contributed to the realization of this quality enhancement. Examination of the numerous issues and papers published *by IEEE Transactions on Reliability* over the past 55 years clearly demonstrates the significance of the academic role in the advancement of our field.

However, it is also important to recognize that recently our profession seems to have stagnated in terms of making new contributions to the emerging technologies, electronics and otherwise. How much have we contributed to the reliability of the existing, reliable MEMS and nano devices?

Although reliability is very much a central concern in nano technologies, the reliability community has made little progress in developing new methodologies and standards that are applicable in this realm. Instead, we seem to be leaving that up to the industrial practitioners who had not been rigorously trained in reliability.

2.1. Four challenges

There appear to be four major challenges related to nano electronics that currently face the field of reliability: identification of the failure mechanisms, enhancement of the low yields of nano products, management of the scarcity and secrecy of the available data, and preparation of reliability practitioners and researchers for keeping up with the nano era.

2.1.1. Identification of the failure mechanisms

As new generations of nano electronics are invented almost daily, we become less familiar with the failure mechanisms of these devices, and the reasons behind the failures. With our existing knowledge, we often can not identify the correct faults; and in fact, we are likely to see many no-fault-found failures. Nor can we manufacture reliable products with full confidence.

Shorting (e.g., inadequate etching processes or insulating structure), and opening (e.g., electro migration of nano wires) of interconnect lines caused most of the failures in traditional electronic products. Will the new trend be toward more open / resistive related failures because of the new materials, large number of contacts/vias, higher functional speeds, new circuit design rules, and other factors? Identifying the failure mechanisms in nano electronics will have impact on determining the right strategies for life testing, highly accelerated stress screening (HASS), burn-in screening for reliability enhancement, reliability prediction, warranty duration and conditions, and many other processes. The hurdle in comprehending nano failure mechanisms seems greater than previous hurdles that dealt with similar issues in the past. We are unsure as to whether much of the knowledge that is based on past technologies is still valid for reliability analysis. Understanding the failure mechanisms of nano electronics is critical for preparing system designers to better utilize nano devices, and design better fault tolerant systems.

2.1.2 Enhancement of the low yield in nano products

The development of nano devices, such as those used in commercial and military systems, has generated a lot of excitement. However, the low yield rate [2], [4] of current nano devices, typically 10% or lower, is very troublesome. Low yield makes production extremely expensive, and the product's expected life uncertain. The low yield also creates a challenge for both the designers and scientists to find better materials and fabrication tools. At the early nano product fabrication stage, low yield is actually a technology agenda, rather than a logistics issue, although some believe that scheduling & logistics optimization can improve the yield. Although low yield is a fundamental material-related problem that modern reliability engineers must face in order to improve yield at an affordable cost, it is also a design issue because many modern systems are increasingly complex, and the product life cycles are often too short to achieve better yield.

2.1.3. Management of the scarcity and secrecy of available data

Manufacturers have always kept reliability and yield data secret, or not kept it at all. The problem is compounded by the scarcity of failure data, which makes it almost impossible to use traditional reliability analysis tools and statistical inference to make useful predictions. Therefore, experienced analysts have to perform in-house analyses using *ad hoc* approaches. Despite that many statisticians have in the past been against using the Bayesian approach because of the "lack of credibility" associated with it, we are now forced to be more Bayesian than ever before.

In fact, many engineers have always used the Bayesian approach successfully, although in the eyes of the theoreticians, their methodology has not been mathematically rigorous. It is important to note that the Bayesian approach is more than a tool--it is also a philosophy. Many academic statisticians have contributed to theories of reliability; on the other hand, it is perhaps more obvious that the empirical approaches used by reliability engineers have improved numerous products and systems for consumer use. We predict that the Bayesian approach will be even more frequently utilized in the nano era as product life cycles based on new technologies become even shorter, and it is becoming impossible to obtain sufficient data before a new product requires reliability assessment. The other possibility, with great challenge too, is to predict reliability using the computer-aided tools, based on the physical properties of the nano systems. Here the reliability calculation will be physics-based.

Given the useful life of many products is short (not necessarily because of reliability concerns, but more because of using the new nano technologies which may provide the users with more features) before the customers express an interest in using the new products, is the traditional life-cycle analysis still valid?

2.1.4. Preparation of Reliability Practitioners and Researchers for Keeping up with the Nano Era

As society adapts to the nano and bio world, and we integrate these technologies into more complex systems, it becomes ever more important to hold products accountable, and to require better quality and reliability from them. To cope with this challenge, modern statisticians and reliability engineers need to re-engineer themselves to learn about the nano world. In order not to be left behind the modern society in terms of technology advancement, researchers must become less bogged down in the old, purely academic exercise of separating hypothetical problems from real world problems, and applying only mathematically rigorous approaches.

Reliability academicians need to become more problem-driven than hypothesis-driven. Reliability faculty must update their course materials as well. Biostatisticians appear to be doing a better job of dealing with the fast-changing bio world than we are doing in dealing with the nano electronics. Perhaps they can serve as role models. Therefore, in order to be relevant, reliability specialists need to be versed in modern technology; reliability analysis, and modelling for the nano technologies will have to be more physics-based. At the system level, we need to learn how to integrate nano technologies into larger systems so that interfaces between technologies are reliable and better understood.

3. Conclusion

High reliability and high yield are necessary to guarantee the advancement & utilization of micro, and nano products. Reliability researchers need to be energized to tackle the very real problems that we face in the nano-rich world. Reliability practitioners and researchers need to understand the paradigms and issues, such as those listed above, involved in the nano technologies.

Keeping systems simple is important; otherwise we will add more uncertainties to the compatibility problems [5], [6]. The research dealing with the understanding and application of reliability at the nano level has demonstrated its attraction and viability. Optimal system design that considers reliability within the uniqueness of nano systems has hardly been reported in the literature, and hence deserves a lot more attention. We must share our reliability experience with designers so that, in the future, they can consider other options (e.g., to be more fault-tolerant) when dealing with large, complex systems using nano technologies.

I anticipate that our society will expect reliability specialists to take heavy responsibility for utilizing & certifying the use of nano technologies. To that end, we must break out of this period of disciplinary stagnation, and redouble our efforts to prepare ourselves to advance the state of the art of the nano technologies.

References

[1] The National Academies Keck Futures Initiative Nanoscience and Nanotechnology Steering Committee. (2004). *Designing Nanostructures at the Interface between Biomedical and Physical Systems.* National Academies Press, 106 pp., Washington, DC.

[2] The National Academies Press. (2002). *Implications of Emerging Micro- and Nanotechnologies*, 251 pp., Washington, DC.

[3] Yue Kuo. (2006). *Thin Film Nano & Microelectronics Research Lab.* Texas A&M University.

[4] Way Kuo & Kim, T. (1999). An Overview of Manufacturing Yield and Reliability Modeling for Semiconductor Products. *Proceedings of the IEEE*, 87(8), 1329-1346.

[5] Way Kuo & Prasad, V. R. (2000). An Annotated Overview of System Reliability Optimization. *IEEE Transactions on Reliability*, 49(2), 176-187.

[6] Way Kuo, Velaga, R., Tillman, F. A. & Hwang, C. L. (2001). *Optimal Reliability Design*: *Fundamentals and Applications*, 411 pp., Cambridge University Press, U.K

RISK ASSESSMENT RELATED TO INFORMATION UNCERTAINTY COMPONENTS

Rosická Zdena

University of Pardubice, Faculty
of Restoration, Litomysl, Czech Republic

Keywords
assets, data, experience, information, knowledge management, organization, tacit and explicit knowledge

Abstract

Both organization and individuals deal with and manage knowledge. Considering the basic approach, we distinguish two principal clusters: tacit and explicit knowledge. The knowledge management is targeted at making the organization knowledge operation more effective and providing the right people with relevant information at the right time. Knowledge and information uncertainty components have become one of crucial assets of any company or organization. Their crucial potential consists in smart knowledge management handling, proficiency and art to fit the risky market needs better than competitors.

1. Introduction

Mankind has been working with knowledge from beginning to everlasting end and is trying to find the way how to manage it. The difference consists in technological and scientific level and maturity of current generations. Technological level makes possible for broad masses of public free access to knowledge, and, in addition, there are scientific branches, such as neurology, genetics, psychiatry and psychology that are able to initiate undreamt-of abilities of a human brain. Simultaneously the volume of knowledge rises undoubtedly fast and we need to search for methods and tools that can assist to sort out, classify and systematize the heritage of mankind's knowledge; however, at the same time we should try to eliminate the fact the knowledge is available but the individual who needs it does not know it, therefore it is unavailable.

The purpose and goal of knowledge management are targeted at three crucial phenomena:

- a person should keep at disposal the knowledge he needs,
- the knowledge should be available at the time he needs it,
- it should be nobody but the person who needs this knowledge indeed.

There are many approaches to knowledge and knowledge management. This tendency is remarkably evident in technologically advanced branches, e.g. communications. In fact, organizations in this field do not differ in technical utilities. In case they need to differ from other competitors, they have to attract customer and offer a different product or a product with higher added value, a higher quality product or a cheaper product. Whatever method they select in order to differ from others, they must be able to exploit and take advantage of knowledge available to be better and smarter than their competitors.

2. History of knowledge management

Knowledge management is a new discipline considering its systematic approach to knowledge. People tried to manage the knowledge since its very beginning; however, we can characterize it as more or less intuitive. Depending on needs, our predecessors emphasized various aspects of knowledge utilization. In the Stone Age people's knowledge was oriented at animals, plants, weather and tribe rules and habits. Knowledge passed in tacit form, orally and through non-verbal communication. Ancient Roman period is considered a foundation of intellectual property of mankind: mathematics, philosophy, geometry, astronomy, medicine and logic were developing extremely fast. Considering the approach to r preparation knowledge, Greek philosophers and scholars characterized knowledge as something that exists objectively, i.e., something we can prove. Logical argument was one of crucial veracity tools and it has been used up to now. Plato and other Greek philosophers work with two expressions: doxa (= faith) and episteme (= knowledge). Doxa is characterized as subjective understanding of the world, this view varies, changes, it is subjective and we cannot rely on it or consider it appropriate. What is true at one moment is wrong a moment later. One considers something truth, the other does not believe it. Episteme, knowledge, on the other hand, is something constant, fixed and it does not apply just to the present time. If the consensus is reached, the knowledge is proved as knowledge: once something has been proved, therefore it is truth. In addition, written form was standardized at that time. Greek impact on knowledge understanding is remarkable up to now. Knowledge was something that did not change, i.e. unchanging abstract objects: changing world was not classified as knowledge due to its unsteadiness and changeability. This point of view limits the approach of West cultures to knowledge and it is one reason of explicit knowledge orientation.

3. Basic terminology of knowledge management

There are three basic terms applied and utilized in the field of knowledge management: data, information, and knowledge.

3.1. Data

Data can be characterized as everything able to be monitored through our senses, i.e., all we can feel, taste, see or hear. Data can also be specified as objective facts on events or sequence of attributes. Data are mostly well structured and related to a particular technology. They can be quantitatively assessed

- via expenses, i.e. means we have to spend in order to get them,
- rate, i.e., how fast we get them,
- capacity, i.e. what amount of data is available at particular moment.

Data can also be classified through qualitative indicators. In that case we observe whether

- the data are available if needed,
- they follow required demands,

the coded information included is understood properly

3.2. Information

Information can also be specified as data both through quantitative and qualitative phenomena. Qualitative assessment provides users´ benefit, i.e., to what extent the information is relevant for a user. The information is generated from data as follows:

- contextualization, i.e., the user knows the purpose why the data were gathered,
- classification, i.e., the user knows what category they belong to,
- calculation, i.e., data are analyzed through mathematical and statistical methods,
- correction, i.e., data are corrected and errors are eliminated,
- condensation, i.e., data are summarized by a user.

The information value depends on two factors:

- the price we had to pay to obtain the information,
- personal relation to the information.

Referring to the historical development point of view, our position is very curious: we do not suffer from shortage of information but from its excess and redundancy. The success of both the individual and organization consists in the ability to pick up the information which is relevant and fits the particular situation best. The problem is the user must carry out the selection by him and neither information system nor technology can substitute for him. In order to succeed and select the right one, he must acquire knowledge and information becomes a fundamental building block of knowledge.

3.3. Knowledge

Knowledge can be specified as a varying system covering interaction between experience, abilities, facts, relations, values, thoughts and meaning. It can also be specified through the term of information:

$$K = I + x,$$

where K is knowledge,
I is information,
x is what the information in the brain interacts with, i.e., our previous knowledge and abilities, experience, mental models, relations, values, principles we follow in our life, what we believe in, etc.

Knowledge is always closely related to activities and emotions and human mind: it is a part of routines, processes, practices and standards.

Knowledge
↑
Information
↑
Data

There are several ways how knowledge can be derived from the information:

- comparison, i.e., we compare new information and already familiar knowledge of similar or different situations,
- coherence, i.e., we assess the importance of information due to further decision-making and activities,
- interlinkage, i.e., we try to find the relation to knowledge that has already been available either for us or other individuals,
- conversation, i.e., we try to find out what other individuals guess about the information.

Knowledge is created in human mind and its quality and importance are assessed through activity. Sometimes it is very complicated to find, characterize and specify this delicate relationship between knowledge and activities. Knowledge cannot be stored, transported and expressed via technology. Attempts focused on its externalization resulted in knowledge damage and finally its value declined or was damaged as well.

4. Western and Eastern knowledge understanding

There are two basic approaches towards the knowledge concepts: tacit and explicit. A Swede, Karl-Erik Sveiby [6], represents explicit Western knowledge approach: he realized the importance of knowledge in order to support the competitive strength of an organization. On the other hand, his followers, Japanese representatives Nonaka and Takeuchi [3], pointed out Japanese and Asia cultural specificities. We should be aware of these crucial differences and do not underestimate them, otherwise essential mistakes and misunderstandings result in practical fails very easily. Japanese society principals are substantially different from Western cultural ones.

Western nations emphasize individuality, independence and responsibility of an individual. Japanese and other Asian nations prefer team interests and knowledge is understood primarily as tacit one. They do not understand the Western explicit verified knowledge, they consider it absolute, static and inhuman because it cannot record relative, dynamic and human dimensions. Resulting from their understanding, the same knowledge can be, depending on the situation and context, true, half-true or untrue. True knowledge is considered relative. Knowledge is a dynamic quantity created by social interactions among individuals and across the entire organization.

Knowledge and experience of Western cultures with tacit knowledge result from this specific situation and it is very complicated or sometimes impossible to apply it to Western culture. For example, typical Japanese spend all life working for one organization. Social contacts are related to the organization they work for. The individuals have minimal relationships from their organization. Every organization builds own policy, structure, identity, rules, specific communication codes, procedure and interpretation practice. As all the members know each other well, rules can be specified as informal restrictions such as taboo, habits, penalties, traditions. There are not preferred formal rules typical for Western cultures, i.e. constitution, acts, law of property, etc. This type of environment supports tacit knowledge activities. When using Japanese materials and experience, these differences have to be considered seriously. A great amount of knowledge is applicable to European or Western environment, nevertheless there are procedures and counseling which might cause demotivation or do not work at all.

5. Explicit and tacit knowledge concept

Knowledge can be understood from many points of views. Basic classification follows the explicit and tacit concept is presented in *Table 1.*

Table 1. Explicit and tacit knowledge

Explicit knowledge (objective)	**Tacit knowledge (subjective)**
Rational (mind)	Experience (relation to body)
Successive (logically provable)	Simultaneous (it is available just at a particular moment)
Theory	Related to activities

Explicit knowledge can be expressed through a formal and systematic language, i.e., we can pronounce, write, draw or visualize it. It can be expressed by formulas, data, specifications, manuals, it can be stored and carried over. Professional and scientific literature classifies explicit knowledge as information.

Tacit knowledge is created by interaction of explicit formalized knowledge and experience, abilities, intuition and personal ideas, mental models, etc. It is closely related to activities, routines, procedures, ideas, values and emotions of a particular individual. It is very complicated to express and share it. Its personal characteristic is very high and its possessor does not have to know about it at all.

There are scientists who believe that tacit knowledge can be converted into explicit one (Nonaka and Takeuchi [3]). Others (Polanyi [4]) argue it is not possible because tacit knowledge is highly personal, it cannot be formalized and transferred as it is deeply inracinated in activities and it is a part of particular operations. In case we are trying to formalize it, tacit knowledge is damaged.

Sometimes it is not possible to isolate explicit knowledge dimension from tacit one. Too much attention paid to explicit knowledge component can result in “paralysis due to analysis”. If there is dependence on tacit component too high, it can result in harmful dependence on previous success and neglecting new information, ideas and views. Explicit and tacit knowledge interacts at creative activities of individuals, e.g., we learn how to drive a car, how to manage complicated software, etc. Some knowledge classification considers not only ability to formalize knowledge but also its role and importance for the organization. Boisot [1] based its classification on the following matrix, see *Table 2.*

Table 2. Boisot knowledge classification matrix

	Non-	**Distributed**

	distributed knowledge	**knowledge**
Codified (formalized) knowledge	Proprietary knowledge	Public knowledge
Uncodified knowledge	Personal knowledge	General subconscious knowledge

Boisot classifies *public knowledge* as codified and distributed, i.e., books, textbooks, journals, periodicals and news. Public knowledge is easily transferable, however, on the other hand, it is usually fixed and cannot be simply modified.

General subconscious knowledge is distributed, generally spread and less codified compared to the previous one. Individuals get this knowledge gradually resulting from their personal life experience, their colleagues´ experience, family members, mental models, etc. This knowledge can be internalized and has impact on further understanding reality and what knowledge the individual is going to apply to.

Personal knowledge can hardly be codified, transferred and shared. It depends on personal knowledge of individual and character itself.

Proprietary knowledge always originates within particular context, and therefore it cannot be spread because it looses predictability. Organization builds proprietary knowledge depending on its development and progress.

Cultural knowledge should not be left out of consideration as well, and there are scientists who emphasize this up-to-date phenomenon, e.g. Choo [2] specifies concept of three knowledge components: explicit, tacit, cultural.

Regardless of various types of classification, every organization must understand its priorities and needs and select the relevant balance between tacit and explicit knowledge that fits demands best. Cultural criterion, however, should fundamentally be considered because factor of globalization is present, multinational expert teams and organizations are more numerous and maximum organization efficiency has become task number one and nightmare for top management [5].

6. SECI – how knowledge is created

Conversion is a theoretical simplification and example how knowledge is created. By Nonaka and Takeuchi [3], knowledge is created through interaction between individuals and different type and knowledge content. There are four basic ways how knowledge is created, see *Figure 1.*

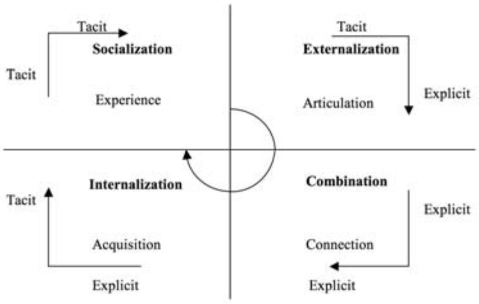


Figure 1. SECI

In real situations all four steps proceed simultaneously, nevertheless it is worth to know how to differ and classify them (combination calls for different approach than socialization), what has to be focused and how potential problems can be troubleshot.

Combination (explicit – explicit) is the simplest way and there are minimum problems. Separated explicit pieces of knowledge are associated and new explicit knowledge is created. Three basic steps are as follows:

- explicit knowledge inside and outside the organization is gathered and new explicit

knowledge is created,
- knowledge is extended,
- knowledge is edited and passed on to other users.

During internalization process (explicit – tacit) the tacit knowledge is derived from explicit one. The crucial process is classified as “learning through practical activities”. It requires time and patience and we have to realize that internalized explicit knowledge interacts in the individual mind with his previous knowledge, experience, abilities and mental models: therefore, the same explicit knowledge can result in two different outputs (it becomes useful to verify results by tests in order to prevent further misunderstanding), e.g. Hoskova [8].

Externalization (tacit – explicit) is a process of tacit knowledge articulation. There is one practical reason why to apply this method. It is easier to use explicit knowledge, it can be simply spread and distributed, and therefore it becomes a foundation for new knowledge. Tacit knowledge can be transformed into explicit one by metaphors, analogies and models.

Socialization (tacit – tacit) is a process of sharing, i.e., tacit knowledge based on other tacit knowledge, transfer and re-creation of other knowledge. It is very complicated to manage socialization because confidence and friendliness are crucial qualities of co-workers in an organization. Since externalization is time and money-consuming and requires human resources as well, organizations prefer to keep tacit knowledge in its form and share it among individuals or within a group or working unit.

6. 1. Knowledge assets

Assets in general are specific risky resources of any organization for creating values, and knowledge belongs to these assets as well. Knowledge assets are classified as input and output of knowledge creation, see *Figure 2*.

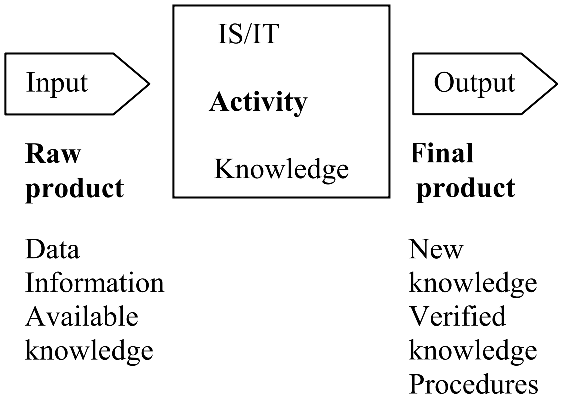


Figure 2.

Fundamental knowledge assets, i.e., data, information, knowledge, both tacit and explicit, are available for members of organizations. Knowledge is a highly dynamic and subjective concept and it has to be understood related to activities and events and is always applied to a particular individual.

Japanese approach (see *Table 3*) classifies four types of knowledge assets having direct impact on SECI conversion:

- experimental knowledge assets,
- conceptual knowledge assets,
- systematically organized knowledge assets,
- routine knowledge assets.

Table 3. Knowledge assets classification

Experimental knowledge assets	**Conceptual knowledge assets**
Tacit knowledge is shared through common	Explicit knowledge is articulated through concepts,

experience • abilities and know-how of individuals • confidence, interest , safety • energy, emotions, effort	symbols and language • product concept • design • characteristic features of the branch
Systematically organized knowledge assets Systematically organized explicit knowledge • documents, specifications, manuals • databases • licenses, patents	**Routine knowledge assets** Tacit knowledge becomes routine and it is applied to activities and practices • know-how • organization routines • organization culture

7. Conclusion

Knowledge assets are one of crucial key-stones of knowledge creation process. In order to manage process successfully, organization must be able to know and map its sometimes uncertain and risky assets in detail and find the way how to use them best for its particular needs. All the time it has to be considered that knowledge assets are highly dynamic, sometimes risky "raw material" with mutual interlinkage and relations and new knowledge is often created and origins from assets already available inside the organization.

In addition, key technological abilities must be considered as well because synergy of four dimensions is in operation simultaneously: competence of knowledge uncertainty and abilities of individuals, physical and technological support (software, machinery, and devices), managerial systems, values and standards (applied to knowledge available for particular individuals). There is always risk in knowledge management for every organization

- to know WHAT ("raw material" for decision making – who knows what + common sense, concepts, theories, mental models…),
- to know HOW (sources for effective behavior – manuals, automated processes, plans, expert knowledge, intuition, culture…).

Finally, regardless the type of knowledge – tacit or explicit, every organization is offered the same chance: to fill a gap in the market. Its crucial potential consists in smart knowledge management handling, proficiency and art to fit the market needs better than competitors.

