ELECTRONIC JOURNAL
OF INTERNATIONAL GROUP
ON RELIABILITY

Gnedenko Forum Publications

RELIABILITY:
THEORY&APPLICATIONS

RELIABILITY
RISK ANALYSIS
MAINTENANCE
SAFETY

Vol.1
No.4 (19)
•
December
2010

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

•

ISSN 1932-2321

•

VOL.1 NO.4 (19)
DECEMBER, 2010

San Diego

ISSN 1932-2321

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

RELIABILITY:
THEORY & APPLICATIONS

Vol.1 No.4 (19),
December, 2010

San Diego
2010

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
igusha22@gmail.com

or

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

Table of Contents

ON THE PROBLEMS OF MODELLING AND RELIABILITY ASSESSMENT OF CONSTRUCTION PROJECTS DURATION

S. Biruk, P. Jaskowski

•

Lublin University of Technology, Department of Civil Engineering
and Architecture, Lublin, Poland

e-mail: s.biruk@pollub.pl, p.jaskowski@pollub.pl

ABSTRACT

Construction projects are subject to risk. There are a number of methods that allow the planner to consider the effect of random occurrences on the project performance and to assess the chances of meeting the deadlines defined by the contract. PERT belongs to the most popular methods as it assumes a simple approach to estimating the distribution parameters of random variables (task durations) based on the experience of the planner.

The paper summarises PERT's assumptions on the type and parameters of task duration distributions, task duration independence, and the approach to the analysis of the network model in the function of time. The effects of these assumptions on the project makespan estimate are then examined and illustrated by an example.

1 INTRODUCTION

Duration of construction projects, as well as duration of particular tasks the project scope may be broken down into, is affected by a variety of occurrences whose frequency and impact depend on the project-specific, contractor-specific and location-specific conditions (e.g. Biruk and Jaskowski (2008), Dawood (1997), Jaworski and Biruk (2000), Jaskowski et al. (2010), Nasir et al. (2003), Schatteman et al. (2008)).

Table 1 lists top ten risk factors of the greatest mean impact, greatest mean frequency of occurrence and greatest mean importance (impact times frequency), defined on the basis of a survey among chartered engineers employed by construction companies in Poland.

Standard production rates, being often the basis for planning duration of construction processes, are usually expressed by single values – medians. To determine process duration distribution types and parameters, a considerable number of time measurements would be necessary to make the results statistically sound. This might be too costly, time consuming and in some cases unjustified as, due to the unique character of construction projects and processes, statistical data from the past may be of little use in the future.

Many models have been proposed to describe and predict activity / project durations or work produktivity on the basis of risk analysis. According to the way of describing the risk factors impact on activity duration, two groups of methods can be distinguished: quantitative and qualitative. The qualitative models use a verbal description of the impact. The quantitative models base on analytical or numerical relations; there exist simple analytical (e.g. Neil and Knack (1984), Woodward (2003), Ovarain and Popescu (2001), Jergeas and McTague (2002)), neural network (e.g. Kog et al. (1999), Chua et al. (1997), Zayed and Halpin (2005), Shi (1999), AbouRizk et al. (2001), Sonmez and Rowings (1998)), Bayesian belief network (Nasir et al. (2003)), fuzzy set (e.g. Lee and Halpin (2003), Perera and Imriya 2003)), regression (e.g. Hanna and Gunduz (2005), Jaselskis and Ashley (1991)) and simulation models (e.g. Dawood (1997), Schatteman et al. (2008)) to choose from. Most of the quantitative models assume that particular factors affect the processes independently. However, no model is considered to be superior as providing more reliable solutions than the other models. This is so because there are no reliable methods of comparing the results obtained by means of these models. Moreover, no comparative studies on the ease of application of these models in practice have been conducted.