References

[1] Boisot, M. H. (1995). Information Space: A Framework for Learning in Organizations: An Overview and Interpretation. Organization Studies 16, USA.

[2] Choo, Wei Chun. (1998). *The Knowing Organization.* Oxford University Press, UK, ISBN 0-19-511012-9.

[3] Nonaka, I. & Takeuchi, H. (1995). *The Knowledge Creating Company.* Oxford University Press, UK, ISBN 0-19-50929.

[4] Polanyi, M. (2001). Personal Knowledge towards a Post-Critical Philosophy In Nonaka, I., Toyama, R., Byosiere, P. A Theory of Organisational Knowledge Creation. Understanding the Dynamic Process of Creating Knowledge, Eudokma, Copenhagen.

[5] Rosicka, Z. (2004). Preparation of crisis manager in the area of effective communication. *Conference proceedings Crisis Situations in Specific Environment.* Zilina University, Slovakia, ISBN 80-8070-273-X.

[6] Rosicka, Z. (2006). Risk in Problems of Knowledge Management. *Proceedings of Sixth International Scientific School MASR in Complex Systems.* Saint Petersburg, Russia. ISBN 5-8088-0181-8.

[7] Sveiby, K. E. (2002). Strategy in Knowledge Economy. *Lecture at Conference KM Europe 2002*, London.

[8] Hoskova, S. (2007). Teacher – crucial subject in education and mathematical training, *In International Conference Didza 2007, Žilina,* Slovakia. in print.

COLLECTION AND ANALYSIS OF CLIMATIC MEASUREMENTS FOR THE ASSESSMENT OF SNOW LOADS ON STRUCTURES

Sadovský Zoltán

ÚSTARCH SAV (Inst. of Construction and Architecture
of the Slovak Academy of Science), Bratislava, Slovakia

**Faško Pavol, Pecho Jozef, Bochníček Oliver,
Mikulová Katarína, Šťastný Pavel**

SHMÚ (Slovak Hydrometeorological Institute), Bratislava, Slovakia

Keywords
climatic measurements, snow load, structural reliability

Abstract

Climatological measurements for the assessment of snow loads on structures as practiced in Slovakia are discussed in the light of methodologies described in the relevant backgrounds to Eurocodes. The database of yearly snow load maxima based on the weekly measurements of water equivalent of snow cover on 660 rain-gauge stations in Slovakia recorded during the last 52 winter seasons is analysed. Special interest is focused on the influence of heavy snowfalls in the winters 2004/2005 and 2005/2006, particularly on the extreme cases observed.

1. Introduction

Snow loads are of importance for the reliability of structures in the major part of European territory. Particularly, they are determining actions for light roofs of industrial buildings made of structural steel and wood.

The basic input for the design of structures subject to the actions of snow loads is the value of ground snow load at relevant site. Further step represents the definition of the relation between ground snow loads and snow loads on roofs. The present paper deals with the collection and analysis of climatic measurements for the assessment of snow loads on the ground.

A directly useable climatological record is the water equivalent of snow cover, i.e. the weight of melted snow cover. However, it has been measured only in a few countries. The most often available record is only depth measurements. Several models have been suggested for transformation of the depth of snow cover into loads taking possibly into account also other climatological measurements as density, humidity, temperature, etc.

In order to harmonise the methodologies of measurements and their analysis and evaluations of snow loads for the design of structures across European countries, a research program was launched by an international project team; see the preliminary report of Del Corso et al. [1]. The works were completed issuing the Final Reports Sanpaolesi et al. [8]-[10]. Based on the reports, the European norm EN 1991-1-3 „General Actions - Snow loads" 2003 was elaborated. The European snow map does not include the newly integrated states.

In the present paper, the methodologies of collection and analysis of climatic measurements for the assessment of snow loads in [8]-[10] are discussed from the viewpoint of the regional climate and practice applied in Slovakia and former Czechoslovakia. Particularly, the influence of the heavy snowfalls in the winters 2004/2005 and 2005/2006 on the choice of an extreme value probability distribution and the assessment of characteristic values of snow loads is studied. The study employs database of yearly snow load maxima based on the weekly measurements of water equivalent of snow cover on 660 rain-gauge stations in Slovakia, which have been recorded during 52 years since the winter 1954/1955. Finally, probabilistic snow load models for reliability calculations of structures taking into account seasonal occurrence of snow cover are briefly outlined cf. [6].

Because of high time and spatial diversity of climate conditions, the assessment of snow loads on structures necessitates an integrated effort of structural engineers and climatological experts [2]-[4], [13].

2. Measurements and evaluations of the water equivalent of snow cover

Snow cover can significantly influence the processes, which are explored as a subject of interest by climatology, hydrology, biology and some other earth sciences. The changes of snow cover during the wintry season affect the runoff of atmospheric precipitation from river-basin (watershed). The snow cover effect on surface layer of atmosphere is well known. The presence of snow on the ground represents not only important water storage but also a protective layer of vegetation against strong frosts. Conditions of snow cover of involved region are considered for selection of its recreational utilization as well as for protection against avalanches.

Climatological observations of snow layer are mostly confined to measurements of the depth of accumulated snow cover. Measurements of water equivalent of snow cover, which is required for the assessment of snow loads on structures, are rather scarce. The water equivalent of snow cover, expressed in mm of melted snow cover or in kN/m2, is directly measured only in some countries as Germany, Finland, Switzerland, partially UK [8] and among the new member states of EU also in Czech Republic and Slovakia. For example, in Finland the water equivalents are recorded twice each month, and daily values are calculated by using daily precipitation and air temperature measurements, cf. [8].

In Slovakia weekly measurements are carried out, each Monday at the time of morning measurement at 7.00 a.m. within the whole snow cover profile (depth). In the late 1940s, during 1950s and in early 1960s water equivalent of snow cover measurements have been executed regularly at the beginning of each month decade, similarly at 7.00 a.m. in the morning. The measurements are practised in two ways; in the first case water equivalent of snow cover is carried out by means of rain-gauge and in the second one balance snow gauge is used.

The water equivalent of snow cover measurement by using the rain-gauge is similar to solid precipitation gauging. The captured water quantity from melted snow is gauged by measuring cup analogous to liquid precipitation gauging. Measurements are carried out at a place of uniform snow distribution with the same depth as at a snow-stake. This technique is often applied in the lowland regions of Slovakia, where the snow cover usually reaches low depth values.

In the mountain regions where the snow cover depth is evidently higher than in lowlands, the balance snow gauge is used. Its system functioning mechanism is based on non-uniform lever weights tenet. Within the Slovakian rain-gauge network, the balance snow gauge is being used since 1956. The sample weight is received in grams. The water equivalent of snow cover H is received in millimetres by the formula:

$$H = p/q, \qquad (1)$$

where p is the weight of sample in grams and q the cross-section area of snow gauge in square centimetres (50 cm^2).

Total rainfall, and mainly the form in which it falls out on the surface, significantly influences the water equivalent of snow cover. Higher precipitation totals and lower air temperature in higher situated regions and on the other hand, frequent snow cover duration discontinuances in lower situated locations cause significant differences in the water equivalent value of snow cover even within small regions.

Specific water equivalents of snow cover in regions with different altitudes are incomparable. As regards the density of snow cover, which is a relative quantity, similar values ought to be registered in larger as well as more broken regions. During the wintry season the snow cover density varies depending on duration, atmospheric conditions, snowfall period occurrence, etc. Its characteristics are affected by different physical changes within the layer.

Generally, solid precipitations increase the value of the water equivalent of snow cover. This is not the case for liquid precipitations. There have been observed significant increases of water equivalent of snow cover due to rainfalls. However, in some cases the water equivalent of snow cover remained almost unchanged or occasionally decreased after rainfall.

The above-mentioned changes of the water equivalent of snow cover depend likely on type and structure of snow in the layer, possibly also whether the soil under the layer is frozen or thawed. If the snow is dry and less thick or if the rain water doesn't have possibility to runoff, it will stay on in the snow layer. But if the snow is saturated by the rain water and this water has possibility to runoff to soil, the water equivalent of snow cover value may stay without change or diminishes during the liquid or mixed precipitation period.

The measurements of precipitations and of water equivalent of snow cover can be affected by some specific influences of surroundings of a meteorological station. Particularly, the solid precipitation gauging is biased by serious errors. Consequently, it holds generally that during the wintry seasons with sporadic occurrence of liquid and mixed precipitations the water equivalent of snow cover should be higher than weekly precipitation totals. We shouldn't forget about the wind affect, which is very important for snowdrift formations and of course makes the measurements of snow cover characteristics more difficult. Under ideal conditions, assuming that the precipitation gauging hadn't been biased by errors and evaporation, runoff, blowing away and blowing on or other snow cover changes, the curves representing cumulative precipitation totals and water equivalents of snow cover would have had a similar course in a graph figuration. Because of the non-ideal conditions in the nature, the differences between the above-mentioned curves are more or less obvious.

Because of the non-existence of a reliable physical model for conversion of snow depth empirical formulae are used. Then, the obtained daily values of snow load are used for the determination of the yearly maximum [1], [8]-[10]. Promising results offers the recently published formula of Němec et al. [4] employing daily measurements of: precipitation total, height of new snow cover, total height of snow cover and mean water vapour tension.

3. Characteristic values of snow loads and extreme value probability distributions

The definition of characteristic values of snow loads is based on probability analysis of annual maxima. The statistical distribution of these extreme values may be approximated by one of the extreme value distribution functions. Following the backgrounds to Eurocodes [1], [8], the characteristic value of snow load is defined by a probability of 0.02 of being exceeded within any one year. This corresponds to the so-called mean recurrence interval of 50 years. The characteristic value is thus expressed as the 98% fractal of the extreme value probability distribution of annual snow load maxima.

The up to date database of annual snow load maxima in Slovakia is based on weekly measurements of water equivalents of snow cover. It comprises data from the winter 1954/1955 to the winter 2005/2006 at 660 rain-gauge stations. For the selection of suitable extreme value distribution function, eight representative stations and four distribution functions, namely the gamma, Gumbel, Weibull for minima and lognormal distributions have been chosen [7].

The computational procedure using RCP software STATREL [5] included checks of probability papers (where available), estimation of distribution parameters: the method of moments, the maximum-likelihood optimiser method (ML-opt) and the least squares estimation; and distribution tests: the Kolmogorov-Smirnov test and the χ^2-test at the critical significance level of 0.05. More weight has been posed on the former test as being theoretically more satisfying. Visual tests of upper tails of empirical and theoretical distribution functions and tests for outliers were also included. The conclusion has been to apply the Gumbel distribution and the moment method for subsequent calculations.

Special issue investigated in [7], which will be further pursued in this section, is the study of how the heavy snowfalls in the last two winters 2004/2005 and 2005/2006 influenced the characteristic values calculated using annual maxima since the winter 1954/1955. The differences obtained by deducting the value corresponding to the shorter period of 50 years from the other one of 52 years have shown in a number of stations significant increases of characteristic values. Specifically, at 415 stations the differences were negligible – between -0.05 to +0.05 kN/m^2, at 110 stations the observed interval was 0.05 to 0.1 kN/m^2, at 101 stations 0.1 to 0.2 kN/m^2, at 25 stations 0.2 to 0.3 kN/m^2 and at 9 stations the values ranged from 0.3 to 0.56 kN/m^2.

In this paper we focus on the data of two stations from the class of top differences. At Oravská Lesná station, which is one of the eight representative stations, the characteristic value increased by 0.34 kN/m^2 and the slope of regression line changed from negative to positive, see *Figures 1* and *Figure 2*. Despite of this, the test results gave very high scores of significance levels, confer *Table 1*. However, visual check of *Figure 2* suggests a gradual increase of maxima, not obeying the form of a "steady state" process assumed in statistical evaluations of snow load data [8].

For the data at Handlová-Nová Lehota station, the highest increase of the characteristic values, being of 0.56 kN/m^2, has been found. Visual check of *Figures 3* and *Figure 4* and low significance levels of tests, see *Table 2*, show that the highest annual maximum of 3.72 kN/m2 attained in winter 2005/2006 does not fit the rest of the record. For the gamma and Gumbel distributions, using the maximum-likelihood optimiser method for parameter estimation, it has been detected as an outlier.

An exceptional snow load value has been defined in [8] as: "If the ratio of the largest value to the characteristic load determined without the inclusion of that value is greater than 1.5 then the largest load value shall be treated as an exceptional value". Such snow load values should be considered in design separately as accidental actions [8]. Thus, the characteristic values should be assessed without the exceptional snow load. Plot of 51 annual maxima and the corresponding regression line is in *Figure 5*. The results of distribution tests including the characteristic values are in *Table 3*. One can check that the ratio of the exceptional load 3.72 kN/m^2 to the majority of characteristic values from *Table 3* is about 2.

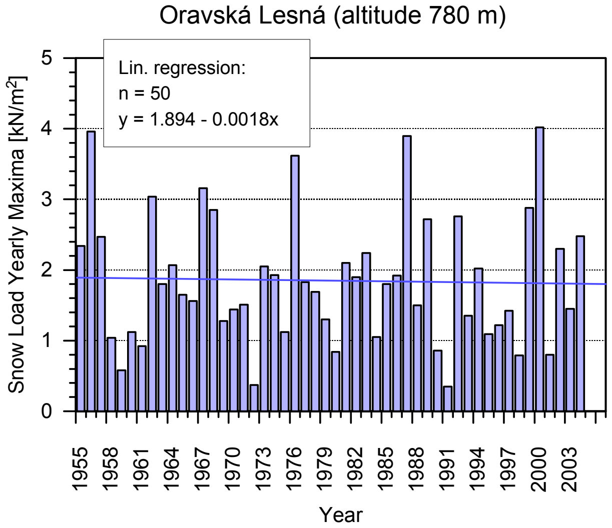


Figure 1. Snow load yearly maxima at Oravská Lesná station, 50 years period

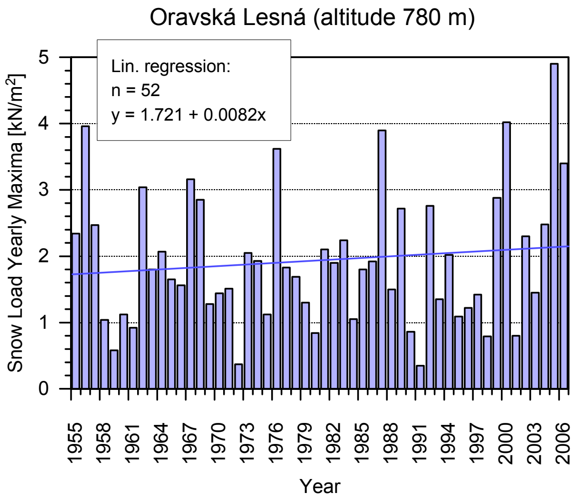


Figure 2. Snow load yearly maxima at Oravská Lesná station, 52 years period

Table 1. Test results at Oravská Lesná station (alt. 780 m), 52 years period

Probab.	Params	Kolmog.-	Chi-	Char. val.

distrib.	estimate	Smirnov	square	98%
Gamma	Moments	0.99997	0.904	4.53
	ML-opt	0.99997	0.904	4.55
Gumbel	**Moments**	**0.99996**	**0.974**	**4.57**
	ML-opt	0.99996	0.974	4.55
	Least sqs	0.997	0.974	4.84
Weibul min	ML-opt	0.997	0.857	4.42
Log-normal	Moments	0.995	0.904	4.71
	ML-opt	0.967	0.860	5.38
	Least sqs	0.974	0.813	5.93

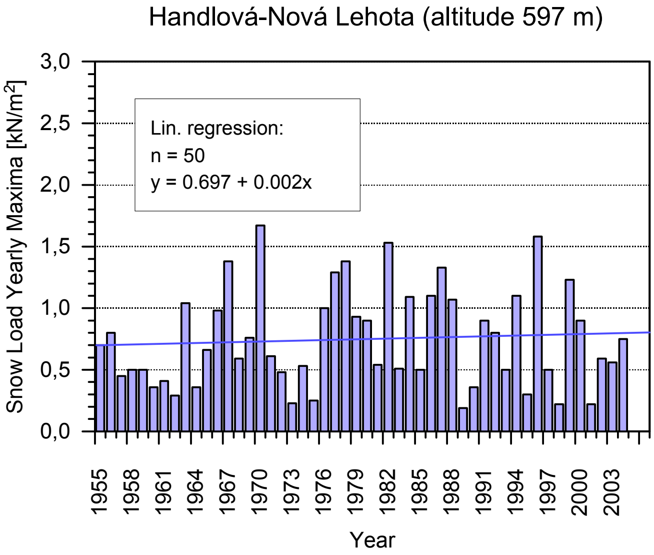


Figure 3. Snow load yearly maxima at Handlová-Nová Lehota station, 50 years period

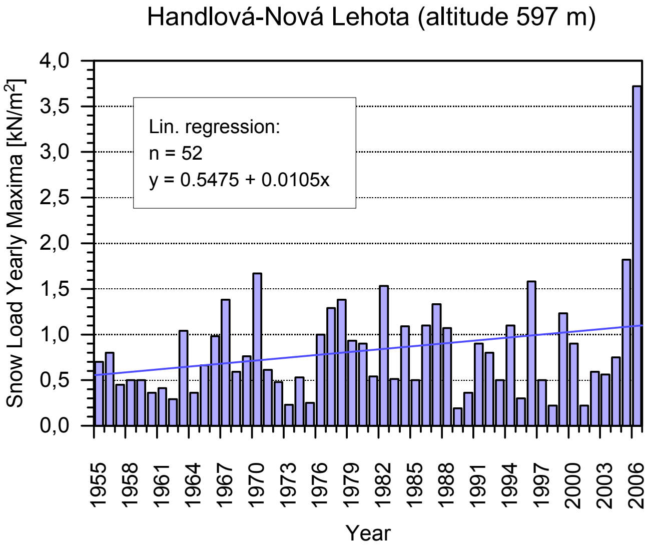


Figure 4. Snow load yearly maxima at Handlová-Nová Lehota station, 52 years period

Table 2. Test results at Handlová-Nová Lehota station (alt. 597 m), 52 years period

Probab. distrib.	Params estimate	Kolmog.-Smirnov	Chi-square	Char. val. 98%
Gamma	Moments	0.767	0.100	2.41
	ML-opt^{1*}	0.837	0.444	2.15
Gumbel	**Moments**	**0.641**	**0.170**	**2.34**
	ML-opt^{1*}	0.660	0.338	2.01
	Least sqs	0.205	<0.05!	2.61
Weibul min	ML-opt	0.741	0.166	2.41
	Least sqs	0.100	<0.05!	5.36
Log-normal	Moments	0.906	0.188	2.49
	ML-opt	0.911	0.230	2.45
	Least sqs	0.935	0.138	2.71

1* in index position denotes detection of one outlier

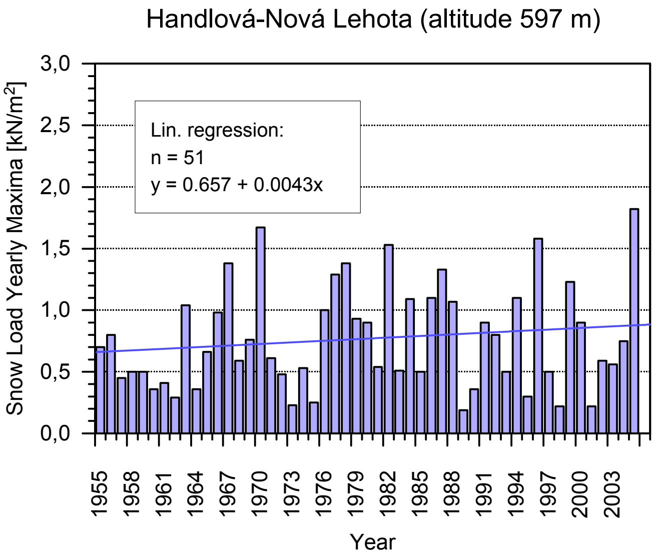


Figure 5. Snow load yearly maxima at Handlová-Nová Lehota station, 51 years period

Table 3. Test results at Handlová-Nová Lehota station (alt. 597 m), 51 years period

Probab. distrib.	Params estimate	Kolmog.-Smirnov	Chi-square	Char. val. 98%
Gamma	Moments	0.895	0.248	1.85
	ML-opt	0.905	0.248	1.86
Gumbel	**Moments**	**0.781**	**0.522**	**1.86**
	ML-opt	0.831	0.401	1.85
	Least sqs	0.865	0.274	1.98
Weibul min	Least sqs	0.083	<0.05!	5.08
Log-normal	Moments	0.625	0.248	1.93
	ML-opt	0.719	0.148	2.18
	Least sqs	0.871	0.615	2.40

Figures 6 to *8* illustrate importance of parallel visual checks of upper tails of theoretical (here lognormal) and empirical distribution functions. The best test results, *see Table 3*, are obtained for parameter estimation by the least squares method, however, the worst tail approximation accounts for an unrealistically high characteristic value of snow load. Generally, the application of the least squares method leads to higher characteristic snow loads [7], [8].

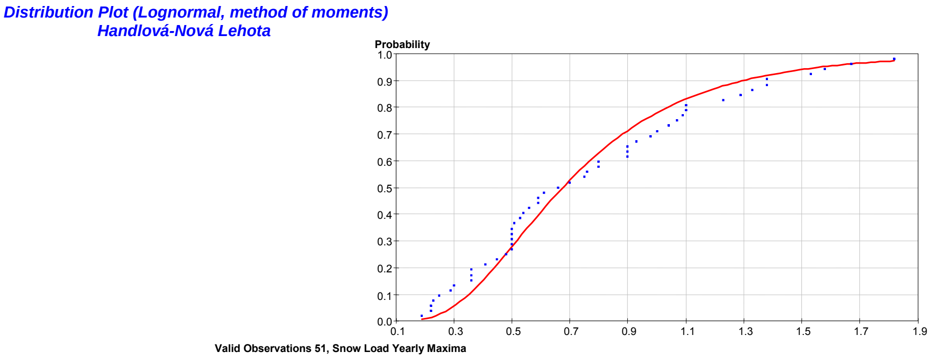


Figure 6. Lognormal distribution of snow load yearly maxima at Handlová-Nová Lehota station, method of moments, 51 years period

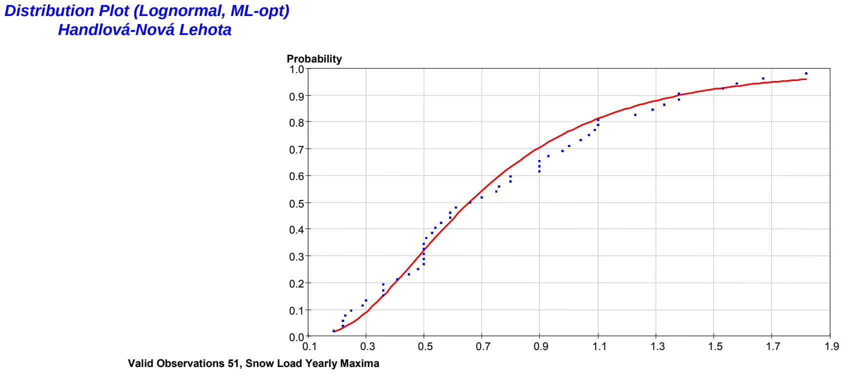


Figure 7. Lognormal distribution of snow load yearly maxima at Handlová-Nová Lehota station, Maximum-Likelihood optimiser, 51 years period

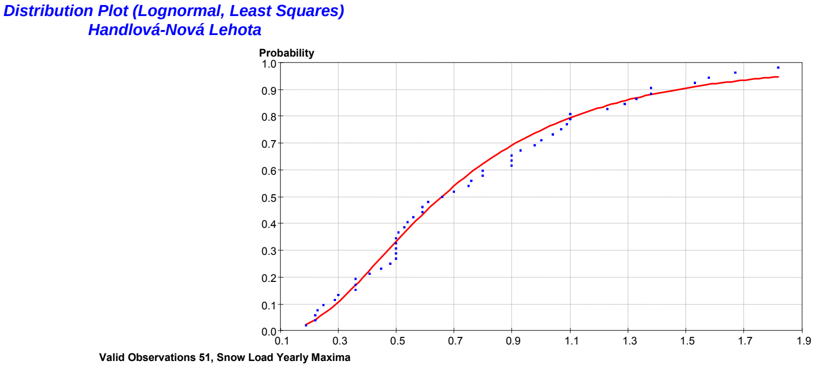


Figure 8. Lognormal distribution of snow load yearly maxima at Handlová-Nová Lehota station, least squares, 51 years period

4. Snow load models for reliability calculations

An exact description of snow loads can be obtained using time-dependent processes. Less involved options are the event-based maxima approach and annual maxima approach [8]. The former can be used in climates, where snowfalls occur as discrete events and between the events the snow cover completely melts, e.g. in Denmark [8]. In continental climates with continuous and longer lying periods of snow cover and resulting snow layer accumulation in wintry season the latter approach applies.

In majority of European countries the characteristic values of snow load are assessed by the probability distribution function of annual snow load maxima. As a rule the Gumbel distribution is applied:

$$F_1(x) = \exp\{-\exp[-\frac{\pi}{\sigma\sqrt{6}}(x-\mu)-\gamma]\} \tag{2}$$

where μ and σ denote the mean value and standard deviation of the yearly maxima. For a probabilistic analysis of structures in a lifetime of n years, the adjusted distribution function $F_n(x)$ can be used:

$$F_n(x) = F_1(x)^n. \tag{3}$$

However, the distribution function (2) or (3) does not take into account the seasonal occurrence of snow cover. In paper [11], the intermittent occurrence of snow cover has been considered for a probabilistic design of industrial buildings. This idea has been further applied to calibrations of safety factors by probabilistic optimisation, cf. [6].

Denoting by p_{snow} the expected relative frequency of snow presence in a year, the yearly mixed distribution is obtained as [6]

$$F_{1,mix}(x) = (1-p_{snow})\mathbf{1}_{0\le x} + p_{snow}F_1(x), \tag{4}$$

while for the lifetime of n years it is

$$F_{n,mix}(x) = (1-p_{snow})\mathbf{1}_{0\le x} + p_{snow}F_1(x)^n. \tag{5}$$

The distribution functions (4 and 5) are less severe than those given by equations (2 and 3). Despite of this, the optimisation of safety factors for industrial buildings considering seasonal occurrence of snow cover by (4 and 5) led to partial factor for snow of 2 [6], in contrast to the standardised value of 1.5. The use of distribution functions (2 and 3) would yield even higher snow factor, which may imply an unnecessarily cost increase if applied.

5. Conclusion

The long-term practice in collection of climatological measurements in Slovakia shows up their good standard and suitability for the assessment of snow loads on structures.

The analysis of the influence of heavy snowfalls in the winters 2004/2005 and 2005/2006 on the characteristic values calculated using annual maxima since the winter 1954/1955 led to detection of an exceptional snow load in the sense of [8], which has to be treated separately within an accidental design case.

For the reliability studies of structures in continental climates a probabilistic snow model with mixed distribution function taking into account the seasonal occurrence of snow cover together with the distribution function of annual maxima is recommended. Of course, the characteristic snow loads result from the in European countries harmonised methodology based on an extreme value distribution function of annual maxima derived without the seasonal issue.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-51-024505.

References

[1] Del Corso, R. et al. (1995). New European Code for Snow Loads. Background document. *Proc. Dept. Structural Engng Univ. Pisa,* No.264, Pisa, 76p.

[2] Faško, P. & Lapin, M. (1996). Snow cover and precipitation changes in Slovakia in the 1921 – 1995 period. *Proceedings on the 24 th ICAM 96.* HMI of Slovenia, Bled, 259 – 266.

[3] Handžák, Š., Faško, P. & Nejedlík, P. (2000). Selected snow cover characteristics change during the period 1921 – 2000 in Slovakia. CD, ICAM 2000, Innsbruck, Session 6.

[4] Němec, L., Květoň, V., Setničková, I. & Škáchová, H. (2003). Estimation of the Water Equivalent of Snow Cover from the Other Meteorological Instruments, *ICAM Conference, Brig,* www.map2.ethz.ch/icam2003.

[5] Consult, (2003). RCP Reliability Consulting Programs: STRUREL: A Structural Reliability Analysis Program System, STATREL User´s Manual: Statistical Analysis of Data for Reliability Applications, München. RCP

[6] Sadovský, Z. (2006). Climatic loads and reliability of light roof industrial buildings. In C. Guedes Soares & E. Zio (eds.), *Safety and Reliability for Managing Risk*; *Proc ESREL 2006,* (vol. 2, 1535-1539). London: Taylor & Francis.

[7] Sadovský, Z., Bochníček, O., Faško, P., Mikolová, K. & Šťastný, P. (accepted for ESREL 2007). Revision of snow load data for structural design in Slovakia.

[8] Sanpaolesi, L. et al. (1998). *Phase 1 Final Report to the European Commission, Scientific Support Activity in the Field of Structural Stability of Civil Engineering Works: Snow Loads*. Department of Structural Engineering, University of Pisa, 170p.

[9] Sanpaolesi, L. et al. (1999)^{a}. *Phase 2 Final Report to the European Commission, Scientific Support Activity in the Field of Structural Stability of Civil Engineering Works: Snow Loads*. Department of Structural Engineering, University of Pisa, 341p.

[10] Sanpaolesi, L. et al. (1999)^{b}. *Annex B to the Final Report - European Ground Snow Loads Map.* Department of Structural Engineering, University of Pisa, 41p.

[11] Schleich, J.B., Sedlacek, G. & Kraus, O. (2002). Realistic Safety Approach for Steel Structures. *Proc. 3th European Conference on Steel and Composite Structures.* Eurosteel, Coimbra, 1521-1530.

[12] Tichý, M. et al. (1987). *Loads on Structures* (Zatížení stavebních konstrukcí – in Czech). TP 45, SNTL, Praha, 466p.

[13] Vojtek, M., Faško, P. & Šťastný, P. (2003). Some selected snow climate trends in Slovakia with respect to altitude. *Acta Met. Univ*. Comenianae, Vol. XXXII, 17-27.

POSSIBILITIES OF TRAFFIC ACCIDENTS AND RISK CRASH EVALUATION

Stodola Jiri

University of Defense, Faculty of Military Technology, Brno, Czech Republic

Keywords

traffic accident, risk factor, road traffic safety, traffic accident consequence, road traffic risk and safety evaluation

Abstract

This article analyses the traffic accident rate on roads and highways and possibilities of risk evaluation related to traffic accident occurrence based on factors that were the causes of accidents. A new term – risk of traffic accident occurrence is a product of probability of accident occurrence and its impacts. The results are presented by way of example that uses selected statistical data of the Czech Republic traffic accident rate between 1993 - 2001. The article provides a brief methodological procedure of evaluation of the traffic accident rate using the risk of traffic accident occurrence.

1. Introduction

Recently, the safety of road traffic has become a very serious problem for nearly all countries. A growing density of the traffic causes an increasing amount of accidents associated with heavy losses of property and injuries or fatalities. That is way national and international authorities pay an exceptional attention to this problem and try to mitigate the negative trends in the time development of safety of road traffic, for example by modifications of traffic regulations. To be rational and effective, the measures taken by the authorities have to result from a detailed analysis of the causes of accidents. For these reason usually the authorities in the developed countries maintain the national accident databases that gather the information on the consequences of each road accident.

2. Traffic accident statistics

Data from accident databases enable to carry out the required analyses and establish the trends of the traffic safety. An analysis of time development of absolute or relative number of accidents and their consequences is the most common way of evaluation of the trends of the traffic safety. The time development of number of accidents with a certain cause or number of injuries, fatalities and amount of property damages associated with this certain kind of accident is beyond any despite useful indicator of development of safety, but sometimes the results of the above-mentioned analysis can be quite controversial. A certain weakness of this system is the fact that it employs absolute numbers that prevent comparison between the individual periods of month/day/year, causes, etc., and inaccuracy due to changes resulting from individual data changes. Substantial disadvantage of this system consists in a non-existence of a measure of severity, or acceptability of the traffic accident impacts. That is why it is not possible to determine whether the traffic accident is or is not socially acceptable, or, it is at least satisfactory.

3. Risk, and degree of risk

The given evaluation obviously lacks a common feature of risk level that consists in:

- Simultaneous consideration of features (risk factors) of each traffic accident,
- Probability of a certain traffic accident occurrence,
- Appropriate expression (evaluation) of traffic accident consequences,
- etc.

It is evident that there exists a more complex evaluation using the institute of risk *R* in the following form:

$$\mathbf{R} = \mathbf{P} \times \mathbf{C}\,,$$

where **R** - risk of traffic accident,
P - probability of traffic accident occurrence,
C - consequence of traffic accident.

A risk defined in this way is a non-dimensional parameter and it provides mutual comparison of various groups of causes of traffic accidents, their characteristics and it also enables mutual comparison of individual types of traffic accidents. To enumerate the risk of traffic accident according to this equation it is necessary to quantify probability of accident occurrence P and consequences of traffic accident C. Possibilities of that are presented in paragraph 4 and 5.

The second way in which it is possible to evaluate risks associated with traffic accident is usage of rate of accidents that represent probability of accident per one kilometer with respect to fatalities, severe injuries, and slight injuries. In the case of evaluation of damage caused by accident it is suitable to use co called specific damage that represents average damage per one kilometer. Equations for rate of accident and specific damage enumeration are presented below:

rate of accidents

$$\mathbf{R_A} = \frac{N_\Sigma}{D_C}\,,$$

rate of fatalities

$$\mathbf{R_F} = \frac{N_F}{D_C}\,,$$

rate of severe injuries

$$\mathbf{R_{SEI}} = \frac{N_{IS}}{D_C}\,,$$

rate of slight injuries

$$\mathbf{R_{SLI}} = \frac{N_{ISL}}{D_C}\,,$$

specific damage

$$\mathbf{R_D} = \frac{N_D}{D_C}\,,$$

where D_C – a distance covered in the Czech Republic in calendar year,
N_F – *a* number of fatalities in calendar year,
N_{IS} – a number of severely injured people in calendar year,
N_{ISL} – a number of slightly injured people in calendar year,
N_D – a sum of damages.

Next possibility of risk evaluation is usage of so called degree of risk D_R that can be expressed by the following equation:

$$\boldsymbol{D_R} = \frac{C_{Ai} N_\Sigma}{C_{A\Sigma} N_i},$$

where C_{Ai} – a number of consequences by given cause of accident,
$C_{A\Sigma}$ – a number of consequences by all accidents,
N_Σ – a number of all accidents,
N_i – a number of accidents by given cause of accident.

Degree of risk D_R indicates how many times the given cause of accident is more risky than statistically significant average cause of an accident.

4. Probability of traffic accident occurrence

Probability of traffic accident occurrence encompasses a complete system of phenomena and, using a classical definition, equals to the probability share of frequency of specific type of traffic accident and total amount of traffic accidents in the period under survey. Probability of traffic accident P can be expressed in the following equation:

$$\boldsymbol{P} = \frac{N_i}{N_\Sigma},$$

where N_i – a number of accidents of evaluated i-th type in calendar year,
N_Σ – a total number of accidents in calendar year.

To determine this probability we can use sufficient credible data in the statistics of the traffic accident rate. Classical probability defined in this way shall be valid exactly in two-status model and its constraints rest in a necessity or assumption of similar possibilities of occurrence of random events – e.g. types of traffic accident. In practice, it may often happen that random event– type of traffic accident is not definite and may not happen anyway. There are possibilities of more generally approach to a probability, in practice - an axiomatic, or, in our case - statistic approaches are used.

5. Impact of traffic accident

The impact can be considered a measure of the traffic accident severity. It is a significant part of magnitude of risk. Here exists a general inversion principle based on the fact that an accident with a high level of probability of occurrence, but with non-serious impacts has also a low level of risk rate. And vice versa, an accident even very improbable but with serious impacts is considered as highly risky. To date, no transport standards provide a unique method of evaluation of the impacts of traffic accidents. In general, the impact of traffic accident can be established using three methods:

1) Use of expert methods when a severity level can be attributed to each accident as a relative value of accident impact with a meaning of weight, e.g., within the range of values from the interval: $0 \le C \le 1$, with possible interpretation: with no impacts $C\,min \to 0$, catastrophic impacts $C\,max \to 1$.
2) Use of international standards when severity of single categories of accidents is established by a scale - Minor, Major, Critical, Catastrophic, with exact definition of severity of individual categories. In some domains (e.g. aviation, etc.) for each category there exists a maximum value of socially acceptable probability of accident occurrence.
3) Expressed impact is a tool with similar meaning as probability; to assess the impact of traffic accident it is possible to use a probability when the traffic accident impact is expressed, for example, by the number of persons killed at the type of traffic accident examined against the total number of persons killed in all accidents in the period under survey. Thus, a severity of a given type of traffic accident if „weighted" relative to other accidents by the weight of number of persons killed, or by other „weight",

e.g., a property damage as a proportion of the magnitude of resulting property damage of the participants of the accident at the type of traffic accident relative to the total property damage of the participants of all traffic accidents in the period under survey.

6. Example of application

Resulting from statistical data the rate of accident, fatalities, severe and slight injuries, specific damages, and degree of risk were evaluated. From results presented it is evident that the most risky factors in the Czech Republic are as follows:

- hitting the oncoming vehicle during overtaking,
- riding a motorcycle,
- pedestrian on the road,
- excessive speed.

Resulting from the analysis there can be stated that are the following most hazardous factors: wrong overtaking, higher than permissible driving speed, riding a motorcycle, and pedestrian behavior. Analyses showed that low level of alcohol in blood does not significantly increase the traffic accident risk. *Figure 1* show forecast of number of fatalities in the course of accidents per one million inhabitants and compare the Czech Republic and Great Britain, the Netherlands and Sweden.

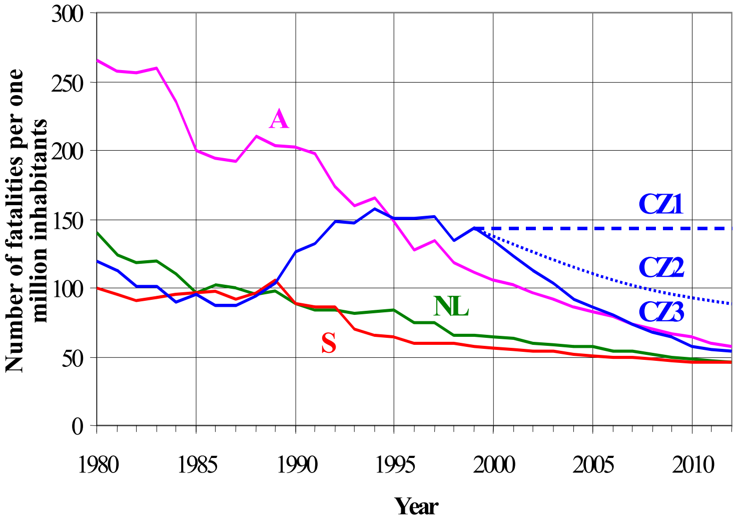


Figure 1. Forecast of number fatalities in the course of accidents per one million inhabitans

where A- Great Britain,
NL - the Netherlands,
S - Sweden,
CZ1 - zero variant is the extrapolation of accinent frequency development as in progress in the last five years,
CZ3 - desirable variant, i.e. the accident level in the Czech Republic striving for the situation in the development EU countries in the real-time horizon,
CZ2 - hypothetical variant expresses the compromise between two above mentioned variants.

7. Conclusion

The Police of the Czech Republic maintain annual detailed statistics of the traffic accidents in the form of summary numbers and figure surveys divided by various criteria. This system provides important information that may serve as the grounds for creation of new and effective preventive measures. However, this information system does not use the institute of risk in the road traffic. And at the same time it is evident that trends in development of risk provide relatively objective and complex information to solve these traffic accidents as serious all-society phenomena. It refers mainly to the causes and consequences of traffic accidents and influence of various factors that determine the traffic accident this information system does not use the institute of risk in the road traffic. And at the same time it is evident that trends in development of risk provide relatively objective and complex information to solve these traffic accidents as serious all-society phenomena. It refers mainly to the causes and consequences of traffic accidents and influence of various factors that determine the traffic accident rate.

Described methodology defines selected terms as objective tools for the systems analysis of causes and impacts of the traffic accidents. Risk of traffic accident rate is a non-dimensional parameter that can enable comparison of various effects and circumstances otherwise incommensurable. The advantage is that we can use existing statistical surveys and alternatively evaluate the safety of the road traffic. A certain disadvantage is the fact that in road traffic field there are no generally binding criteria of social or individual acceptability of the magnitude of risk related to the traffic accident. That is why the information system of the traffic accident rate cannot be used to establish whether the Czech Republic traffic accident rate is at an acceptable level, or whether it is necessary to reduce it.

References

[1] Chudoba, J. (2002). *Determining of Probability of Car Accident by Conveyance of Car*. Project. University of Liberec.

[2] Czech Traffic Police Force. (1993-2002). Statistics of the Traffic Accident Rate in the CR, Set of Documents from 1993 to 2002.1, 1, Ministry of Interior, Praha.

[3] Furch, J. (2006). Processing Preventive Maintenance Programme. Magazine *Machine building and Electrical Engineering.* Sofia, ISBN 0025-455X.

[4] Hajek, M. (2003). *Solution of problems verbal communication between participants of road traffic by risk situations in traffic*. Technical university Ostrava.

[5] Rosicka, Z. (2005). Safety and Adaptability – Multinational Rescue Team Challenge and Goal. *Glasnik ZRS Koper*, č. 4, s. 197-198. ISSN 1318-9131.

[6] Stodola, J. (1982). Safety of Traffic of Motor Vehicles. *Military Technical Magazine*. Nr 6. Praha.

[7] Stodola, J. (1987). For Active Safety of Automobiles. *Military Technical Magazine*. Nr 4. Praha.

[8] Stodola, J. (2004). Risk of Traffic Accident and Possibilities of its Evaluation. Žilina, 127 – 130, ISBN 80-8070-121-0.

[9] Stodola, J., VINTR, Z. (2004). Traffic Accident Information System and Possibilities of Risk Crash Evaluation. *Book of Abstracts of World Automotive Congress FISITA. STA Barcelona Depósito legal*. B-26597-04.

[10] Stodola, J. (2006). Traffic Accident Information System and Risk Crash Evaluation. *International Scientific School: Modeling and analysis of Safety and Risk in Complex System.* Saint-Petersburg. Russia, ISBN 5-8088-0181-8.

[11] Vintr, Z., HOLUB, R. & VALA, M. (2002). A Risk-based Evaluation of Safety Development in Road Traffic. In: Probabilistic Safety Assessment and Management (PSAM 6). *Proceedings of 6th International Conference on Probabilistic Safety Assessment and Management.* Oxford: Elsevier Science, p 493 – 498, ISBN 0-08-044122-X.

ADOPTED ISOCHRONES METHOD IMPROVING SHIP SAFETY IN WEATHER ROUTING WITH EVOLUTIONARY APPROACH

Szłapczyńska Joanna, Śmierzchalski Roman

Maritime University, Gdynia, Poland

Keywords
weather routing, isochrones method

Abstract
The paper is focused on adaptation of an isochrones method necessary for application to a weather routing system with evolutionary approach. Authors propose an adaptation of the isochrones method with area partitioning assuring that the route found by the adopted method would not cross land. In result, when applied to a weather routing system with evolutionary approach, this proposal facilitates creation of initial population, resulting with routes of reduced collision risk and low costs of passage.

1. Introduction

Weather routing services play important role in securing ship safety, especially when ocean-going ships are considered. During such voyages adverse weather conditions may impact not only the passage time, a crucial resource nowadays, but also security of people and commodities on board. Most of recent scientific researches focus on shortening the passage time and avoiding severe weather i.e. tropical cyclones. Though these actions have significantly amended the security level, still more improvements increasing ship safety might be proposed.

One of the first approaches to minimum time route planning based on weather forecasted data was an isochrone method proposed by R.W. James in 1957 [3]. The method, where recursively defined time-fronts are geometrically determined, was in wide use through decades. In late seventies based on the original isochrone method the first computer-aided weather routing tools were developed. However, along with computer implementation a problem arose with so called "isochrone loops". Numerous improvements to the method were proposed since early eighties, with [2], [6], [7] among others.

Evolutionary approach as a natural successor of genetic one has become popular in the last two decades and has been successfully applied to anti-collision manoeuvre modelling [5]. Modern weather routing tools also utilize evolutionary algorithms instead of the deprecated isochrone time-fronts. Yet isochrones can still be utilized for generating initial populations. In such cases special attention must be given to assure that the route found by the isochrone method does not cross any landmasses. Otherwise, land crossings in first evolutionary population may result at least in extended, time-consuming computations or ultimately – in determining a hazardous route. Thus, it is extremely important to adapt the isochrone method in such a way that its resulting route would obey the "no land crossing" rule.

This paper is organized as follows: section 2 introduces classic isochrone algorithms with their advantages and disadvantages referring to computer implementation in evolutionary application. Section 3 presents a possible solution of collision risk reduction in route planning process. Section 4 provides detailed description of a proposal concerning adaptation of the isochrone method with area partitioning. Then in section 5 an example of usage is presented. Finally, section 6 summarizes the material presented.

2. Classic isochrone algorithms

2.1. Original isochrone method

The isochrone method was originally proposed by R.W. James in 1957 [3]. The method was intended for manual use by navigators as an aid for route planning process. An isochrone introduced by James is a set of connected points that a ship can reach within given time limit starting from one point and going in all possible directions. These points are dependent among other things on weather factors such as wave direction and height. Given this definition the first isochrone visualizes ship's speed characteristic. Then, in order to determine second isochrone, from each point belonging to the first one a perpendicular line to tangent is determined (*Figure 1*). A segment of the line depicting distance that the ship is able to cover within next time limit defines a point on second isochrone. A set of such connected points forms second isochrone. Next isochrones are generated identically.

Main disadvantage of the method when implemented as a part of computer application are so called „isochrone loops" [7]. Such a loop is in fact an irregularity in shape of an isochrone caused by non-convexity of speed characteristic for given weather data. Unfortunately isochrone loops propagate with number of isochrones and as a result make the procedure not applicable for computer programs.

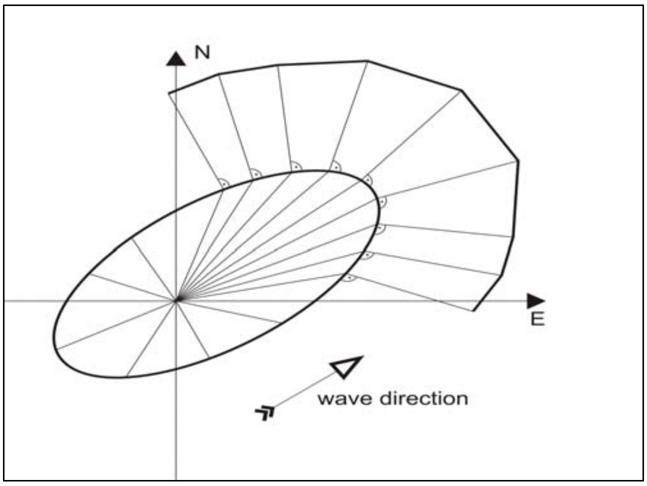


Figure 1. Construction of the first and second isochrone

2.2. Modified isochrone method

Modified isochrone method, presented in [7], removes the main disadvantage of original James' method. The modified method is based on an observation that for a given point on an isochrone the perpendicular to the isochrone is not always the optimal direction. Instead, a course change is required such that its projection on the perpendicular to the tangent is maximized. Not only does this solution remove "isochrone loops" problem, but also is applicable to computer application. However, some problems occur when strict rule of no land crossing should be met. According to the description given by [7], in order to allow the method bypass landmasses it is sufficient to inscribe zero ship velocity with ship's speed characteristic for land points. However, when applied some isochrone points appear to be stuck at landmass shore (*Figure 2*). This behaviour is caused by the fact that when a point of an isochrone is a landmass (e.g. due to not sufficient resolution of weather data) it does not allow creating any new point for next isochrones. In addition to that, inscribing zero velocity for landmass points together with low-resolution weather data may cause isochrone route to cross the land regardless of all other protections.