Table 1. Ranking of risk factors, based on local experts' opinion survey

Rank	Hierarchy of factors according to:		
	impact (*i*)	frequency of occurence (*f*)	importance (*i·f*)
1	Contractor's cash flow problems	Winter affecting structural works, facade works and external works	Winter weather affecting structural works, facade works and external works
2	Delay of preceding works (Delays in subcontractors' works)	Precipitation affecting structural works, facade works and external works	Precipitation affecting structural works, facade works and external works
3	Winter affecting structural works, facade works and external works	Mistakes and discrepancies in design documents	Delay of preceding works (Delays in subcontractors' works)
4	Precipitation affecting structural works, facade works and external works	Shortage of skilled labour	Shortage of skilled labour
5	Unforeseen ground conditions causing change of substructure works scope and quantity	Variations of works (scope and quantity) due to design changes	Mistakes and discrepancies in design documents
6	Client's low speed of decision-making	Delay of preceding works (Delays in subcontractors' works)	Client's low speed of decision-making
7	Inexperienced / unreliable subcontractors	Demotivating remuneration system	Variations of works (scope and quantity) due to design changes
8	Poor site management and supervision	Client's change of requirements	Demotivating remuneration system
9	Work stoppage according to inspection agencies order	Difficulty with finding subcontractors	Client's change of requirements
10	Delay with design (if delivered in packages)	Client's low speed of decision-making	Difficulty with finding subcontractors

The existing models find application in predicting duration of particular construction processes, groups of works and whole projects and than enable project timing and scheduling.

The measure of project schedule reliability level, R, is the probability of the project's being completed no later than at the contractually agreed completion date, t:

$$R = P(T \le t). \tag{1}$$

Due to the complexity of production processes in construction, the organization structure of the project team may be variable (Jaskowski (2008)). Harmonizing the work of all project participants at the planning stage is thus a complex task. To allow for all constraints and conditions, the planner would have to solve complex mathematical problems (Biruk and Jaskowski (2008), Jaworski and Biruk (2000)). In the practice of construction, simplified, but still reliable enough models are in demand.

The first attempt to allow for risks in project planning was made by the inventors of *PERT* (Program Evaluation and Review Technique). In spite of far going simplifications that inevitably affect reliability of results, the method stays popular in project management.

2 PERT ASSUMPTIONS ON DISTRIBUTION TYPE AND PARAMETERS OF TASK DURATION RANDOM VARIABLE

The authors of *PERT* assumed that the duration of a process (i.e. a task of a network model) is a random variable of beta distribution. The probability density function of a standardized beta distribution ($x \in [0, 1]$) with parameters $\alpha > -1$ and $\beta > -1$ is:

$$f(x) = \begin{cases} \dfrac{\Gamma(\alpha+\beta+2)}{\Gamma(\alpha+1)\Gamma(\beta+2)} x^{\alpha}(1-x)^{\beta}, & 0 < x < 1, \\ 0 & \text{for other } x. \end{cases} \tag{2}$$

The shape of the probability distribution function depends on the values of the shape parameters α and β and the relation between them. As observed in real life, the function representing a production process distribution is usually unsymmetrical and positively skewed. Another assumption concerns the standard deviation (Littlefield and Randolph (1987)): it is postulated that it equals one sixth of the range of the variable (as for the normal distribution), which implies that $\alpha + \beta = 4$. This assumption is difficult to accept, and its only justification seems to be this three-sigma empirical rule.

The distribution parameters of a process duration are determined on the basis of three estimates, given by a group of experts or a planner considering project risk analysis. These estimates are: optimistic (t_a), pessimistic (t_b), and most likely duration (t_m) that is considered to be the mode of the process duration distribution.

Applying a linear transformation $T = t_a + (t_b - t_a)X$ to the random variable of density function described by Equation 2, one obtains the following formulas that describe expected value and standard deviation of the process duration *T*:

$$E(T) = \mu = \frac{t_a + 4t_m + t_b}{6}, \tag{3}$$

$$D(T) = \sigma = \frac{t_b - t_a}{6}. \tag{4}$$

Figure 1 presents probability density function plots of three variables of beta distribution. All of them positively skewed ($0 \le m \le 0{,}5$), but of considerably different standard deviations. All of them could be approximations of the actual distribution of a process duration (MacCrimmon and Ryavec (1964)). The curve marked as D_1 corresponds to the distribution assumed by *PERT*. Its expected value is $\mu_1 = 1/6(4m+1)$, and standard deviation is $\sigma_1 = 1/6$. The curve D_2 represents a distribution close to a uniform distribution ($\mu_2 \approx 0{,}5$, $\sigma_2 \approx \sqrt{1/12}$). The parameters of the distribution D_3 are $\mu_3 \approx m$ and $\sigma_3 \approx 0$. For D_3, the maximum absolute error of the mean relative to the estimate as used by *PERT* is (MacCrimmon and Ryavec (1964)):

$$max\left\{\left|\frac{1}{6}(4m+1) - \frac{1}{2}\right|, \left|\frac{1}{6}(4m+1) - m\right|\right\} = \frac{1}{3}(1-2m),$$

and the maximum absolute error of the standard deviation is (MacCrimmon and Ryavec (1964)):

$$max\left\{\left|\sqrt{\frac{1}{12}} - \frac{1}{6}\right|, \left|0 - \frac{1}{6}\right|\right\} = \frac{1}{6}.$$