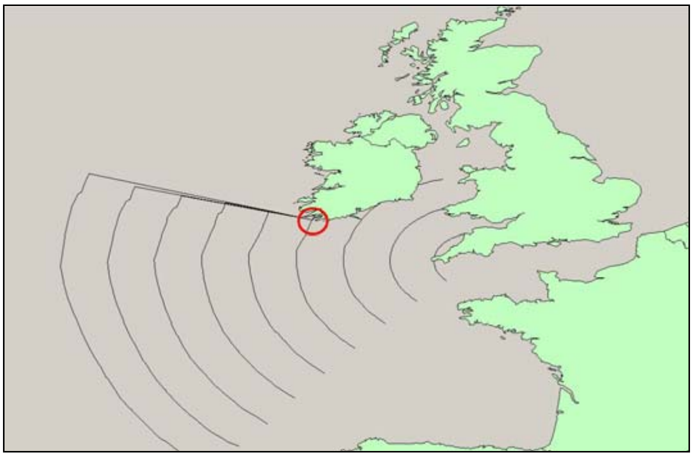


Figure 2. Example set of isochrones with a point being stuck at landmass

Last but not least, this method is prone to failure in situation when a ship is about to cross a narrow strait. A reason behind that is that only a single point can be generated from a point on the current isochrone. Thus, if only one point, assuming sufficient isochrone accuracy, is put inside the strait, hardly can it browse the area around.

2.3. Modified isochrone method with area partitioning

Another modified isochrone method was proposed by H. Hagiwara in 1989 [2]. The method with area partitioning assumes that when a new isochrone is to be generated first the search sector's area is partitioned. After a set of calculations the set of sub-areas produce a set of points constructing the new isochrone. For each sub-area sector only one point can be selected, the one having maximum distance from the starting point. Graphical representation of the method is often different than other classic isochrone methods. Here all isochrone points are drawn and, instead of connecting every point from one isochrone like in other isochrone methods, they are connected in such a way that a point is connected with his predecessor and all successors (*Figure 3*).

Due to area partitioning this algorithm is less non-convexity-error prone. It is also more flexible than the previously described method. The method can easily handle narrow strait crossings as well as other crossings. Hagiwara [2] provides only general solution for assuring no land crossings though, giving universal formula for method restrictions including land obstacles. Thus, detailed solutions for "no land crossing" rule should be introduced to the method.

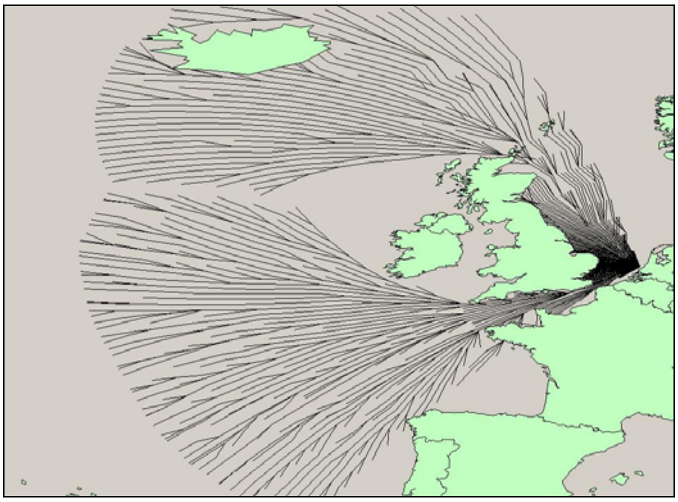


Figure 3. Graphical representation of the modified isochrone method with area partitioning

3. Reducing collision risk in route planning process

Modern weather routing services focus primarily on achieving low costs of passage by means of either minimization of passage time or reducing transport costs i.e. fuel consumption. Hardly is there any collision risk factor taken into account among the safety criteria in a multicriteria route planning process. It is mostly because collision risk often conflicts with economic criteria. Instead, a trade-off between safety and economic criteria are to be sought. Thus, the authors propose to introduce into the weather routing optimisation procedure another safety criterion, namely traffic intensity factor. When a Pareto-based multiobjective evolutionary algorithm is the main optimisation engine, it is guaranteed that the route found should not cross any high traffic intensity area. In result, the risk of potential collision with other vessels would be significantly reduced. In order to achieve the goal of reducing collision risk while preserving possibly low costs of passage a proper set of initial routes, constituting the initial population, should be determined. These routes must obey all the navigational constraints, particularly the “no land crossing” rule. Thus, an algorithm is required specifying how to determine such routes.

4. Proposed adaptation of isochrone method

As a base for adaptation the modified isochrone method with area partitioning was selected due to it’s flexibility and good browsing capabilities e.g. in narrow straits. A focus of research was provided to introduce mechanisms assuring that the final route is free from land crossings.
In order to prevent selecting a route crossing land obstacles following restrictions should be imposed:

1. Neither start nor finish point of the route may lay at landmasses.
2. On creation of a new isochrone candidate point it must be checked whether a line between the point and his predecessor does not cross land (bitmap-based algorithm).
3. If the point in 2. crosses land another candidate point must be found. The new point must not violate ship’s speed characteristic or cause land crossing.
4. When selecting the last isochrone point leading directly toward the finish point it must be checked whether land is not crossed (again bitmap-based algorithm).

Next subsections describe in detail the bitmap-based algorithm required to perform steps 2 and 4 as well as the process of new candidate point generation (step 3).

4.1. Bitmap-based algorithm for checking a line for intersection with land area

Let us assume we have a vector-based land map in latitude-longitude projection. The land is defined by a set of polygons (in general they do not have to be convex), with their vertices described by pairs of geographical coordinates: longitude and latitude. Unfortunately, there is no sufficiently fast and robust algorithm that checks a line (defined by start and finish points) for intersection with any polygon, especially non-convex one [1]. Here, for purposes of the isochrone method, complexity of algorithm for checking a line for intersection with land area must remain as low as possible. On the other hand there are some effective algorithms for checking a point inclusion in any polygon, also non-convex one [1].

Having analysed these facts an algorithm may be proposed that performs checking a line for intersection with land area in a twofold way. First a high-resolution bitmap is created covering the entire map. Every bitmap cell holds a boolean “True” or “False” value depending whether land covers entire cell. Due to time consuming process of bitmap creation it is sufficient to be performed once only and its results to be stored in an outer file for future utilization. To keep the file compact it is recommended to store only the boolean values in predefined order of bitmap cells. Once the bitmap is available, algorithm presented below (Figure 4) is able to perform the final check.

The presented algorithm keeps linear computational complexity O(n) ([4]), where n denotes the number of cells. Since the access to the land bitmap is done in constant time (O(1)) it does not affect total complexity of the procedure.

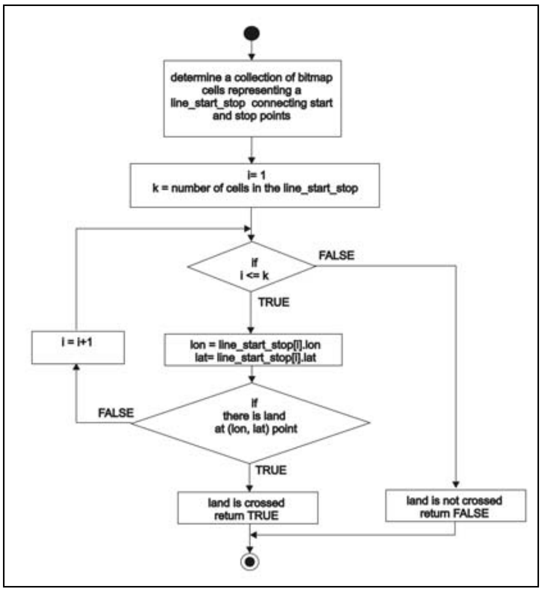

determine a collection of bitmap cells representing a line_start_stop connecting start and stop points
i= 1
k = number of cells in the line_start_stop
if
i <= k
FALSE
TRUE
i = i+1
lon = line_start_stop[i].lon
lat= line_start_stop[i].lat
FALSE
if
there is land
at (lon, lat) point
TRUE
land is crossed
return TRUE
land is not crossed
return FALSE

Figure 4. Bitmap-based algorithm for checking if a line crosses land

Land bitmap resolution is another important issue having impact on calculation accuracy. It is recommended to generate a bitmap with cell size at most equal to the smallest observable map object. Otherwise there is a risk of inaccurate computation due to rough land bitmap data.

4.2. Generation of a new candidate point assuring no land crossings

To generate a new point that does not violate ship's speed characteristic nor crosses land it is necessary to utilize previously described bitmap-based algorithm. Let us assume we have points A and B, where A is a predecessor of B, B was found as a border point of ship's speed characteristic and segment A-B does cross land. Another point C on the A-B segment is sought such that A-C segment does not cross land. In addition to that the C point should maximize the length of the A-C segment. An algorithm presented below finds proper C point for the input parameters: points A and B, distance step and land bitmap.

In the algorithm below (*Figure 5*) a C point is searched such that, starting from A towards B, new points are generated with distance of distance step between them. The first one that causes land crossing breaks the loop. In this moment the previous point (the one that does not cause land crossing) is returned as the C point.

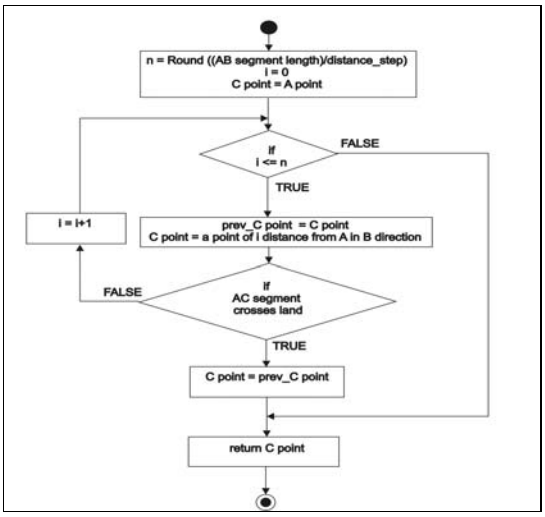


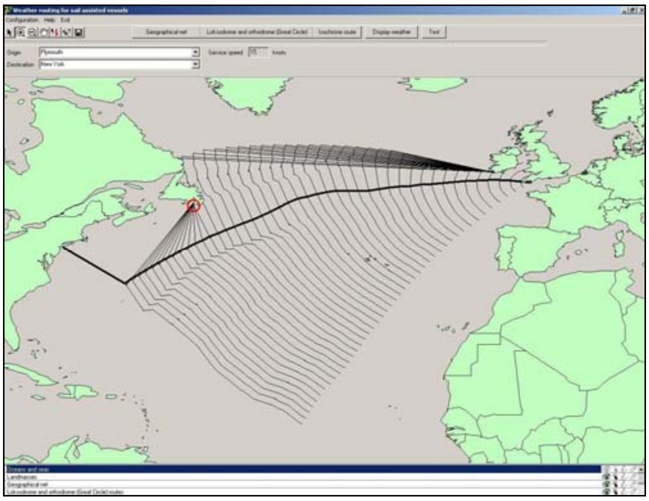
Figure 5. Algorithm for finding new candidate point C on A-B segment
that A-C segment does not cross land

5. Application example

Following the proposed solution described above an application including applied isochrone method has been implemented. Route determined by the adopted isochrone method will serve as a base for the initial population in a route finding multiobjective algorithm with evolutionary approach.

Let us assume there is a route to be found starting in Plymouth and finishing in New York. Unfortunately classic modified isochrone method [7] fails to find a proper route due to land obstacles as shown in *Figure 6*. When the isochrones come across a landmass, i.e. an island, they tend to stuck in some points (marked by a circle in *Figure 6*). In such points there is no possibility to find another non-land point for given search sector when a new isochrone is being generated. As a result, route found by the classic modified isochrone algorithm is suboptimal.

The adapted isochrone method, as shown in *Figure 7,* does not encounter the problem of isochrone points being stuck at landmasses. Furthermore, it does find time-optimal Plymouth-New York route (*Figure 8)*. Configuration settings of the method are presented in *Table 1*.


Weather routing for sail assisted vessels
Configuration Help Exit
Geographical net
Loksodrome and orthodrome (Great Circle)
Isochrone route
Display weather
Test

Origin: Plymouth
Service speed 15 knots
Destination: New York

Oceans and seas
Landmasses
Geographical net
Loksodrome and orthodrome (Great Circle) routes

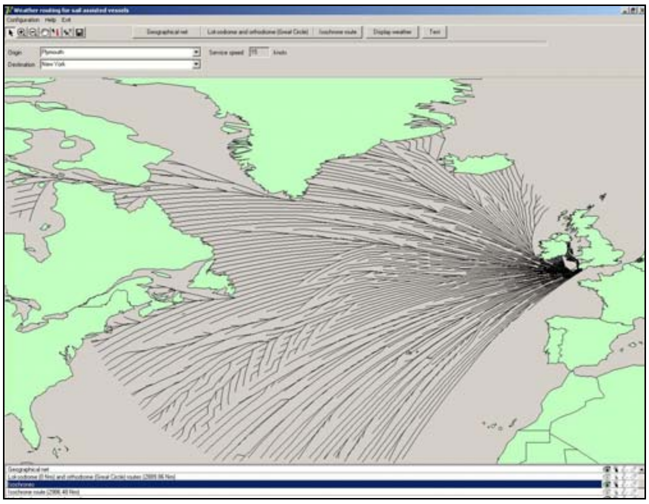
Figure 6. Isochrones and isochrone route (thick solid line) for Plymouth –
New York voyage found by classic modified isochrone method

Table 1. Configuration settings of the adopted isochrone method

Parameter name	**Value**
Search subsector angle	± 60°
Weather data grid resolution (lon x lat)	1.25° x 1.0°
Land bitmap resolution (lon x lat)	0.05° x 0.05°
Time step between isochrones	4 h
Points per isochrone	100

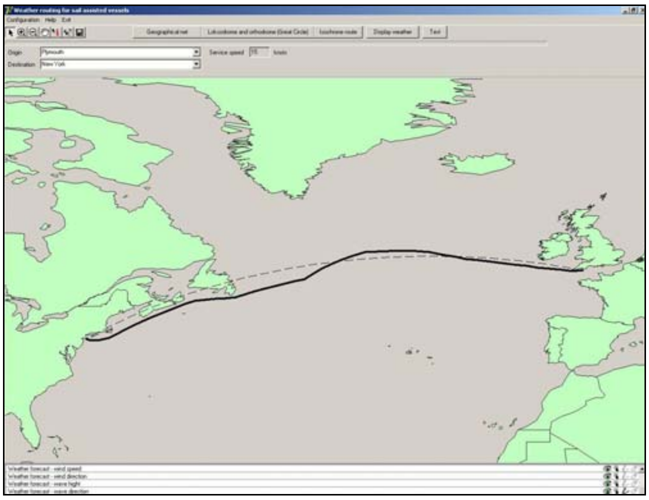
Route Plymouth – New York as shown in *Figure 8* easily bypasses all land obstacles and reaches the destination port. It is worth noticing that the route found is close to the Plymouth – New York orthodrome (Great Circle), the shortest possible geographical route, marked in *Figure 8* by a dashed line. *Table 2* compares length of Plymouth – New York routes determined by classic modified isochrone method, adopted modified isochrone method and the orthodrome as well as their execution times.

Results presented in *Table 2* depict that the route determined by the proposed adopted isochrone method is much shorter (more than 9.5%) than the one determined by the classic modified isochrone method. Time required to execute the proposed method is 7 sec. longer than the one for the classic method. It is justified by the necessity of performing additional operations assuring “no land crossings”. Nonetheless, the execution time of the proposed method is still acceptable. Of course, both isochrone methods are significantly more time consuming than simple orthodrome determination procedure. It is caused by the fact that the latter is a simplified mathematical procedure, disregarding land obstacles and ship’s speed characteristic.


Weather routing for sail assisted vessels
Configuration
Help
Exit
Geographical net
Loxodrome and orthodrome (Great Circle)
Isochrone route
Display weather
Test
Origin: Plymouth
Destination: New York
Service speed: 15 knots

Geographical net
Loxodrome (0 Nm) and orthodrome (Great Circle) routes (2889.86 Nm)
Isochrones
Isochrone route (2986.48 Nm)

Figure 7. Isochrones found by proposed adopted isochrone method for Plymouth – New York voyage


Weather routing for sail assisted vessels
Configuration
Help
Exit
Geographical net
Loxodrome and orthodrome (Great Circle)
Isochrone route
Display weather
Test
Origin: Plymouth
Destination: New York
Service speed: 15 knots

Weather forecast - wind speed
Weather forecast - wind direction
Weather forecast - wave hight
Weather forecast - wave direction

Figure 8. Isochrone route (thick solid line) found by proposed adopted isochrone method for Plymouth – New York voyage and appropriate orthodrome route (dashed line)

Table 2. Length of Plymouth – New York routes determined by various methods and methods’ execution time

Name	Plymouth – New York route length	Method execution time
Classic modified isochrone method	3306.88 Nm	18 sec.
Proposed adapted isochrone method	2986.48 Nm	25 sec.
Orthodrome (Great Circle)	2889.86 Nm	< 1 sec.

6. Conclusion

Isochrone method, although deprecated as a general route finding tool, still can be utilized in modern weather routing evolutionary systems for initial population of routes. However, special attention must be given to assure that the isochrone method does not produce a route crossing landmasses. Currently, no detailed description of how to meet this requirement is available. Thus, an adaptation proposal of the isochrone method with area partitioning is provided. The proposal improves the classic isochrone method the way that resulting routes are free from land crossings. In result, when applied to a weather routing system with evolutionary approach, this algorithm facilitates creation of initial population, resulting with routes of reduced collision risk and low costs of passage.

References

[1] Franklin, W.R. (2006). PNPOLY – Point Inclusion in Polygon Test. *Web site: http://www.ecse.rpi.edu/Homepages/wrf/Research/Short_Notes/pnpoly.html*.

[2] Hagiwara, H. (1989). *Weather routing of (sail-assisted) motor vessels.* PhD thesis. Delft.

[3] James, R.W. (1957). *Application of wave forecast to marine navigation.* US Navy Hydrographic Office, Washington.

[4] Papadimitriou, Ch. (1994). *Computational complexity.* Addison Wesley.

[5] Smierzchalski, R. & Michalewicz, Z. (2000). Modeling of a Ship Trajectory in Collision Situations at Sea by Evolutionary Algorithm. *IEEE Transaction on Evolutionary Computation* No. 3 Vol. 4, 227-241.

[6] Spaans, J.A. (1986). *Windship routeing.* Mongraph. Delft.

[7] Wisniewski, B. (1991). *Problemy wyboru drogi morskiej statku*. Wydawnictwo Morskie, Gdańsk.

NON-LINEAR BACKSTEPPING SHIP COURSE CONTROLLER

Witkowska Anna
University of Technology, Gdańsk, Poland

Śmierzchalski Roman
Maritime University, Gdynia, Poland

Keywords
backstepping, Lapunov function, asymptotic stability

Abstract
A ship, as an object for course control, is characterised by a nonlinear function describing the static manoeuvring characteristics. One of the methods, which can be used, for designing a non-linear course controller for ships is the backstepping method. It was used here for designing the configurations of non-linear controllers, which were then applied for ship course control. The parameters of the obtained non-linear control structures were tuned to optimise the operation of the control system. The optimisation was performed using genetic algorithms. The quality of operation of the designed control algorithms was checked in simulation tests performed on the mathematical model of the tanker completed by steering gear.

1. Introduction

In recent ten to twenty years a number of new methods were developed for designing controllers to control non-linear dynamic systems. These are usually recursive methods, such as backstepping, forwarding, and methods being the mixture of these two. A common concept in these two recursive methods is the design of a globally stable control system, revealing a cascade structure, for a class of non-linear dynamic systems. In particular, the backstepping method is bases on the Lapunov function theory [10] but its origin can be found in some theories of linear control, such as the feedback liberalisation method, or the LQR method.

The beginning of development of the backstepping method oriented on the design of a non-linear control systems can be dated on the turn of Eighties and Nineties of the last century, a list and discussion of publications issued in that time can be found in an overview by Kokotović and Arcak [7], and also in Fossen [5] and in fundamentally book of backstepping methods [8]. The backstepping method directly bases on the mathematical model of the examined system, introducing to it new variables in the form depending of the state variables, controlling parameters, and stabilising functions. The task of a stabilising function is to compensate non-linearity's that occur in the system and affect the stability of its operation. The liberalisation methods used in the feedback-based systems usually aim at eliminating the non-linearity's in the system. The use of the backstepping method makes it possible to form, in an arbitrary way, additional non-linearities and introduce them to the control system. However, only the undesirable non-linearities are eliminated from the system [3]. The backstepping method allows to obtain a global stability in cases when the feedback linearisation method only secures local stability.

In marine technology, the presented backstepping method was used in systems steering a ship on its course [12], to secure course stabilisation. In 1999, Fossen published a work [4], which focuses on practical use of the backstepping method in mechanical systems and its application to ship steering. However, attempts to apply this method in real marine systems revealed numerous problems, which needed solving. One of them is the structure and selection of stabilisation functions and identification of their parameters. In order to obtain optimal quality of control of the designed non-linear course controller, its parameters need tuning. The presented in the literature design systems that make use of the beckstepping method are optimised using classical methods, usually based on the solution of the Riccati equation [9].

The article presents the method of automatic optimisation of ship course controller parameters, performed with the aid of a genetic algorithm. So far, this technique has not been employed to solve such kind of problems. The operation of the genetic algorithm bases on generating solutions by imitating the evolutionary process [6], [11].

2. Model of the ship

The geometry of the ship motion is defined in the coordinate system Xo, Yo, while the motion of the ship itself is described in the relative coordinate system (x,y), fixed to the ship. Motion of the ship is shown in Figure 1.

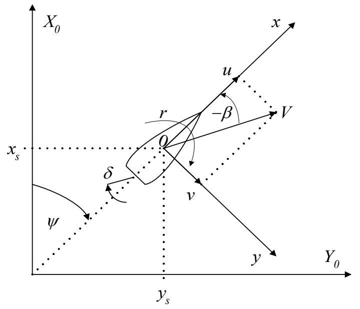


Figure 1. Ship motion co-ordinate system

The control system discussed in the article was designed for steering a ship on the course. In the system, the controlled parameter is the ship course, ψ(t), while the controlling parameter is the rudder angle, δ(t). The equations describing dynamical characteristics of the ship were derived from Newtonian dynamics laws. It was assumed that for large displacement ships, tankers for instance, transverse movements can be neglected. In the presented investigations, the mathematical model of dynamical characteristics of the ship was assumed that of a model tanker described by Astrom and Wittenmark in „Adaptive Control" [1], [2] and modelled by a non-linear second-order differential equation, referred to as the Norrbin model [1].

The obtained model is given by the following equation.

$$T \cdot \ddot{\psi}(t) + H_N(\dot{\psi}(t)) = K\delta(t) . \tag{1}$$

Function

$$H_N(\dot{\psi}(t)) = \frac{\alpha}{\beta}\dot{\psi}^3(t) + \beta\dot{\psi}(t)$$

expresses the steady-state relation between δ(t) and $\dot{\psi}(t)$ .The parameters α and β are real constants and determined from the "spiral test", taking values α = β = 1 in the model. The parameters *T = T₀(L/u),* where $T_0 = T_{10} + T_{20} - T_{30}$ and *K* was determined from relation (2).

$$K = K_0\left(\frac{u}{L}\right),\; T_i = T_{i0}\left(\frac{L}{u}\right),\; i = 1,2,3 \tag{2}$$

The model parameters were determined at speed *u* = 5 [m/s]. The length of the examined tanker is *L* = 350 [m]. In the article, the tanker in two loading states is examined. The first state is the ship without cargo (liquid), in this case ballast tanks are filled with water and it is a so called the ballasting state. For the examined tanker in this loading state the model parameters take the values:

K_0 = 5.88, T_{10} = –16.91, T_{20}= 0.45, T_{30} = 1.43.

The second state of operation refers to the tanks fully laden with the transported liquid and bears the name of the full load state. In this case the model parameters take the values:

K_0 = 0.83, T_{10} = –2.88, T_{20} = 0.38, T_{30} = 1.07.

The model of dynamic characteristics of the ship was completed by the model of the steering gear, described by [14] and schematically shown in *Figure 2*.

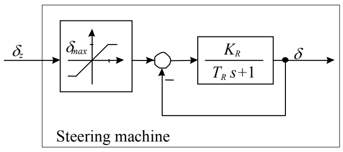


Figure 2. Steering gear system block diagram

In this article it was assumed that the rate of rudder motion is approximately limited to $\dot{\delta}_{\max} = 6$ [deg/s] until $|\delta_z - \delta| \le 3$ [deg], when the rudder operates in the linear region of the characteristic. The maximum rudder angle is $\delta_{\max} = 35$ [deg]. For this assumption the steering gear dynamical characteristic was given by the following equation (3), in which T_R =156 [s] and K_R =96 [deg].

$$\dot{\delta}(t) = \frac{K_R}{T_R}\delta_z(t) - \frac{1}{T_R}\delta(t). \tag{3}$$

The discussed model of dynamic characteristics of the tanker, and the model of the steering gear, were modelled in Matlab/Simulink.

3. Designing non-linear controllers

As mentioned before, the controller was designed using the backstepping method. When designing the steering rules with the aid of this method, new state variables z_i and stabilising functions α_i are introduced, in a recurrence way, in i-th step. The number of steps depends on the number of state variables used in the mathematical model of the examined object.

In the present article, the backstepping method was used for developing two algorithms of nonlinear ship course control (nonlinear controllers), denoted as version A and version B. The form of dynamical characteristics of the ship used in version A and B for deriving control rules for the nonlinear controllers is given by formula (1). When deriving the rules of the nonlinear control in version A, dynamical characteristics of the steering gear described by equation (3) was neglected and the control rule were obtained in two steps of backstepping procedure. In version B dynamical characteristics of the steering gear were taken into account and control rule were obtained in three steps

$$\begin{aligned} &\dot{x}_1(t) = x_2(t), \\ &\dot{x}_2(t) = -\frac{1}{T}H_N(x_2(t)) + u(t), \\ &H_N(x_2(t)) = \frac{\alpha}{\beta}x_2^3(t) + x_2(t). \end{aligned} \tag{4}$$

Version A

Step 1: In the first step new variables are introduced. The first virtual variable z_1 is the control error defined as

$$z_1 = \Delta\psi(t) = \psi(t) - \psi_z(t) = x_1(t) - \psi_z(t), \tag{5}$$

while the second variable z_2 is the virtual variable determined from the relation

$$z_2 = x_2(t) - \alpha_1(z_1), \tag{6}$$

where $\alpha_1(z_1)$ is the virtual control introduced in the first step. After differentiating Eq. (5) with respect to time and placing relation (4) and (6) we arrive at

$$\dot{z}_1 = \dot{x}_1(t) - \dot{\psi}_z(t) = x_2(t) - \dot{\psi}_z(t) = z_2 + \alpha_1(z_1) - \dot{\psi}_z(t). \tag{7}$$

Then the first Lapunov function is defined as

$$V_1(z_1) = \frac{1}{2} z_1^2 . \tag{8}$$

The derivative of the first Lapunov function along the solution (7) takes the form

$$\dot{V}_1(z_1) = z_1 \dot{z}_1 = z_1 [z_2 + \alpha_1(z_1) - \dot{\psi}_z(t)]. \tag{9}$$

From relation (9) the virtual control $\alpha_1(z_1)$ is derived as

$$-k_1 z_1 = \alpha_1(z_1) - \dot{\psi}_z(t) . \tag{10}$$

Transforming Eq. (10) leads to

$$\alpha_1(z_1) = -k_1 z_1 + \dot{\psi}_z(t) . \tag{11}$$

After placing the derived relation (11) in Eq. (9) we get the formula for the first derivative of the Lapunov function in this step

$$\dot{V}_1(z_1) = -k_1 z_1^2 + z_1 z_2 . \tag{12}$$

Comparing equations (7) and (11) gives us the formula for the first derivative of the newly introduced variable z_1

$$\dot{z}_1 = -k_1 z_1 + z_2 . \tag{13}$$

Based on relation (11) and (13) the derivative $\dot{\alpha}_1(z_1)$ for the next design step is also derived, as

$$\dot{\alpha}_1(z_1) = -k_1(-k_1 z_1 + z_2) + \ddot{\psi}_z(t), \tag{14}$$

which is the virtual control derivative in step 1.
Step 2: The derivative of the second variable is determined from Eq. (6) and (4).

$$\dot{z}_2 = \dot{x}_2(t) - \dot{\alpha}_1(z_1) = -\frac{1}{T} H_N(x_2(t)) + u(t) - \dot{\alpha}_1(z_1) . \tag{15}$$

The second Lapunov function and its derivative takes the form

$$V_2(z_1, z_2) = V_1(z_1) + \frac{1}{2} z_2^2 , \tag{16}$$

$$\dot{V}_2(z_1, z_2) = -k_1 z_1^2 + z_1 z_2 + z_2 \dot{z}_2 , \tag{17}$$

After placing relation (15) into Eq. (17), we get

$$\dot{V}_2(z_1, z_2) = -k_1 z_1^2 + z_2 \left[z_1 - \frac{1}{T} H_N(x_2(t)) + u(t) - \dot{\alpha}_1(z_1) \right]. \tag{18}$$

Form the second derivative given by formula (18) the control is determined as

$$u(t) = -k_2 z_2 - z_1 + \frac{1}{T} H_N\left(x_2(t)\right) + \dot{\alpha}_1(z_1)\,, \tag{19}$$

By substitution the obtained control rule (19) into relation (18), we arrive at the final form of the Lapunov function derivative

$$\dot{V}_2\left(z_1, z_2\right) = -k_1 z_1^2 - k_2 z_2^2\,, \tag{20}$$

which is negatively determined for k$_1$, k$_2$ > 0. Tuning parameters k$_1$ and k$_2$ of the control rule derived with the aid of the backstepping method and given by Eq. (19) is performed using the genetic algorithm described in Chapter 4.

4.6 *Version B*

The mathematical model of the ship was complemented by the equation of the steering machine (3), which can describe by state equation in form of

$$\cdots \dot{x}_3(t) = -\frac{1}{T_R} x_3(t) + \frac{K_R}{T_R} u(t), \tag{21}$$

where $x_3(t)$ is the rudder angle and $u(t)$ is the controlling input. For an object described by state equations (4) and (21) the procedure to design the non-linear control rule was introduced similarly like in the version A but in three steps. The different was in third step, where we introduced third new state variable $z_3(t) = x_3(t) - \alpha_2(z_1, z_2)$, where α_2 is the second stabilizing function. Then the control rule for the ship and the steering gear as an object is determined as

$$u(t) = \frac{T_R}{K_R}(-k_3 z_3 + \frac{1}{T_R} x_3(t) + \dot{\alpha}_2(z_1, z_2) - z_2), \tag{22}$$

where the time derivative $\dot{\alpha}_2\left(z_1, z_2\right)$ is described by equations

$$\dot{\alpha}_2(z_1,z_2) = -k_2\dot{z}_2 - \dot{z}_1 + \frac{1}{T}\dot{H}_N(x_2(t)) - k_1\left(-k_1\dot{z}_1 + \dot{z}_2\right) + \dddot{\psi}_z(t), \tag{23}$$

$$\dot{H}_N(x_2(t)) = 3\frac{\alpha}{\beta} x_2^2 \dot{x}_2 + \dot{x}_2\,, \tag{24}$$

for k_1, k_2, k_3> 0.

4. Parameters of non-linear controllers

The optimisation of the parameters for the derived control rules of the non-linear controllers given by the formula (19) and (22) were performed using genetic algorithm. *Figure 3* shows, in a block schematic form, the structure of the genetic algorithm used in the present analysis for tuning parameters of the examined ship course controller. The tuning programme works until conditions for its stop are met. Two types of algorithm stop conditions are possible. The first condition consists in limiting the maximum number of generations in the optimisation process, while in the second condition the algorithm checks whether the newly generated populations improve considerably the previously obtained solutions. The entire process is repeated until the maximum number of generations is reached. In the examined case, the maximum number of generations was equal to 100, which on the basis of previous investigations was assumed satisfactory. The final solution was the best solution in the most recent population. Below described are particular steps of operation of a genetic algorithm.

Creating the initial population. In order to initiate the initial population the chromosomes are generated randomly using the bit-by-bit method. The length of the chromosome depends on the number of parameters to be coded, their maximum and minimum values $k_{\max}$, $k_{\min}$ and their accuracy n, according to the formula

$$(k_{\max} - k_{\min}) \cdot 10^{n_i} \le 2^{m_i} - 1\,, \tag{25}$$

where: n – number of meaningful decimal places defining the accuracy of the parameter, mi – length of the code sequence for the coded parameter.

Decoding. From the chromosome extracted are the successive sequences of bits that correspond to the coded parameters. The decimal value for each parameter is calculated using the following formula where: decimal (1010...0112) is equal to the decimal value of the binary chain.

$$k = k_{\min} + decimal(1010...011_2)\frac{(k_{\max} - k_{\min})}{2^{m_i} - 1}\,. \tag{26}$$

Simulations and evaluation cost. The quality of control of the ship course controller was evaluated here with the aid of a digitised version of the integral quality coefficient, having the form:

$$J_E = \frac{1}{N}\sum_{i=1}^{N}(\Delta\psi_i(t))^2 + \lambda\frac{1}{N}\sum_{i=1}^{N}\delta_i^2(t)\,, \tag{27}$$

where N is an integer number of iterations in control simulations, λ is the scale factor, in the examined case $\lambda = 0.1$, $\Delta\psi_i(t)$ is the i-th course error determined by subtracting the obtained course from its set value, $\delta_i(t)$ is the i-th angle of the rudder deflection. The genetic algorithm minimises the value of the function (27), by minimising both the course error $\Delta\psi$ and the rudder angle $\delta(t)$. The component connected with the rudder angle is scaled to have similar amplitude to that of the course error.

Genetic operations. Genetic operations comprise selection, crossover, and mutation. More information about used genetic operation can find [14].

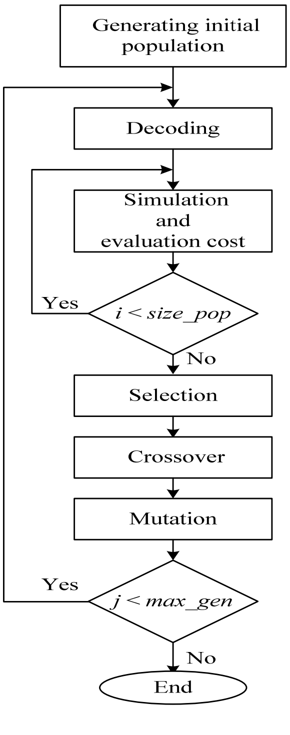


Figure 3. Block diagram of operations performed by a genetic algorithm

5. Simulation tests

In order to evaluate the quality of the derived algorithm of non-linear control, simulation tests were performed using the programme package Matlab/Simulink.

Tuning the course controller's parameters with the aid of the genetic algorithm made use of the ship dynamic characteristic equations with the parameters set for the ballasting state. The set course was rapidly changed by 40 [deg]. The quality coefficient, given by formula (27), was determined from the tests trials performed within 500 [s] with sampling period 0.01 [s]. The parameters of the genetic algorithm were: the probability of crossover was $p_c = 0.60$, while the probability of mutation was $p_m = 0.01$.

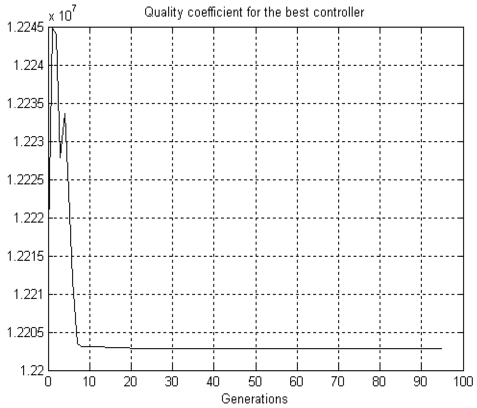
The best values of the tuned parameters for the examined controller in version A were k_1*=0.0152, k_2=335.8*. The best values of the tuned parameters for the examined controller in version B were k_1*=436.07, k_2=1973.3*, k_3*=0,0196.* These are the parameter values at which the minimum values of the quality coefficient were obtained at the stage of tuning with the aid of the genetic algorithm. The example results of tuning the parameters of the non-linear controller with two tuned parameters (version A) are collected in Table 1. In this case the identical minimum values of the quality coefficient were obtained in as many as three tests. The example process of tuning parameters for the non-linear controller with two parameters is shown in *Figure 4*.

Table 1. Results of tuning settings for non-linear controller with two parameters with the aid of genetic algorithm

Test no.	N	k_1	k_2	J_E
1	16	0.0156	375.3	12 204 599
2	57	0.0151	337.3	12 202 863
3	**52**	**0.0152**	**335.8**	**12 202 858**
4	33	0.0151	337.5	12 202 912
5	100	0.0151	334.4	12 202 886
6	**53**	**0.0152**	**335.8**	**12 202 858**
7	100	0.0156	375.7	12 204 557
8	48	0.0155	375.6	12 204 457
9	100	0.0152	332.8	12 202 913
10	**96**	**0.0152**	**335.8**	**12 202 858**

The investigations were focused on the effect of changes of object parameters on the quality of control. The controller were tuned for the ship dynamic characteristic equations corresponding to the ballasting state, but in this part of analysis they were used for controlling the ship motion with two different states of load: ballasting and full load. *Figure 5a* compare results of simulation with two controllers with two tuned parameters (19), marked with solid line and with three tuned parameters (22), marked with a dashed line. In the first 1000 [s] of the tests, the mathematical model of the ship made use of the parameters corresponding to the ballasting state, while during the remaining time the full load parameters were used.

a)



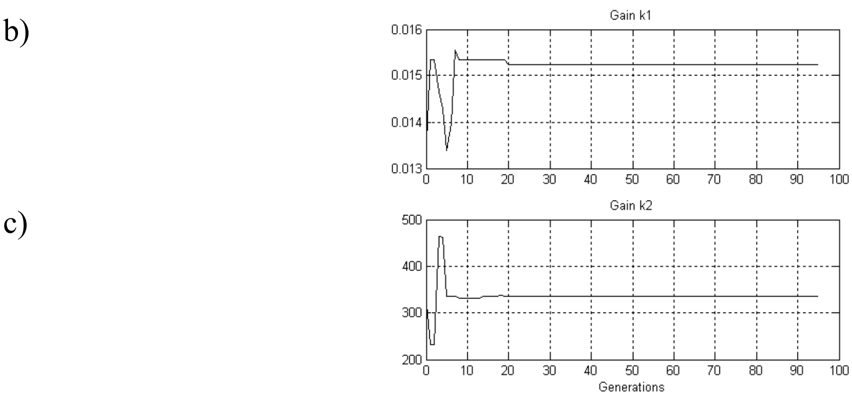


Figure 4. The process of tuning parameters for the non-linear controller with two parameters. (a) quality coefficient for the best controller, (b) parameter k_1, (c) parameter k_2

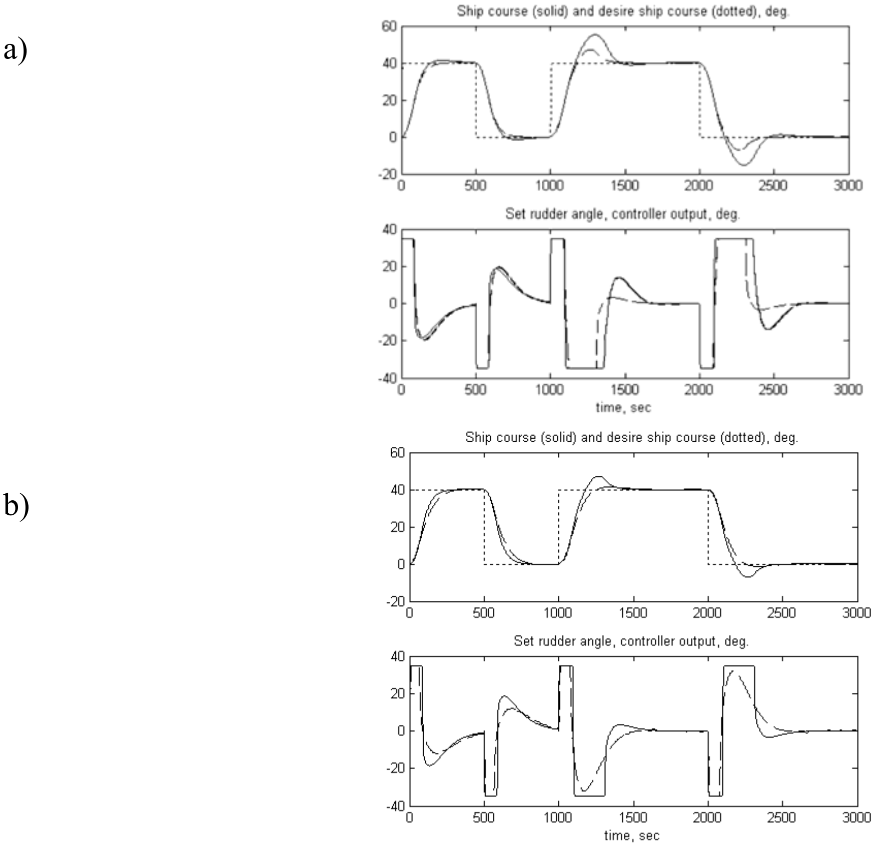


Figure 5. Comparing results of simulation with tuned controllers: a) non-linear controller with two parameters (solid line), non-linear controller with three parameters (dashed line), b) non-linear controller with two parameters (solid line), PD controller (dashed line)

6. Conclusion

The article discusses the two control rules derived for non-linear controllers designed with the aid of the backstepping method and used for controlling the ship motion on the course. The first control rule with two parameters (version A) were design by neglected the steering gear, the second control rule with three parameters (version B) were taken into account the steering gear in aim of improvement of quality controlled, as shown in *Figure 5a*. Non-linear controllers designed with the aid of the backstepping method require tuning of their parameters to the optimal values. The use of genetic algorithms for this purpose produced excellent results. Sample results illustrating the process of tuning the parameters for the non-linear controller were shown in *Figure 4*. The tuned non-linear controller with backstepping procedure (version B) was compared with PD controller. The results were shown in *Figure 5b*. When the ship was in the full load state better results were produced by the PD controller than by the non-linear controllers designed using the backstepping method. The reason of this regularity lies in the fact that the parameters of the controllers were only tuned for the ballasting state and then were used unaltered for the full load state, which was the source of some error. It turned out that the backstepping method is more sensitive to changes of parameters than the PD controller, which seems to be more robust. Therefore it is necessary to perform the analysis of the model parameters using adaptation techniques, which will be examined in the nearest future.

References

[1] Amerongen, J. (1982). *Adaptive steering of ship. A model reference approach to improved manoeuvering and economical course keeping.* PhD Thesis, Delft University of Technology, Netherlands.

[2] Astrom, K. J. & Wittenmark, B. (1989). *Adaptive Control.* Addison Wesley, Reading MA.

[3] Fossen, T. I. & Strand, J. P. (1998). Non-linear Ship Control (Tutorial Paper). *Proceedings of the IFAC Conference on Control Application in Marine Systems CAMS'98.* Fukuoka, Japan pp. 1□75.

[4] Fossen, T. I. & Strand, J. P. (1999). *A Tutorial on Non-linear Backstepping: Applications to Ship Control, Modelling, Identification and Control,* MIC-20(2), 83-135.

[5] Fossen, T. I. (2002). *Marine Control Systems. Guidance, Navigation, and Control of Ships, Rigs and Underwater Vehicles. Marine Cybernetics.* Trondheim, Norway.

[6] Goldberg, D. E. (1989). *Genetic algorithms in searching, optimisation and machine learning.* Reading, MA: Addison Wesley.

[7] Kokotović, P. & Arcak, M. (2001). Constructive non-linear control: a historical perspective. *Automatica 37*(5), 637-662.

[8] Krstić, M. Kanellakopulos, I. & Kokotović, P. V. (1995). *Non-linear and Adaptive Control Design.* John Willey & Sons Ltd., New York.

[9] Krstić, M. & Tsiotras, P. (1999). Inverse Optimal Stabilization of a Rigid Spacecraft. *IEEE Transactions on Automatic Control, 44*(5), 1042-1049.

[10] La Salle, J. & Lefschetz, S. (1966). *Zarys teorii stabilności Lapunowa i jego metody bezpośredniej*. BNI. Warszawa..

[11] Michalewicz, Z. (1996). *Genetic algorithms + data structures = evolution programs.* Berlin, Springer.

[12] Pettersen, K. Y. & Nijmeijer, H. (2004). Global practical stabilization and tracking for an under-actuated ship - a combined averaging and backstepping approach. *Modelling, Identification and Control, 20*(4), 189-199.

[13] Tomera, M., Witkowska, A. & Śmierzchalski, R. (2005). A Nonlinear Ship Course Controller Optimised Using a Genetic Method. *Materiały VIII Krajowej Konferencji nt. Algorytmy Ewolucyjne i Optymalizacja Globalna.* Korbielów, 255-262.

[14] Velagić, J., Vukić, Z. & Omerdić, E. (2003). Adaptive fuzzy ship autopilot for track-keeping. *Control Engineering Practice, 11*(4), 433-443.

SENSITIVITY ANALYSIS OF A FUZZY EXPERT SYSTEM FOR MODELLING DEPENDENCIES IN HUMAN OPERATORS' EMERGENCY TASKS

Zio Enrico, Baraldi Piero, Librizzi Massimo
Department of Nuclear Engineering, Polytechnic of Milan, Milan, Italy

Podofillini Luca, Dang H. Vinh
Paul Scherrer Institute, PSI Villigen, Switzerland

Keywords
human reliability analysis, fuzzy expert system, sensitivity analysis

Abstract

This paper analyzes the behaviour of a fuzzy expert system for evaluating the dependence among successive operator actions, through a sensitivity analysis on the fuzzy input partitioning and assessment. Preliminary results are presented with respect to a case study concerning two successive tasks of an emergency procedure in a nuclear reactor. Work is in progress to perform a thorough sensitivity analysis to generalize the results obtained.