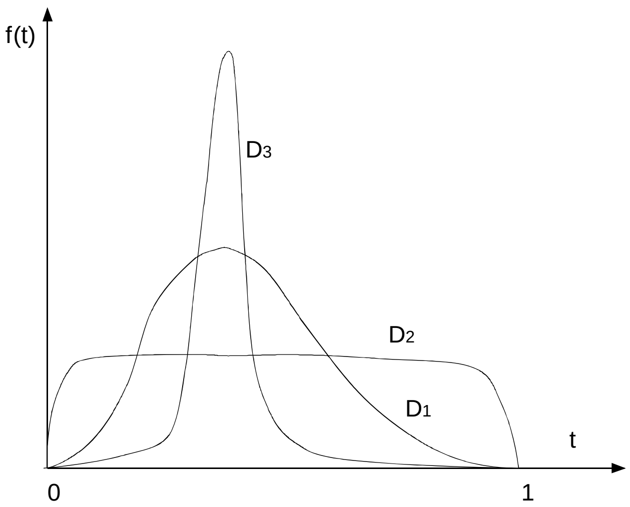


Figure 1. Examples of density functions of beta distribution defined on the interval [0 , 1]

Considering the fact that the actual distribution of a process duration may be significantly different from that assumed by *PERT*, the errors may propagate along the paths of the network model, increasing or decreasing the total error (Hon-Siang and Somarajan (1995)). Elimination of the mean's and standard deviation's errors can be achieved by increasing the number of estimates being predefined quantiles of the process duration. Usually, 7 quantiles are used, e.g. $T_{0.01}, T_{0.125}, T_{0.25}, T_{0.50}, T_{0.75}, T_{0.875}, T_{0.99}$. With so many estimates, one can determine the probability function's shape parameters α and β with precision by means of the least squares method. This approach gives more accurate results than the classic *PERT* three estimates approach because more input is available, and the input is considered to be more accurate: the experts giving estimates are reported to be more accurate with estimates closer to the mode or the mean than to the extreme values (Lichtenstein et al. (1982)).

Three quantiles are sufficient to calculate the parameters of a beta distribution. These could be e.g. $T_{0.05}, T_{0.50}, T_{0.95}$ (Cox (1995)), so no difficult to estimate extreme values are needed. Keefer and Verdini (1993) provided a numerical proof that, in most cases, following formulas are adequate for estimation of the mean and standard deviation of a beta distribution:

$$\mu = 0.630\,T_{0.50} + 0.185\left(T_{0.05} + T_{0.95}\right), \tag{5}$$

$$\sigma^2 = 0.630\left(T_{0.50} - \mu\right)^2 + 0.185\left(T_{0.05} - \mu\right)^2 + \left(T_{0.95} - \mu\right)^2. \tag{6}$$

Estimates (5) and (6) by Pearson and Tukey (1965) generate smaller errors than estimates (3) and (4) of the classic *PERT*.

The experts' opinions on the pessimistic, optimistic and modal duration have a considerable impact on the error of distribution parameter estimates. If the input is to be given by a group of experts, it is advisable to use the median and not the mode of their opinions to reduce the error.

3 PERT ASSUMPTIONS OF THE ANALYSIS OF A NETWORK MODEL IN THE FUNCTION OF TIME

PERT assumes that the expected value of the project duration and its variance equal, respectively, the sum of expected durations and the sum of variances of the critical processes. However, this assumption is statistically sound only if the random variables being added are independent and if a process starts after only one of its predecessors has finished.

If a process start is conditioned by a number of predecessors' being completed, the distribution of the random variable of the event that represents the successor's start becomes a complex problem (described by e.g. Cox (1995) and Clark (1961)). Therefore, PERT networks are often analysed by means of the *Monte Carlo* simulation.

The problem is illustrated by the following example (network model presented in Figure 2) where the problem consists in estimating the early start of the event 4.

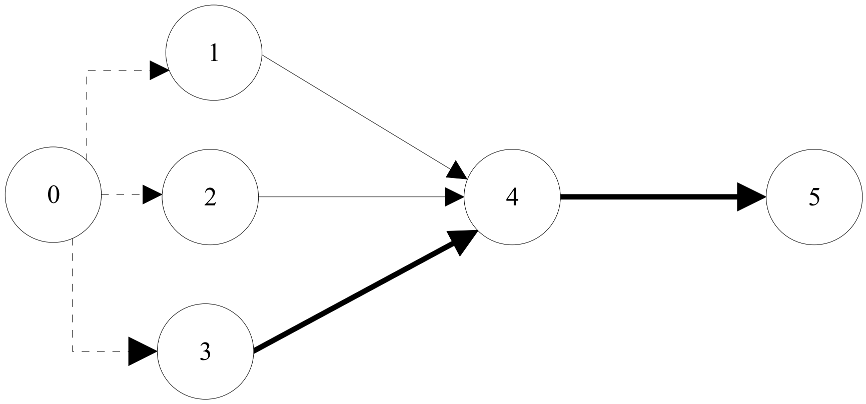


Figure 2. Example: predecessors of a process 4-5 (activity on arrow model)

In the example, the durations of processes were assumed to be random variables of beta-*PERT* distribution, and that their parameters were calculated on the basis of three estimates: optimistic, modal and pessimistic (respectively t_a, t_m, t_b):

– t_{1-4} : t_a =16, t_m =22, t_b =40,
– t_{2-4} : t_a =10, t_m =15, t_b =40,
– t_{3-4} : t_a =23, t_m =24, t_b =29.

Table 2 lists values of each process duration provided by means of a random number generator. Event 4 earliest occurrence is possible when all the predecessors of the process 4-5 have been completed. For 20% of possible cases, the moment of event 4 is not decided by the duration of the critical process 3-4.

Table 2. Generated process durations (example)

Run	t_{1-4} ($\mu = 24, \sigma = 4$)	t_{2-4} ($\mu = 18{,}33, \sigma = 5$)	t_{3-4} ($\mu = 24{,}67, \sigma = 1$)	Earliest occurrence of event 4
1	21,00	15,98	**24,30**	24,30
2	24,02	**27,52**	23,39	27,52
3	18,47	12,51	**23,04**	23,04
4	**30,18**	17,34	25,66	30,18
5	22,83	11,57	**26,35**	26,35
6	25,03	17,80	**26,24**	26,24
7	21,45	18,97	**24,65**	24,65
8	19,48	17,97	**25,42**	25,42
9	25,25	24,32	**25,31**	25,31
10	21,76	10,50	**25,93**	25,93
11	21,00	15,98	**24,30**	24,30

If the duration of all processes on a critical path is substantially greater than the duration of the processes on the other paths that connect the project network's start and finish nodes, the interaction of processes at network "sinks" (as illustrated in Figure 2) is not strong and *PERT* may provide accurate results (Jaworski and Biruk (2000)). In the other case, neglecting the analysis of non-critical paths may lead to serious underestimation of the project finish date.

The exact calculation of the probability of not exceeding the project's due date may be done by means of a formula:

$$P(T \le t) = 1 - \left[P(T_1 > t) + P(T_1 \le t \wedge T_2 > t) + \ldots + P(T_1 \le t \wedge T_2 \le t \wedge \ldots \wedge T_{n-1} \le t \wedge T_n > t) \right], \quad (7)$$

where T is the random variable of project duration and T_i is the random variable of duration of processes on the path i ($i = 1, 2, \ldots, n$).

Calculating the probabilities is a complex task. Therefore, practical application of Equation 7 is limited.

The *PERT*'s formulas for calculating distribution parameters of the project duration are correct only under assumption of independence of durations of critical processes. In real life, there are a number of factors, such as weather, that may affect a number of parallel processes in the same way, so the variables of process durations may be positively correlated. A positive correlation may occur between durations of processes executed by the same subcontractor. It is also possible that a negative correlation occurs – an example would be shifting limited resources from non-critical to critical tasks to assure that project due date is met, which may cause delays of non-critical processes.

Furthermore, according to the central limit (Lindeberg's) theorem, *PERT* assumes that the random variable that represents the project duration is of normal distribution as a sum of random variables being durations of critical tasks. The normal distribution would be an adequate approximation of the project duration distribution if the number of critical processes is large enough (more than 30, but smaller numbers as 20 or 10 are also accepted by practitioners). However, the accuracy of the probability estimation of meeting a project due date is conditioned by not only the number of critical processes, but also similarity of process duration distribution types.