1. Introduction

Fuzzy logic (FL) [8] modelling has proven successful in a variety of industrial tasks where ambiguous, qualitative and linguistic data are used to represent the behaviour of the system or process [5]. One of the main strengths of FL compared with other modelling schemes is that the underlying knowledge base capturing the system input/output relations is in the form of simple IF-THEN rules, which are easy to examine and understand and which allow taking into account human expertise. Furthermore, the FL models explicitly include the uncertainty and vagueness of the analyst judgments input into the model [2], [4].

In this paper, a Fuzzy Expert System (FES) for modelling dependencies among human operator actions is considered. The FES is constructed through an expert elicitation procedure for identifying the main factors influencing the dependence between successive tasks and their relationships with the dependence level [9].

The design of the FES requires arbitrary choices in the definition of the partitioning of the involved variables into Fuzzy Sets (FSs). In this respect, the objective of

the present work is to perform a sensitivity analysis to investigate the response of the model with respect to different choices. Preliminary results on a case study are presented. Work is in progress to generalize these results.

The paper is organized as follows. In Section 2, the FL framework of the FES is briefly recalled. Section 3 sketches the basics of the dependence level assessment procedure. The reference case study for the numerical application is illustrated in Section 4. Section 5 and 6 report the sensitivity analyses performed. Conclusions are drawn in the last Section.

2. The Fuzzy Expert System for modelling task dependence

The model underpinning the FES for task dependence assessment considers four input factors [6]: "closeness in time", "similarity of performers", "similarity of cues" and "similarity of functions/goals", the latter two making up the "tasks relatedness" factor, and one output, i.e. the dependence level (*Figure 1*).

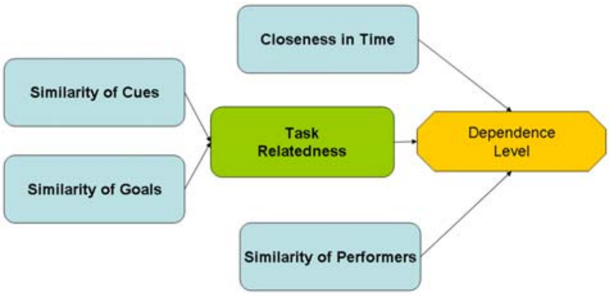


Figure 2. Functional relationships of the dependence model

Each of the four input factors is qualified in terms of linguistic variables with associated linguistic labels (*Table 1*).

Table 1. Linguistic Variables and associated linguistic labels of the input factors

Input Factor	Linguistic Variable	Short Format	Linguistic Labels
x_1	Closeness in Time	"Time"	WIDE (W) NEITHER (NT) CLOSE(CL)
x_2	Similarity of Cues	"Cues"	NONE (N) LOW (L) MEDIUM (M) HIGH (H) COMPLETE (C)
x_3	Similarity of Goals	"Goals"	
x_4	Similarity of Performers	"Performers"	

To the qualifying linguistic labels of each of the four input factors $x_k, k = 1,2,3,4$, in *Table 1*, are associated FSs $X_k^v, v = 1,2,..., k = 1,2,...,4$, with Membership Functions (MFs) $\mu_{X_k^v}(x_k)$, $v = 1,2,...,$ $k = 1,2,...,4$, on their Universes of Discourse (UODs) arbitrarily chosen to be [0,1].

The UOD of the output linguistic variable "Dependence" is formed by the labels y_i={ZERO, LOW, MEDIUM, HIGH, COMPLETE} representing the dependence levels. A singleton FS $Y^v, v = 1,2,...,5$, with $\mu_{Y^v}(y_i) = 0$ for $v \neq i$ and $\mu_{Y^v}(y_i) = 1$ for $v = i$, is associated to each possible label y_i of y (*Figure 2*).

The "task relatedness" is derived from the "similarity of cues" and "similarity of goals" and it is qualified in terms of the linguistic labels contained in *Table 2.*

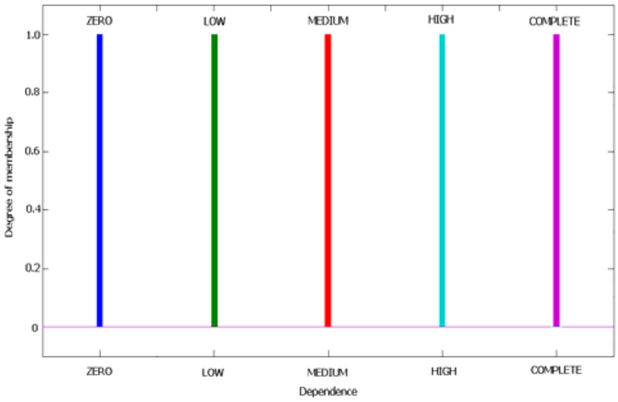


Figure 3. FSs of the discrete output "Dependence"

Table 2. Linguistic Labels of task relatedness

Linguistic Variable	Short Format	Linguistic Labels
Task Relatedness	"Task"	NONE (N) LOW (L) MEDIUM (M) HIGH (H) COMPLETE (C)

Table 3 summarizes the rules which have been identified by the expert to link the "Cues" and "Goals" input factors to the "Task relatedness" [5].

Table 3. Table of rules for the sub-model of "Task"

Cues | Goals	N	L	M	H	C
N	N	N	L	L	M
L	L	L	L	M	M
M	L	L	M	M	H
H	M	M	M	H	H
C	H	H	H	C	C

For example, the first rule has the linguistic form:

If Cues is NONE and Goals is NONE then Task is NONE

Table 4 – Table 8 contain the rules which have been set up by the expert to relate the "Time", "Performer" and "Task" factors to the dependence level.

Table 4. Complete Table of rules for "Task = C"

Perf | Time	W	NT	CL
N	L	L	M
L	L	L	M
M	M	M	H
H	M	M	H
C	H	H	C

Table 5. Complete Table of rules for "Task = H"

Perf | Time	W	NT	CL
N	Z	Z	L
L	Z	L	M
M	L	L	M
H	L	M	H
C	M	H	C

Table 6. Complete Table of rules for "Task = M"

Perf | Time	W	NT	CL
N	Z	Z	Z
L	Z	Z	L
M	Z	Z	L
H	Z	L	M
C	Z	L	H

Table 7. Complete Table of rules for "Task = L"

Perf | Time	W	NT	CL
N	Z	Z	Z
L	Z	Z	Z
M	Z	Z	Z
H	Z	Z	L
C	Z	Z	L

Table 8. Complete Table of rules for "Task = N"

Perf | Time	W	NT	CL
N	Z	Z	Z
L	Z	Z	Z
M	Z	Z	Z
H	Z	Z	Z
C	Z	Z	Z

For example, the first rule in *Table 4* reads:

If Time is WIDE and Performer is NONE and Task is COMPLETE then Dependence is LOW

These rules are obtained by a "label interpolation" procedure founded on few, extreme situations elicited from the expert (grey cells in the *Tables*) [3], [9]. The expert knowledge concerning these extreme evaluations is elicited with few linguistic judgements on pre-specified prototype situations for the input factors. The prototype situations are represented by anchor points placed on the UODs of the input factors. Particular linguistic labels are associated to the anchor points, e.g. the anchor "Different indicators/Different parameters" of "Cues" input factors can be related to its linguistic label NONE(N) and so on (*Figure 3*).

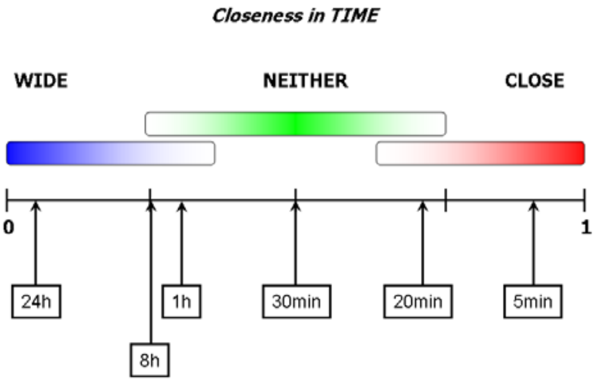
Given the correspondence between the anchor points and the linguistic labels, the rules elicited from the expert take the form:

If Cues is "Different indicators/Different Parameters" and Goals is "Different Functions by Different Systems" then Task is NONE

which is translated into a fuzzy rule of the form:

If Cues is NONE and Goals is NONE then Task is NONE

A "label interpolation" procedure is then used to smoothly spread the consequent labels over the fuzzy rules in order to complete the missing relationships. The complete *Tables* are then presented to the expert who can motivate adjustments and changes aimed at a more adherent representation of its beliefs.



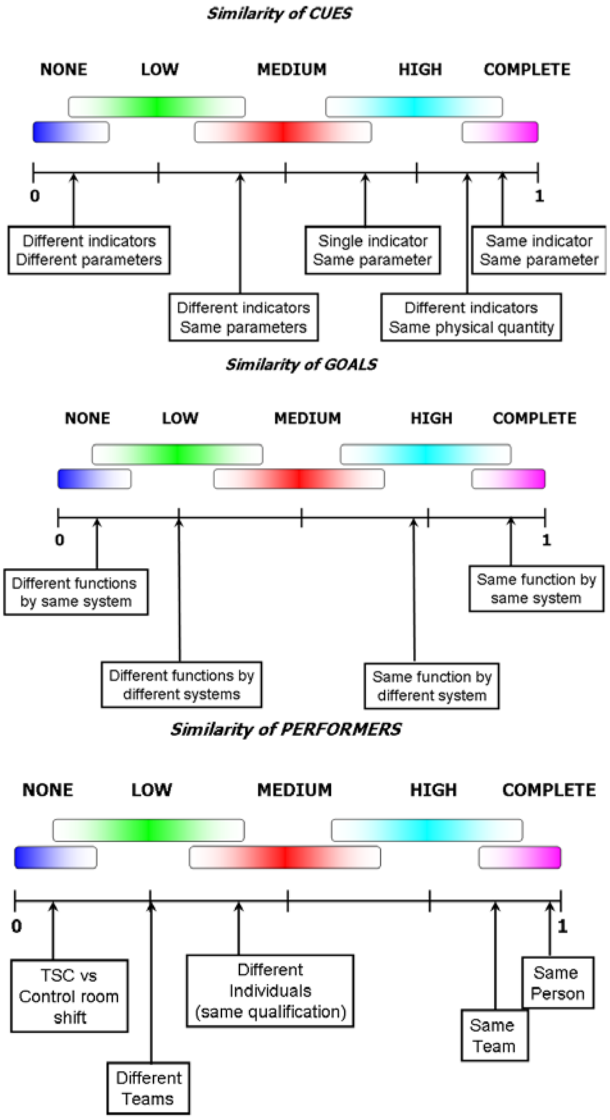

Similarity of CUES
NONE
LOW
MEDIUM
HIGH
COMPLETE
0
1
Different indicators Different parameters
Single indicator Same parameter
Same indicator Same parameter
Different indicators Same parameters
Different indicators Same physical quantity
Similarity of GOALS
NONE
LOW
MEDIUM
HIGH
COMPLETE
0
1
Different functions by same system
Same function by same system
Different functions by different systems
Same function by different system
Similarity of PERFORMERS
NONE
LOW
MEDIUM
HIGH
COMPLETE
0
1
TSC vs Control room shift
Different Individuals (same qualification)
Same Person
Same Team
Different Teams

Figure 4. Anchored UODs with supports of FSs relative to the input factors

3. Assessment procedure

Once the UOD of the inputs and output have been partitioned into FSs and the Table of fuzzy rules has been established, the FES model is completed and ready for use. For a given sequence of tasks, the analyst is required to assign the proper numerical fuzzy values on [0,1] describing the input factors characteristics. This is the so called Fuzzy Fact which enters the model for its quantification. Granting the difficulty of providing such quantitative assessment when it is not possible to introduce a representative measure scale, the input procedure developed for the dependence fuzzy model is based on the same set of anchor points defined by the expert.

This way of proceeding provides an interface between the mathematical model and the analyst's input judgment: the latter is provided by the analyst in terms of point values $x_k^{'}, k = 1,2,3,4$, on the anchored UOD through comparison between the analyzed pair of tasks and the anchor points position (*Figure 3*).

Actually, in practice the analyst might be more comfortable with providing not just point values to describe the input conditions, but also intervals $[a_k^{'}, b_k^{'}]$ reflecting the uncertainty and the ambiguity of the description. In this case, these intervals are taken as supports of corresponding fuzzy input Facts with MFs equal to unity, at least, in correspondence of the analyst assigned point values. *Figure 4* shows an example of an ambiguous input provided by the analyst for the input factor "Performers" and its implementation as Fact in the FES.

On the basis of the FES developed in Section 4, the assessment of the dependence level for a generic Fuzzy Fact $\vec{x}' = (x_1', ..., x_4')$ is performed by a Mamdani fuzzy inference procedure [1] leading to the fuzzy Conclusion y is Y', where Y' is a discrete output FS constituted by the five values

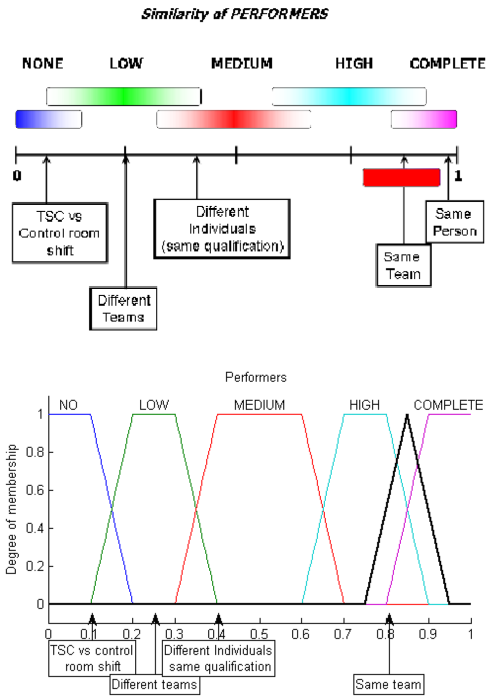


Figure 5. Uncertain input provided by the analyst on the anchored scale (top) with the indication of the support of the FSs; fuzzy input Fact built from the analyst input (bottom)

$\mu_{Y'}(y_i), i = 1, 2, ..., 5$. Thus, the output of the FES consists of a discrete membership function $\mu_{Y'}(y_i)$ that represents the degree of activation of each dependence level y_i={ZERO, LOW, MEDIUM, HIGH, COMPLETE}.

The information available from this kind of output helps the analyst to identify the most activated dependence level that best matches with the input Fact FSs describing the tasks relationships and gives a representation of the uncertainty in the dependence assessment.

4. Case study

The case study considered in this work refers to a set of operator actions intended to avoid excessive boron dilution in the reactor cooling system in case of an Anticipated Transient Without Scram (ATWS) at a nuclear Boiling Water Reactor (BWR). In the considered scenario, the operators have successfully initiated the Standby Liquid Control System (SLCS) to shut the reactor down. To facilitate the reactor shut down, the operators are directed by the procedures to increase the voiding by reducing the level in the reactor to the Top of Active Fuel (TAF). Additionally, they are required to inhibit the actuation of the Automatic Depressurization System (ADS), which is activated by the signal of low water level in the reactor, generated while lowering the reactor water level to the TAF. In case of failure to inhibit the ADS, the reactor pressure would be automatically decreased and low pressure injection systems (e.g. the Core Spray System, CSS), would be activated. The injected water could lead to diluting the boron injected by the SLCS and the consequential failure of controlling reactivity. In case of failure to inhibit ADS actuation, the operators are called to control the level in the reactor using low pressure injection, tripping one of the CSS pumps and controlling the other pump.

The signal to activate the ADS is generated about 7 minutes after the event of failure to scram. At that point, the operators have about 15 minutes to take actions to limit the low pressure injection flow.

The pair of operator tasks involved in the dependence assessment, object of the present case study, is the preclusion of the ADS and the successive control of the reactor vessel level in order to prevent diluting boron concentration after the ADS failure. Both actions are part of the same emergency procedure.

The desired output of the dependence model is the probability of human failure in controlling the reactor vessel level after the failure to preclude the ADS.

4.1. Analyst judgment

The analyst assessment of the four factors entering in input to the dependence model for the scenario at hand (the so called Fact) is as follows:

- "Time": control of low pressure injection would be achieved within about 15 minutes after depressurization of the reactor vessel. The available interval time is assumed from 5 to 20 minutes. Thus the analyst assessment is the interval [5 min, 20 min].
- "Cues": the initial cues are related to the initial failure to scram. The operator is initially successful, the SLCS is properly initiated. The control of low pressure injection is related to maintaining the reactor vessel level. The analyst judgment is: very low (NONE) similarity of cues is present between the two tasks.
- "Performers": the action is carried out by the same team. It is assumed that the Technical Support Center (TSC) does not reach the control room in the time available. The analyst judgment coincides with the anchor point 'same team'.
- "Goals": the two actions relate to different systems and have different goals (inhibit the ADS, the former and controlling the injection, the latter). On the other hand the function of the actions is the same: shut down the reactor by boron control. The analyst considers that the two actions correspond to a prototype situation of tasks with the same function but related to different systems.

5. Model sensitivity to different input UOD partitioning

The quantitative evaluation by the analyst of the Fact in the scenario considered is reported in *Figure 6* (light gray intervals on the interval [0,1]). Note how the interval quantification of the factors "Performers" and "Goals" made by the analyst with respect to the tasks conditions of the case study at hand coincides with the prototypes conditions of "same team" and "same functions by different systems", respectively.

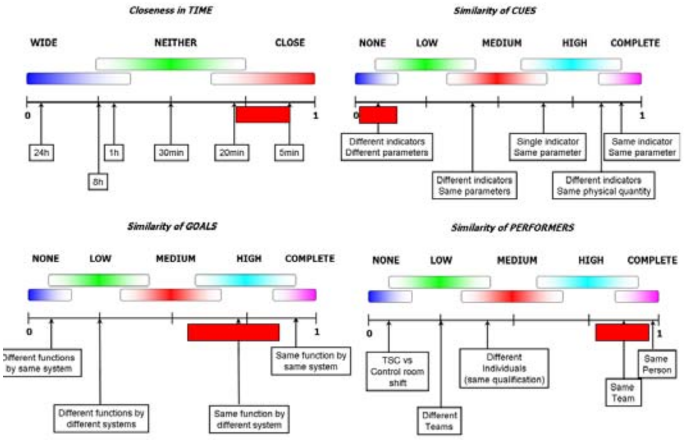

Closeness in TIME
WIDE
NEITHER
CLOSE
0
1
24h
8h
1h
30min
20min
5min
Similarity of CUES
NONE
LOW
MEDIUM
HIGH
COMPLETE
Different indicators Different parameters
Different indicators Same parameters
Single indicator Same parameter
Different indicators Same physical quantity
Same indicator Same parameter
Similarity of GOALS
Different functions by same system
Different functions by different systems
Same function by different system
Same function by same system
Similarity of PERFORMERS
TSC vs Control room shift
Different Teams
Different individuals (same qualification)
Same Team
Same Person

Figure 6. Analyst input assessment on the anchored scale

To investigate the sensitivity of the output FS Y' to variations in the input FSs quantifying the uncertainty in the dependence model definition, both trapezoidal and triangular FSs, are considered keeping the FSs supports fixed. *Figure 6* shows the fuzzification of the analyst interval judgment proposed in *Figure 5* in terms of trapezoidal FSs whereas *Figure 7* presents the case with triangular FSs. The fuzzification of the Fact is achieved by triangular FSs positioned at the centers of the assigned intervals of values.

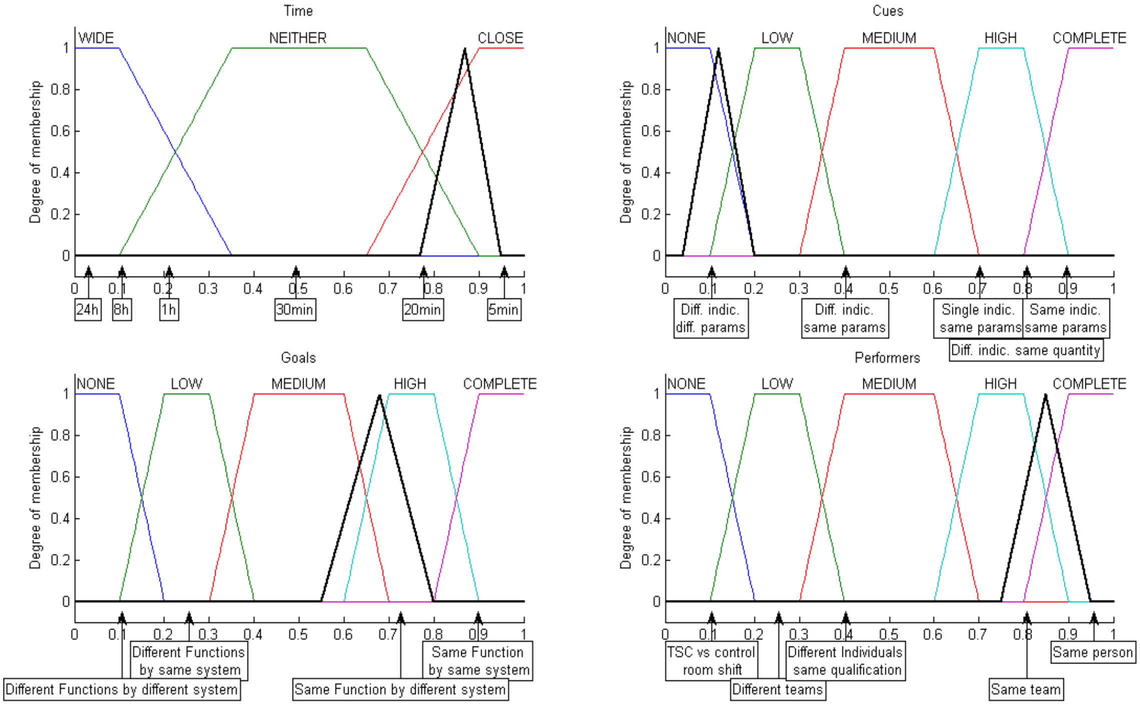


Figure 7. UOD partitioned by trapezoidal FSs. The thick-line triangle represents the FS of the Fact in input to the model

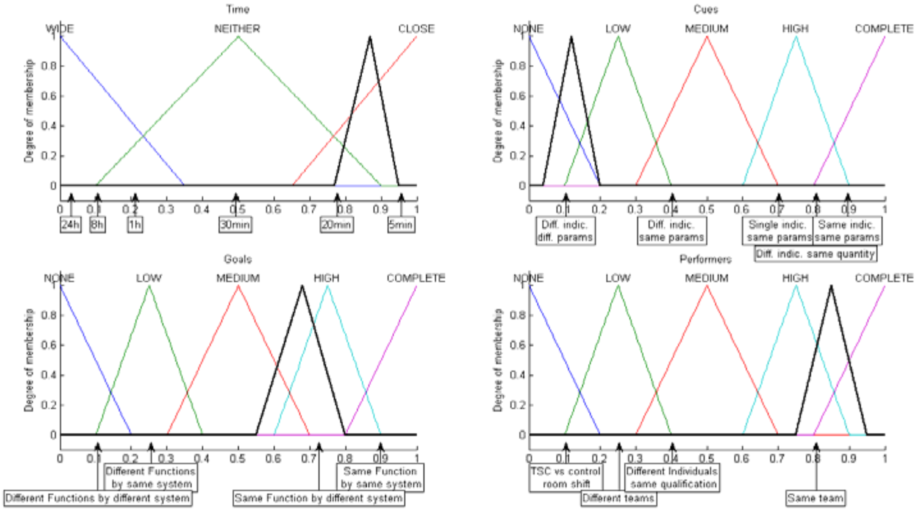


Figure 8: UOD partitioned by triangular FSs. The thick-line triangle represents the FS of the Fact in input to the model.