3 EXAMPLE

Figure 3 presents a network model for the case study – a modernisation project of a partly two-storey, post and beam structured building. The number of critical processes is 15. Table 3 lists the tasks of the work breakdown structure together with their duration estimates.

The project expected duration and standard deviation calculated according to *PERT* are $\mu = 291.83, \sigma = 4.78$, respectively.

In order to verify the accuracy of the results, a Monte Carlo simulation. The project duration mean of 10000 simulations was $\mu = 291.54$, and the standard deviation was $\sigma = 5.53$.

Figure 4 compares the cumulative probability density functions: the one obtained in the course of simulations, and the one of a normal distribution and parameters established by PERT. The maximum error of duration estimate at the predefined reliability level is less than three working days, which is about 1% of the project duration. This accuracy level seems more than adequate for practical engineering applications.

3 CONCLUSIONS

PERT is a simple tool that supports planning projects carried out in random conditions, and, as such, often used in practice. The assumptions of *PERT* made it possible to reduce the complexity of network model analyses but, at the same time, affected the accuracy of time estimates of individual project events and the project as a whole. Understanding these assumptions allows the planner to interpret the results of *PERT* calculations and to prepare more reliable project programmes.

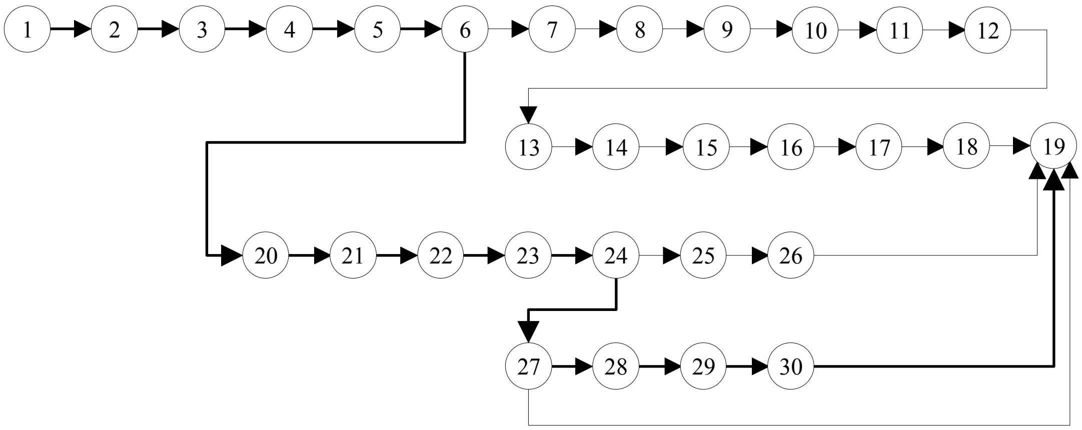


Figure 3. Case study project network model

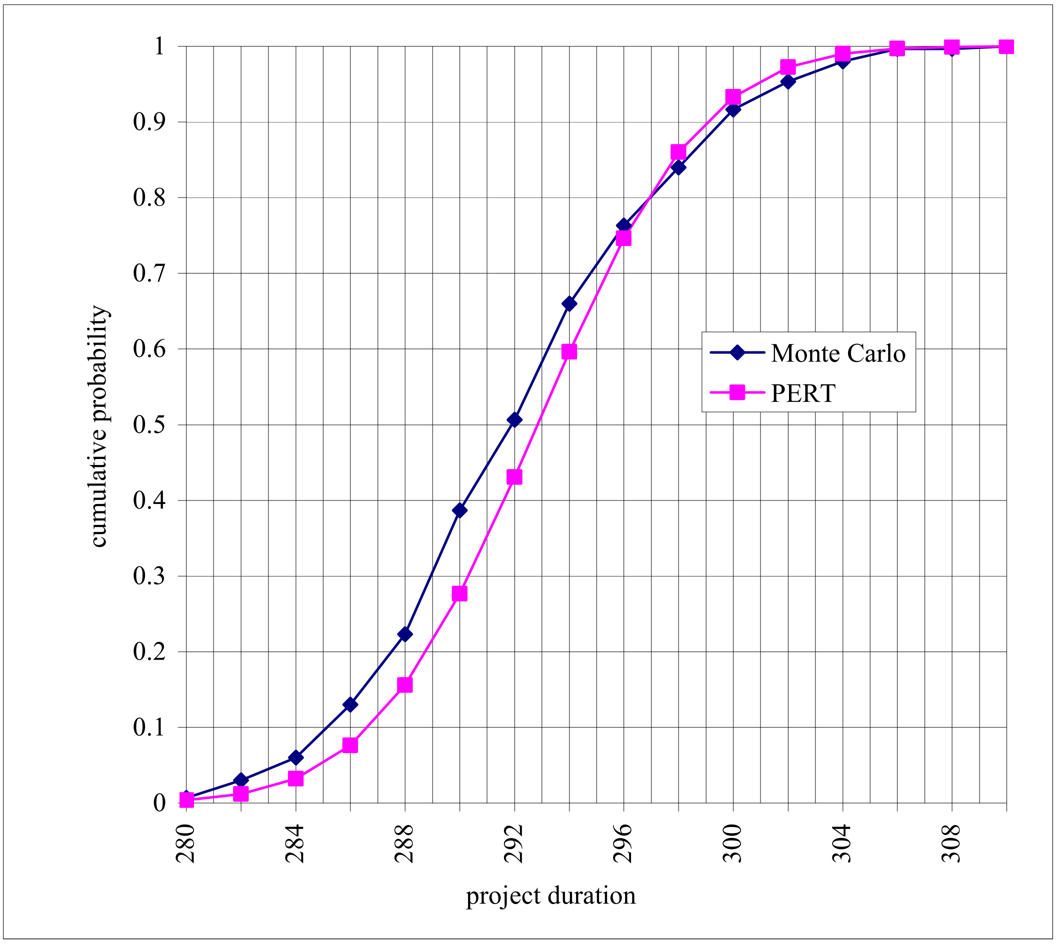


Figure 4. Cumulative probability distribution: simulation based and according to PERT

Table 3. Case study project tasks with estimates of optimistic, most likely and pessimistic durations, in working days

Activity	Activity title	t_a	t_m	t_b
1–2	Removing floor finishings, plastering and wall claddings	57	62	70
2–3	Demolition of partition walls	9	12	17
3–4	Dismantling steel structures	5	6	8
4–5	Dismantling aluminium structures	1	2	3
5–6	Demolition of RC structure elements	5	6	8