Figure 9 reports the discrete output FSs describing the dependence level of the actions, 'preclusion of the ADS' and 'control of the reactor vessel level', in the case of trapezoidal FSs (top) and triangular FSs (bottom).

The two cases present a similar representation of uncertainty, with the most activated dependence level being "LOW" and the highest dependence level with non-zero MF being "HIGH".

To further analyze the response of the model to the different (trapezoidal or triangular) input UODs partitioning, the value of the center of the triangular Fact FS of the input variable "Performer", $X_4^{'}$, is varied in the interval [0,1], while keeping constant the Fact FSs of the other three input variables, $X_1^{'}, X_2^{'}, X_3^{'}$.

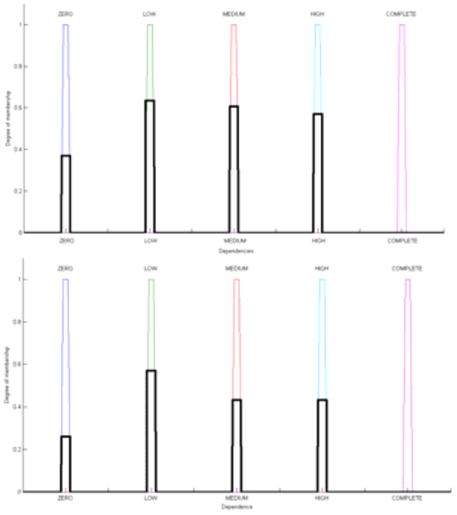


Figure 9. Output FSs of dependence level: input partition by trapezoidal FSs (top) and triangular FSs (bottom).

Figure 9 reports the effects of the variation: the circles represent the degree of activation by the Fact of the dependence levels for the trapezoidal FS input partitioning whereas the asterisks represent the dependence levels for the triangular FS partitioning. The activation degrees of the trapezoidal partitioning are always higher than those of the triangular partitioning. This is due to the fact that the trapezoidal membership functions of *Figure 6* include the corresponding triangular ones of *Figure 7*, as shown in *Figure 10*: this results in larger values of activation of the fuzzy rules and thus higher activation degrees of the output dependence levels.

Furthermore, when adopting a partitioning of the input variables UODs in trapezoidal FSs, the degrees of activation of the output dependence levels are locally more sensitive to variations of the input Fact than in the case of triangular partitioning. This is shown, for example, by the two dips at 0.15 and 0.35 of the "ZERO" dependence level activation degree appearing in *Figure* when the center of the input Fact $X_4^{'}$ is varied.

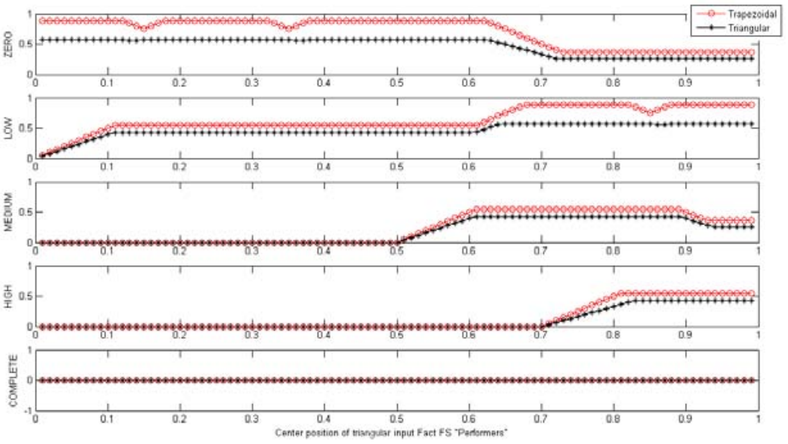


Figure 9. Degree of activation of the dependence levels "ZERO", "LOW", "MEDIUM", "HIGH" and "COMPLETE" as a function of the position of the center of the triangular "Performers" Fact FS. Circles: trapezoidal input partitioning. Asterisks: triangular input partitioning

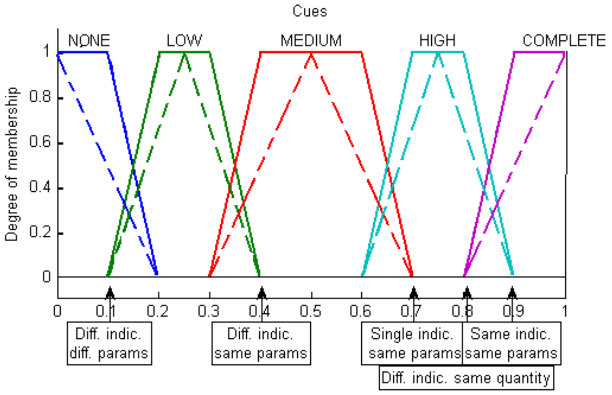


Figure 10. Trapezoidal (solid line) and triangular (dashed line) partitioning of the input factor "Cue"

The reason for this higher sensitivity is due to the more rapid changes of MF values in the side of the trapezoids than in those of the triangles. Thus, two Facts with contiguous centers activating a same rule, would do so with higher activation strengths in the case of trapezoidal MFs than in the case of triangular MFs (*Figure 11*).

A further peculiarity of the trapezoidal MF is the presence of an upper-base interval at constant, unitary value. The effects of this feature can be effectively highlighted by showing the variation of the degree of activation of the "ZERO" dependence level in correspondence of singleton facts ($X_1^{'}, X_2^{'}, X_3^{'}, X_4^{'}$).

Figure 12 shows the case in which the "Performers" Fact is varied in [0,0.2], on both the trapezoidal and triangular input partitioning, for comparison. In correspondence of a variation of the singleton Fact $X_4^{'}$ from 0.09 to 0.1, for example, the degree of activation of the "ZERO" dependence level remains constant and equal to 0.87 in case of trapezoidal MFs because the intersection between the input Fact FS $X_4^{'}$ and the trapezoidal FS "NONE" of the antecedent "Performer" X_4 is always 1 for $x_4^{'}$ varying in [0.09, 0.1]. On the contrary, for the triangular partitioning it varies from 0.54 to 0.49 because of different levels of intersection between the input Fact FS X_4 and the triangular FS "NONE" on the antecedent "Performer".

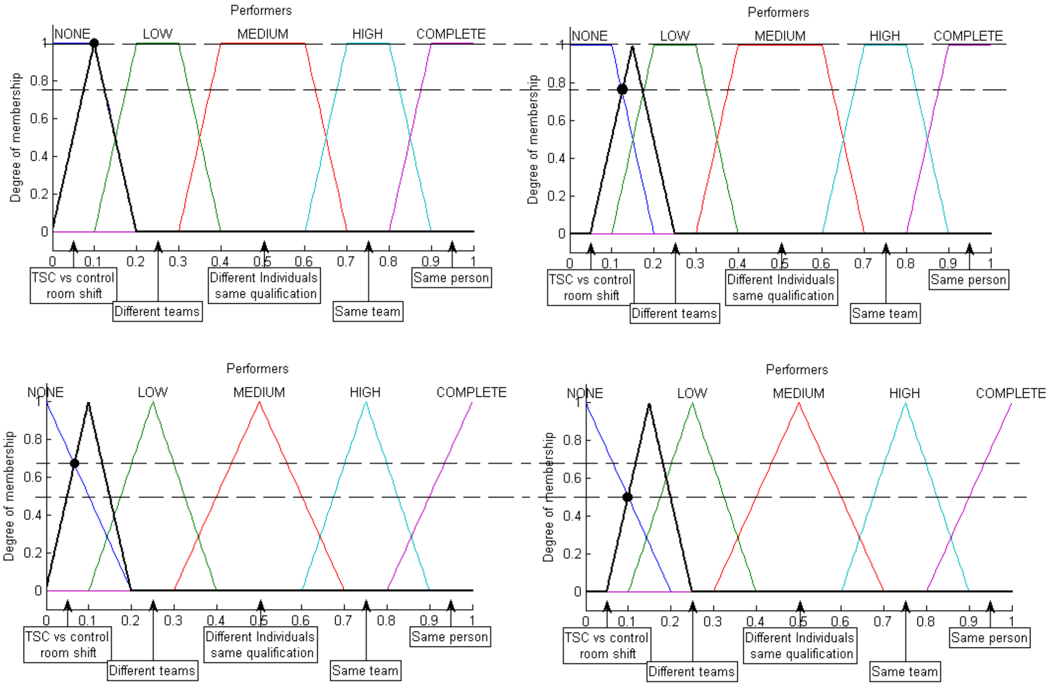


Figure 11. Examples of two contiguous triangular Performer input Facts in trapezoidal (top) input partitioning and in triangular (bottom) input partitioning. The circles represent the intersection of the input Fact with the "NONE" FS. The dot lines represent the corresponding degrees of membership with respect to the "NONE" FS.

In spite of this different absolute sensitivity of the two partitions, the relative differences of the activations of the dependence levels turn out to be less sensitive to the partitioning. *Figure* reports the activation of the dependence levels normalized to sum to 1 for any value of the center of the triangular Fact $X_4^{'}$ on [0,1]. The 'normalized' degrees of activation turn out to be very similar for both trapezoidal and triangular input UOD partitioning.

The results obtained confirm the robustness of the model with respect to the two different shapes of the input partitioning FSs here tested. This is quite important, considering that partitioning is chosen by the expert as basis of the dependence model whereas the analysts only interface with the anchored scale of the input variables and the supports of their linguistic labels.

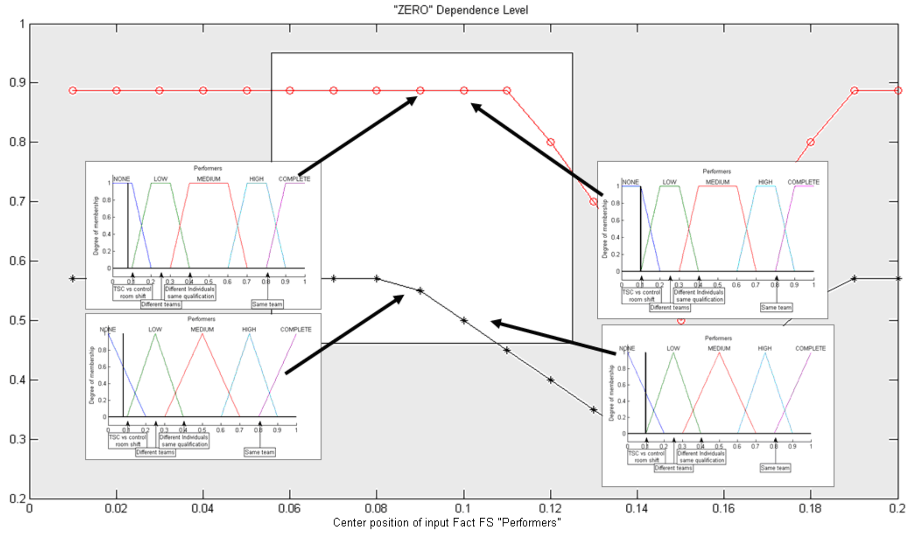


Figure 12. Degree of activation of the dependence level "ZERO" as a function of the singleton Fact "Performers". Circles: trapezoidal input partitioning. Asterisks: triangular input partitioning. The small Figures show the intersection of the singleton "Performers" Fact (at 0.09, left and at 0.1, right) with trapezoidal (top) and triangular (bottom) partitioning of the corresponding UOD.

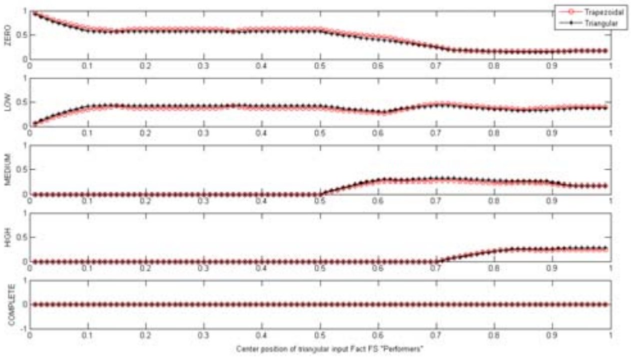


Figure 13. Normalized degree of activation of the dependence levels "ZERO", "LOW", "MEDIUM", "HIGH" and "COMPLETE" as a function of the position of the center of the triangular Fact "Performers" FS. Circles: trapezoidal input partitioning. Asterisks: triangular input partitioning.

6. Model sensitivity to different input Fact FSs

Once the dependence model is fixed, its output depends on the input Fact judgment provided by the analyst. The uncertainty associated to this judgment is represented by the width of the interval supporting the fuzzy MF of the analyst input Fact assessment.

The extreme case of a point estimate judgment, i.e. with no associated ambiguity, leads to the results shown in *Figure 14* and *Figure 15*. The most activated dependence level is still "LOW", as with triangular input Fact FSs (see *Figure 6 – Figure 7*), thus confirming the robustness of the model. Furthermore, the output "LOW" is relatively more pronounced with respect to the other dependence levels, as expected in this less ambiguous assessment by the analyst.

On the contrary, *Figure 16* and *Figure 17* show the effect of a large ambiguity in the analyst assessment, centered at the same point estimates as the previous case analyzed. This ambiguity is clearly propagated to the output which shows almost equally distributed activation of all the dependence levels.

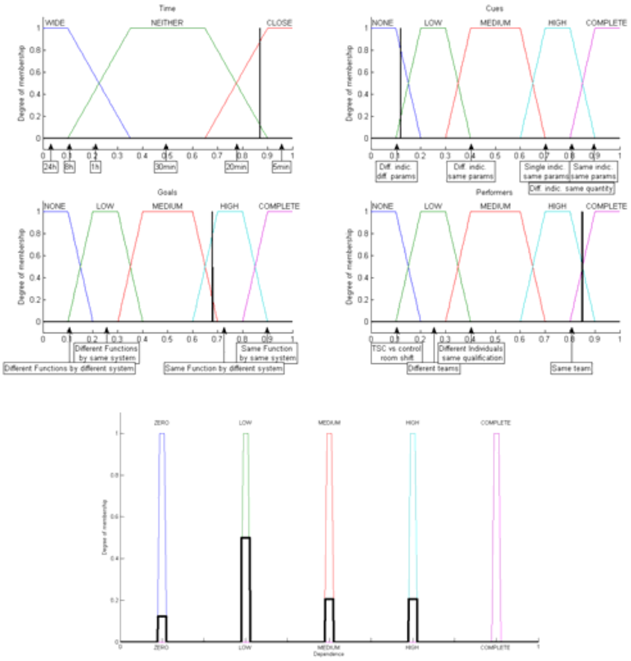


Figure 14. Output discrete FS (right) in correspondence of singleton input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning.

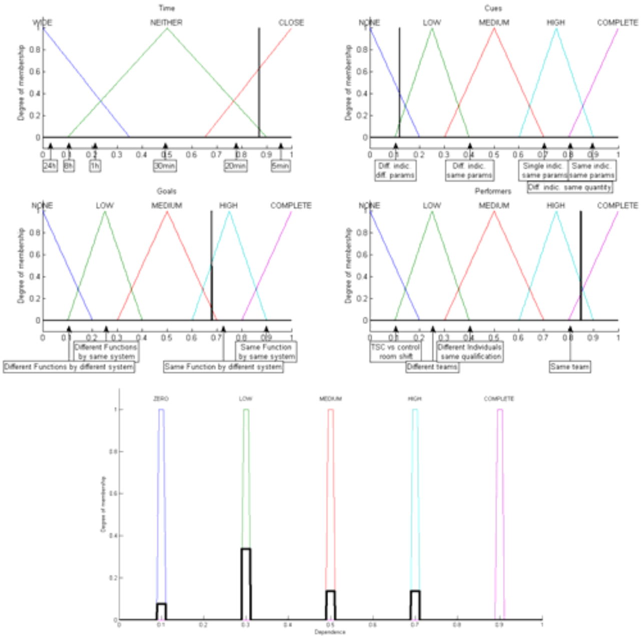


Figure 15. Output discrete FS (right) in correspondence of singleton input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning

Finally, *Figure 18* and *Figure 19* show a case in which the analyst provides only the range where the input Fact may lie, with an equal degree of belief for any points in the range. The support is assumed to be the same of the triangle input Fact FSs used in Section 5 (*Figure 6 – Figure 7*). For this reason, the discrete output FS presents the same number of activated dependence levels as in the case of triangular Fact FSs with the same support.

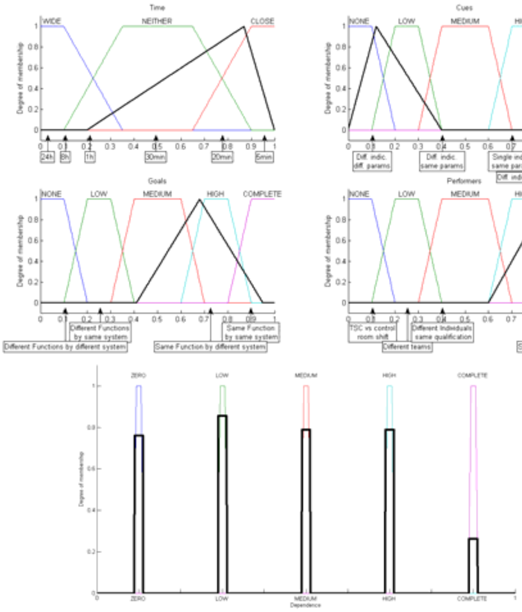


Figure 16. Output discrete FS (right) in correspondence of wide triangle input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning

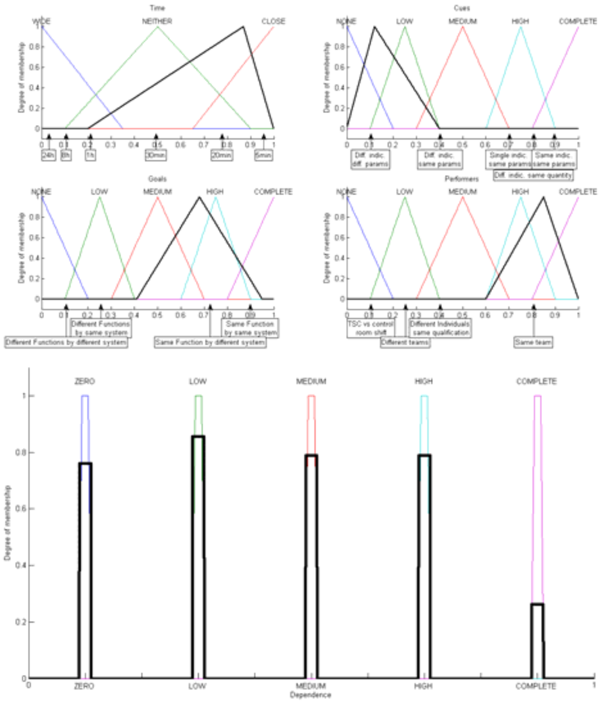


Figure 17. Output discrete FS (right) in correspondence of wide triangle input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning

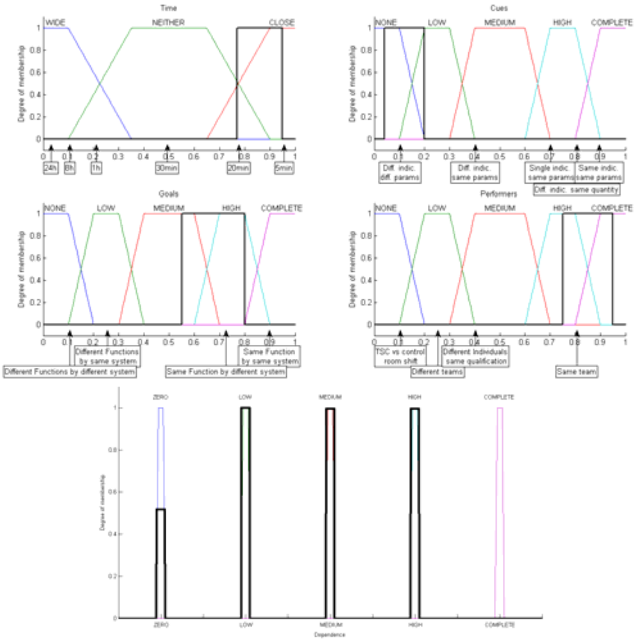


Figure 18. Output discrete FS (right) in correspondence of rectangular input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning

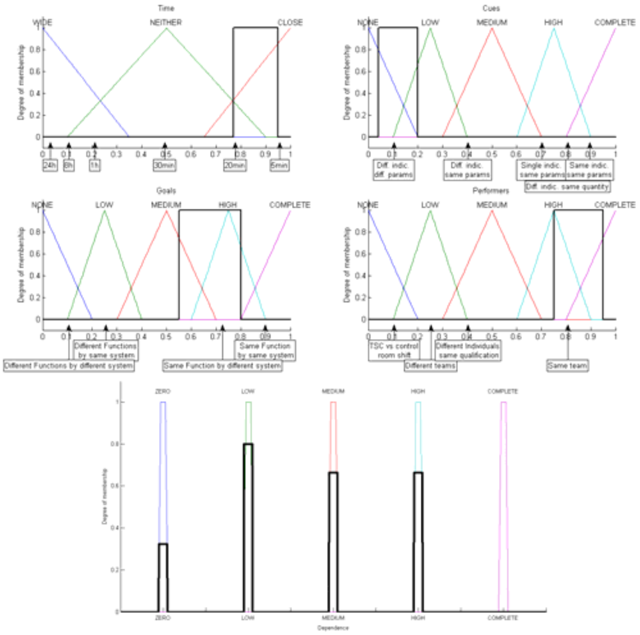


Figure 19. Output discrete FS (right) in correspondence of rectangular input Fact FS (left). Top: trapezoid UODs partitioning. Bottom: Triangle UODs partitioning.

7. Conclusion

In this paper, a fuzzy expert system for the evaluation of the dependence level between operator tasks in an emergency procedure has been considered. The design of the fuzzy expert system rests on an elicitation procedure for the identification of the main relationships between the input factors and the dependence of two successive tasks in correspondence of prototype conditions called anchor points. Then, an interpolation method is used to complete the logical rules necessary for the dependence assessment.

A sensitivity analysis has been performed to investigate the variability of the results obtained with respect to the choice of the input factors UOD partitioning, on a case study regarding the control of the reactor vessel level after the ADS failure in a nuclear reactor. The analysis has shown the robustness and stability of the inferred dependence level in the case considered. A further analysis of the sensitivity with respect to different fuzzy input evaluations by the analyst has been performed. The analyst uncertainty turns out to be properly propagated into the inferred outputs.

Acknowledgements

This work is funded by the Swiss Nuclear Safety Inspectorate (HSK), under DIS-Vertrag Nr. 82610 and by the project Virthualis, (FIS5-1999-00250, funded by the European Union). The views expressed in this article are solely those of the authors.

References

[1] Klir, G. J. & Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic: Theory and Applications.* Prentice Hall.

[2] Konstandinidou, M., Nivolianitou, Z., Kiranoudis C. & Markatos, N. (2006). A fuzzy modeling application of CREAM methodology for human reliability analysis. *Reliability Engineering and System Safety.* Vol.91-6, 706-716

[3] Marseguerra, M., Zio, E. & Bianchi, M. (2004). A fuzzy modelling approach to road transport with application to a case of spent nuclear fuel transport. *Nuclear Technology*. Vol. 146, Issue 3, 290-302.

[4] Marseguerra, M., Zio, E. & Librizzi, M. (2006). Quantitative Developments in the Cognitive Reliability and Error Analysis Method (CREAM) for the Assessment of Human Performance. *Annals of Nuclear Energy* 33, 894–910.

[5] Onisawa, T. (1988). *Fuzzy concepts in human reliability.* M. M. Gupta, T. Yamakawa (Eds.), Fuzzy Logic in Knowledge-Based Systems, Decision and Control, North-Holland, New York.

[6] Swain, A. D. & Guttman, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* NUREG/CR-1278.

[7] Yager, R. R. (1996). Knowledge-based defuzzification. *Fuzzy Sets and Systems*, 80 177-185.

[8] Zadeh, L. A. (1965). Fuzzy sets. *Inform. And Control* 8, 338-353.

[9] Zio, E., Baraldi, P., Librizzi, M., Podofillini, L. & Dang, V. H. *A Fuzzy Expert System for modeling dependence in human operators' errors.* (working paper)

ANALYSIS OF THE SAFETY EFFICIENCY OF A ROAD NETWORK: A REAL CASE STUDY

Zio Enrico, Sansavini Giovanni
Department of Nuclear Engineering, Polytechnic of Milan, Italy

Maja Roberto, Marchionni Giovanna
Department of Industrial Design, of Arts, of Communication and of Fashion, Polytechnic of Milan, Italy

Keywords

complex systems, road networks, safety, vulnerability

Abstract

In this paper, recently introduced topological measures of interconnection and efficiency of network systems are applied to the safety analysis of the road transport system of the Province of Piacenza in Italy. The vulnerability of the network is evaluated with respect to the loss of a road link, e.g. due to a car accident, road work or other jamming occurrences. Eventually, the improvement in the global and local safety indicators following the implementation of a road development plan is evaluated.

1. Introduction

Complexity Science [5], [7]-[8], [10], [15] offers a promising approach to the analysis of technological network systems and infrastructures, such as computer and communication systems [1], [11], [14], power transmission and distribution systems [9], [17], rail and road transportation systems [3], oil/gas systems [3], [4]. The underlying idea is to study the robustness of network systems by analyzing the structure of interconnection of their components (hereafter also called nodes).

In particular, by defining ‘reliability distances’ accounting for the probabilities of failure of the links interconnecting the nodes of the network, global and local reliability efficiency indicators have been introduced for evaluating the network robustness and vulnerability to faults [18].

In this paper, these concepts are extended to the analysis of the safety of a section of the road network of Piacenza Province in Italy. The safety feature of the road sections of the network is analyzed with respect to the probability of car accidents, which depends on the traveling speed and traffic flow. The vulnerability of the network to the loss of a road link can then be evaluated, e.g. due to a blocking car accident, road work or other jamming occurrences. As a result, a ranking of the links is obtained according to their contribution to the decrease of the overall system safety. Eventually, the improvement in the safety global and local indicators following the introduction of a road development plan is evaluated.

The paper is structured as follows. Section 2 briefly introduces the topological and safety indicators used in the analysis of the network system. Section 3 contains the description of the original topology of the Piacenza’s road network and its corresponding abstract graph modeling. The vulnerability analysis is reported in Section 4 together with the effects of modifications to the network topology by a road development plan. Conclusions on the outcomes of the analysis are drawn in Section 5.

4.7

2. Topological and safety efficiency indicators for road networks

Let us consider a network of roads (hereafter also called links or edges, as in graph theory) connecting a number of locations (hereafter also called nodes or vertices, as in graph theory).

From the point of view of the topological characterization of the network, the characteristic path length *L* and the clustering coefficient *C* are typically used to measure the average distance (number of edges) between two generic vertices (a global property of the network topology) and the connectivity of the subgraph formed by each node (a local property of the network topology), respectively [16]. For studying the global properties of the network topology, the probability distribution $P\left(d_{ij}\right)$ of the shortest path lengths d_{ij} between any two nodes i and j in the network can be considered. The shortest path length distribution is synthesized by a point value, the characteristic path length, which represents the average of the shortest distances d_{ij} between all pairs of N nodes in the network

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij} \text{ .} \tag{1}$$

Also the connectivity of the network is typically synthesized at a local level by a single point value, the average clustering coefficient, C The clustering coefficient C_i is a local property of node i defined as follows: if node i has k_i neighbors, then at most $\frac{k_i \cdot \left(k_i - 1\right)}{2}$ edges can exist between them; C_i is the fraction of these edges that actually exist, and C is the average value

$$C = \frac{1}{N} \sum\nolimits_i C_i \text{ .}$$

From the point of view of the characterization of the road safety, the probability of no car accidents p_{ij} (or its complement q_{ij}=1- p_{ij}) on the path γ_{ij} linking the pair of nodes i and j is used. Assuming independence of the accidents occurrence in the various links forming path γ_{ij}, such probability is given by the product of the probabilities of accident on the individual edges of γ_{ij}.
The *safest* path lengths $\{d_{ij}\}$ can be computed as

$$d_{ij} = \min_{\gamma_{ij}} \left(\frac{1}{\prod\limits_{mn \in \gamma_{ij}} p_{mn}} \right) = \min_{\gamma_{ij}} \left(\frac{1}{\prod\limits_{mn \in \gamma_{ij}} \left(1 - q_{mn}\right)} \right), \forall ij \tag{2}$$

where the minimization is done with respect to all paths γ_{ij} linking nodes i and j and the product extends to all the edges of each of these paths [18]. Note that $1 \leq d_{ij} \leq \infty$, the lower value corresponding to the existence of a totally safe path connecting i and j (no accident will occur in the road section from i to j, i.e., $p_{mn} = 1, q_{mn} = 0 \; \forall mn \in ij$) and the upper value corresponding to the situation of no paths connecting i and j (which is equivalent to having in all connections from i to j at least one edge where certainly an accident occurs, $p_{mn} = 0, q_{mn} = 1$).

The safety *efficiency* between nodes i and j is then defined to be inversely proportional to the length of the safest path linking them

$$s_{ij} = \frac{1}{d_{ij}} \; \textit{if there is at least one path connectingi i and j} \tag{3}$$

$$= 0 \; \textit{otherwise} \; (d_{ij} = \infty)$$

The average safety efficiency of the road network **G** is then

$$S_{glob}(G) = \frac{\sum\limits_{i \neq j \in G} s_{ij}}{N(N-1)} = \frac{\sum\limits_{i \neq j \in G} \frac{1}{d_{ij}}}{N(N-1)} \text{ .} \tag{4}$$

This quantity plays a role similar to that of L in defining the network connection characteristics on a global scale, the difference being that it also accounts for the safety of the edges through which the network's nodes are connected. More precisely, whereas the characteristic path length takes into account only the steps required for getting from one node to another through a sequential path along the network, the safety efficiency measure (4) retains also the information about the safety of the path [12]. Since $s_{ij} = 1$ when there is at least one perfect path γ_{ij} in the graph which connects nodes i and j through a sequence of accident-free edges, $S_{glob}(G)$ is equal to one in case of a perfectly connected accident-free network.

As for the local properties of the graph G, these can be quantified by specializing the definition of the average safety efficiency (4) on the subgraph G_i of the k_i neighbors of each node i in the network

$$S(G_i) = \frac{\sum_{n \neq m \in G_i} s_{nm}}{k_i(k_i - 1)}. \tag{5}$$

Averaging the efficiency of the local neighborhoods of all nodes in the network a measure of the network *local safety efficiency* is defined

$$S_{loc}(G) = \frac{1}{N} \sum_{i=1 \in G}^{N} S(G_i). \tag{6}$$

Since $i \notin \mathbf{G_i}$, this parameter reveals how much the road network is fault tolerant in that it shows how safe the connection remains between the first neighbors of i when i is removed.

The quantity defined by (6) has a similar local character as the clustering coefficient C; yet, these two different indicators convey complementary information.

3. Analysis of a real case study

3.1. System description

The road transportation system of the Province of Piacenza depicted in

*Figure **10*** has been modeled as a stochastic, weighted, undirected, connected graph which takes into account its structural, functional and operative features. Each road section is characterized by several features such as typology, i.e. city road, national road or highway, speed limit, traffic capacity, average vehicular flux and average travel speed. Physical points in the network where the road features change, e.g. road junctions and points of road typology change, are defined as nodes.

The road network of N=687 nodes connected by K=789 edges can be represented by a graph G(N, K) defined by its N×N adjacency (connection) matrix $\{a_{ij}\}$ whose entries are 1 if there is an edge joining node i to node j or 0, otherwise.

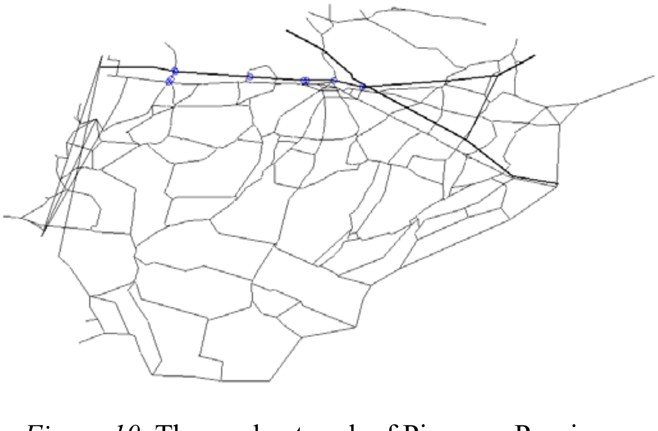


Figure 10. The road network of Piacenza Province.
Highways are represented by thicker lines

It is assumed that car accidents occur along the stretch from node i to node j according to an exponential distribution with constant rate of accident per km, λ_{ij}. Hence, the probability of an accident in the link ij of length l_{ij} is

$$q_{ij} = 1 - e^{\lambda_{ij} \cdot l_{ij}} \, . \tag{7}$$

The accident failure rate λ_{ij} is computed as the product of two factors

$$\lambda_{ij} = u_{ij}\left(v\right) \cdot \alpha_{ij}\left(c\right). \tag{8}$$

where the first factor is the probability per unit distance that an accident occurs when traveling at an average speed v on the stretch of road from node i to node j and the second is a multiplicative factor depending on the average level of traffic congestion c.

As for the first contribution, the accident probability per km is modeled by a sigmoidal function of parameters a_{ij} and b_{ij}

$$u_{ij}\left(v\right) = \frac{1}{1 + e^{a_{ij} \cdot \left(b_{ij} - v\right)}} \, . \tag{9}$$

The reason behind the arbitrary choice of the accident rate (9) lies in the attempt to reproduce the fact that beyond a certain speed the accident probability increases sensibly, mainly due to the decrease in car steering and to the shortening of the reaction time available to the driver to take countermeasures avoiding crashes.

In the specific application which follows, the parameters a_{ij} and b_{ij} have been taken equal for all sections belonging to the same speed limit class; more precisely, the road sections have been divided into the three speed limit classes 50 km/h, 90 km/h and 130 km/h and for each class the parameter values have been set by imposing two constraints on the mean distance to accident $L_{ij} = \frac{1}{u_{ij}}$ in correspondence of two different speeds, as reported in *Table 9* below.

The numbers in *Table 1* have been chosen with the following general philosophy: focusing for example on the 90 km/h speed limit, it is unlikely that an accident occurs if one drives at a speed (e.g. 40 km/h) far below the speed limit but, conversely, accidents become quite likely when driving at a speed doubling the limit (180 km/h). A similar reasoning applies to the cases of 50 km/h and 130 km/h speed limits.

Table 9. Mean distance to accident for different speed limits

Speed limit [km/h]	Mean distance to accident at the speed indicated in parameters	
50	L(30km/h) ~ 70000km	L(150km/h) ~ 6km
90	L(40km/h) ~ 200000km	L(180km/h) ~ 30km
130	L(70km/h) ~ 500000km	L(250km/h) ~ 12km

As for the multiplicative factor α_{ij} accounting for the traffic flow intensity c_{ij} on link ij, it is given by

$$\alpha_{ij} = \frac{\alpha_{MAX} - \alpha_{\min}}{c_{MAX} - c_{\min}} \cdot c_{ij} + 1 \, , \tag{10}$$

where the traffic flow intensity $c_{ij} \in [c_{min}, c_{MAX}]$ is computed as the ratio between the average vehicular flux and the traffic capacity of the road. Note that $\alpha_{ij} \in [\alpha_{min}, \alpha_{MAX}]$, where α_{min} and α_{MAX} are the values taken by α_{ij} in correspondence of the minimum (c_{min}) and maximum (c_{MAX}) value of traffic intensity on the road links of a given speed limit class. In this work, α_{min} and α_{MAX} have been arbitrarily set equal to 1 and 10 for all links, independently of the speed limit class. *Figure 2* shows the behaviour of q_{ij} as a function of v and parameterized on α_{ij}.

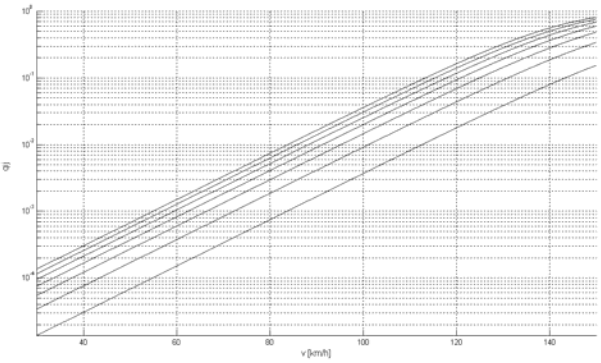


Figure 11. Accident probability q_{ij} as a function of v, for c_{ij} values in the range [0, 1.815]. The curves refer to the case of 50 km/h speed limit and a link of unitary length l_{ij}=1

A limitation of the proposed model is that no relation is accounted for between travel speed and traffic intensity; on the other hand, this is artificially reflected in the data itself which are such that roads with high traffic have a low average travel speed.

3.2. Evaluation of the safety of the road network connection

The values of the topology indicators L and C and of the safety efficiencies of the road network of the Piacenza Province in

Figure 10 are reported in column 2 of *Table 2.* The network degree distribution of *Figure 3* (the distribution *P(k)* of the number of links *k* departing from a node of the network) shows that the predominant series structure of the network connection is responsible for the large number of sparse subgraphs around the nodes, a phenomenon which leads to the small values of the average clustering coefficient and local efficiency.

As a result, if a node is disconnected many nodes become no longer connected to each other by relatively short paths. Thus, the network does not present the desirable small world characteristics of good global and local connectivity. On the other hand, such topological structure of the network reflects solely the change in road typology since, as previously explained in Section 3.1, points of change in the road features, e.g. junctions and points of typology change, are taken as nodes. Actually, only road junctions are significant for the physical connectivity of the network topology whereas typology changes are relevant with respect to the travel and, thus, the safety characteristics of the network. These are quantified by the global and local safety efficiencies which turn out to be very low, the values mainly driven by the serial topology of the network connections, as just explained.

Table 2. Topological indicators *L*, *C* and safety efficiencies $S_{glob}(G)$, $S_{loc}(G)$, for different network configurations. I: original road network; II: road network without the 10 most vulnerable links; III: the original network augmented with the whole road development plan: IV: the original network augmented with the bypass alone

	I (Figure *10*)	II (Figure *10*)	III (*Figure*)	IV (*Figure*)
L	21	∞	19	20
C	$1.06 \cdot 10^{-2}$	$1.12 \cdot 10^{-2}$	$2.20 \cdot 10^{-2}$	$2.08 \cdot 10^{-2}$
$S_{glob}(G)$	$6.61 \cdot 10^{-2}$	$5.68 \cdot 10^{-2}$	$7.24 \cdot 10^{-2}$	$6.89 \cdot 10^{-2}$
$S_{loc}(G)$	$1.15 \cdot 10^{-2}$	$1.22 \cdot 10^{-2}$	$2.31 \cdot 10^{-2}$	$2.19 \cdot 10^{-2}$

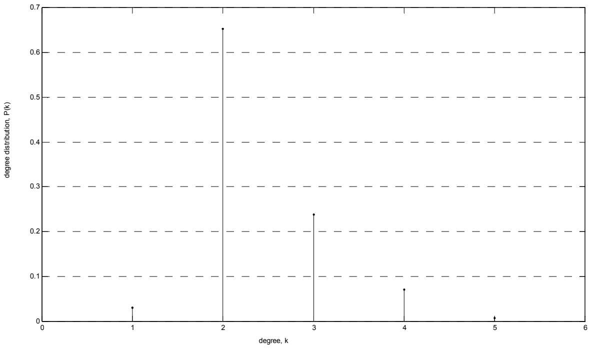


Figure 3. Degree distribution for the road network of *Figure 1*

4. Vulnerability analysis

Further insights in the properties of the road network of *Figure 1* can be inferred from an analysis of the most vulnerable road sections, i.e. those edges most crucial for the safe connectedness of the network [13]. When some edges are unavailable to travel, due to some road blockage, the safest paths between nodes change due to forced detours around the blockages. In this view, the vulnerability of the network is defined in terms of the degradation in the global safety efficiency of the network due to the disconnection, i.e. the interruption, of a set of its road links

$$V^* = \frac{S_{glob}\left(G\right) - S_{glob}\left(G^*\right)}{S_{glob}\left(G\right)}, \tag{11}$$

where G^* is the new graph resulting from G when the disconnected connections are taken out. By construction, V^* takes values in the range [0, 1].

Ranking the links in the network by decreasing vulnerability, it turns out that the 10 most critical roads form the highway path marked with circles in

*Figure **10***. The vulnerability values for these road sections are in the range $\left[2.09 \cdot 10^{-2},\ 3.20 \cdot 10^{-2}\right]$. Taking the whole path of 10 most critical links out of the network leads to the values of topological and efficiency parameters reported in the third column of *Table 2*. First of all, it is not surprising that the characteristic path length becomes infinite, since the nodes previously crossed by the now disconnected path are no longer reachable. Also, when the highway path is disconnected from the rest of the network there is the maximum decrease in global efficiency which stands for an increase in the accident probability in the whole system. This is caused by the need to substitute the missing links with paths along local and secondary streets which are on average longer and less safe. Actually, the vulnerability related to the disconnection of the highway path may even be larger in reality, due to the increase in traffic on the substitute paths. As for the increase in the network local properties (*Table 2*), this is due to the fact that the links deleted are in series in the network and thus bear null contribution to local parameters, whereas they contribute to the averaging in (4) and (6): thus, this increasing is fictitious and meaningless from a physical point of view.

4.1. Evaluation of a road development plan

Let us consider the road development plan concerning the bypass of the town of Piacenza, shown in *Figure 4.*

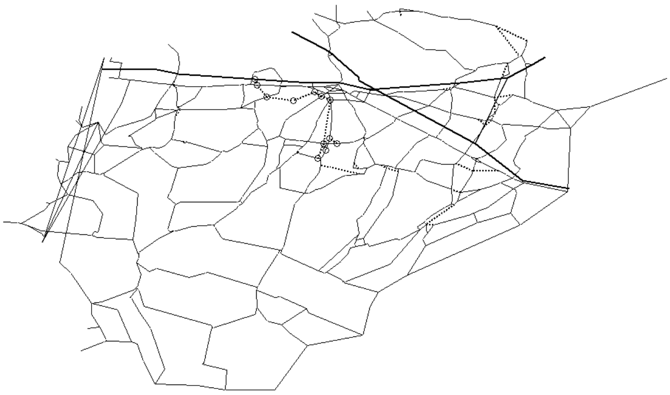


Figure 4. The road network with the bypass development plan: streets are drawn with dotted lines; the bypass is marked with circles.

In the fourth column of *Table 2*, the values of the global and local topological and safety indicators for the road network inclusive of the planned bypass are presented. At a global scale, an increase of 10 percent is noticed in the global safety efficiency, while an increase of 100% occurs at a local scale with respect to the original road network configuration. This was to be expected since the added roads create new alternative paths of increased safety efficiency, i.e. characterized by lower probabilities of car accident.

It is worth noticing that a relevant part of the improvement of the road development plan is due to the bypass (half of the increase in the global safety efficiency and almost the whole improvement in the local efficiency, as shown in *Table 2*, column 5). Consequently, this part should be considered of highest priority when implementing the developed plan.

Eventually, a vulnerability analysis of the augmented network shows that none of the added roads is among the 10 most vulnerable connections and that the maximum vulnerability of a link has decreased with respect to the original scenario ($V^{*} \in \left[1.83 \cdot 10^{-2}, 2.61 \cdot 10^{-2}\right]$, for the 10 most vulnerable connections). Thus, the system has become more resilient to faults in that the increase in accident probability following a road blockage is mitigated by the presence of the bypass.

5. Conclusion

In this paper, recent developments in the study of network systems from the point of view of Complexity Science have been exploited to study the global and local safety features associated to a complex road network. Newly defined, safety *efficiency* measures have been introduced considering the probabilities of car accident along the network interconnecting links. These indicators allow the analysis of the robustness and vulnerability of network systems, for optimal planning and operation.

The proposed approach has been applied to the evaluation of the road network system of the province of Piacenza, Italy. Roads are modelled as edges and points of road feature changes are marked as nodes. The predominant sequential structure of the network leads to a sparse adjacency matrix and affects the global and local connectivity properties in a negative sense. The vulnerability of the network in terms of the degradation of its safety when a road link is blocked has been used for identifying the most vulnerable paths which most contribute to the peril of car accidents.

Eventually, the method has been used to evaluate the safety improvement obtained with the introduction of a given road development plan.

Although the work is methodological in nature, it is of practical relevance that the proposed approach allows bringing the safety features into the analysis of the topology of a road network system.

References

[1] Aggarwal, K. K. (1975). A simple method for reliability evaluation of a communication system. *IEEE Trans Communication*, COM-23, 563-565.

[2] Albert, R., Jeonh, H. & Barabasi, A. L. (2000). Error and Attack Tolerance of Complex Networks, *Nature*, 406, 378-382.

[3] Aven, T. (1987). Availability evaluation of oil/gas production and transportation systems. *Reliability Engineering and System Safety*. 18, 35-44.

[4] Aven, T. (1988). Some considerations on reliability theory and its applications, *Reliability Engineering and System Safety*, 21, 215-223.

[5] Barabasi, A. L. (2002). *Linked: The New Science of Networks*. Perseus Publishing, Cambridge, Massachussetts.

[6] Barabási, A., Albert, R. & Jeong, H. (1999). Mean-field theory for scale-free random networks. *Physica A;* 272, 173-187.

[7] Bar-Yam, Y. (2002). *Dynamics of Complex Systems*. Westview Press.

[8] Capra, F. (1996). *The Web of Life*. Doubleday, New York.

[9] Jane, C. C., Lin, J.S. & Yuan, J. (1993). Reliability evaluation of a limited-flow network in terms of MC sets. *IEEE Trans Reliability*, 42, 354-361.

[10] Kauffman, S. A. (1993). *The Origins of Order*, Oxford University Press.

[11] Kubat, P. (1989). Estimation of reliability for communication/computer networks simulation/analytical approach. *IEEE Trans Communication*, 37, 927-933.

[12] Latora, V. & Marchiori, M. (2001). Efficient Behavior of Small-World Networks, *Physical Review Letters*, 87, N. 19.

[13] Latora, V. & Marchiori, M. (2005). Vulnerability and protection of infrastructure networks. *Physical Review E*. 71, N. 015103.

[14] Samad, M. A. (1987). An efficient algorithm for simultaneously deducing MPs as well as cuts of a communication network. *Microelectronic Reliability*. 27, 437-441.

[15] *Science*, (1999). Special Section on Complex Systems, Volume 284, No. 5411, April 2, pp. 79-109.

[16] Watts, D. J. & Strogatz, S. H. (1998). Collective Dynamics of 'Small-World' Networks. *Nature*, 393, 440-442.

[17] Yeh, W.,C. & Revised, A. (1998). Layered-network algorithm to search for all d-minpaths of a limited-flow acyclic network. *IEEE Trans Reliability*. R-46, 436-442.

[18] Zio, E. From Complexity Science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures, accepted for publication on *International Journal on Critical Infrastructures*.