6–7	Assembling supproting structures for AC units	3	4	6
7–8	Assembling precast concrete elements	2	3	4
8–9	Earthworks - trenches	6	8	11
9–10	RC foundations	3	4	5
10–11	RC stairs and plates	1	2	3
11–12	Substructure waterproofing	3	4	6
12–13	Backfill	2	3	4
13–14	Dismantling elements of roof cladding with gutters and downpipes	1	2	3
14–15	Roof cladding	2	3	4
15–16	Thermal insulation of external walls and substructure	55	59	65
16–17	Roof gutters and downpipes	10	13	16
17–18	External cladding	5	6	8
18–19	Landscaping works	1	2	3
6–20	Partition walls	5	6	8
20–21	Steel gates and doors, aluminium facades, partitions and doors	5	6	8
21–22	PVC windows	3	4	5
22–23	Plastering	34	37	43
23–24	Internal wall cladding	34	37	45
24–25	Underfloor insulation	3	4	5
25–26	Subfloors	1	2	3
26–19	Floor tiling	31	34	39
24–27	Painting	30	34	40
27–28	Suspended ceilings, plasterboard claddings and partitions	60	66	75
28–29	Internal doors	4	5	7
29–30	Assembly of awnings	1	2	3
30–19	Heater screens	2	3	4
27–19	Other floor finishes	42	48	56

ACKNOWLEDGMENTS

The paper is based on the research sponsored by the Polish Ministry of Science and Higher Education (grant N N506 254637).

REFERENCES

AbouRizk S., Knowles P., Hermann U. R. 2001. Estimating labor production rates for industrial construction activities. *Journal of Construction Engineering and Management* 127(6): 502-511.

Biruk S., Jaskowski P. 2008. Simulation modelling construction project with repetitive tasks using Petri nets theory. *Journal of Business Economics and Management* 9: 219-226.

Chua D.K.H., Kog Y.C., Loh P.K., Jaselskis E.J. 1997. Model for construction budget performance-neural network approach. *Journal of Construction Engineering and Management* 123(3): 214-222.

Clark C.E. 1961. The greatest of finite set of random variables**.** *Operations Research* 9: 145-162.

Cox A.A.A. 1995. Simple normal approximation to the completion time distribution for a PERT network. *International Journal of Project Management* 13: 265-270.

Dawood N. 1998. Estimating project and activity duration: a risk management approach using network analysis. *Construction Manngement and Economics* 16: 41-48.

Hanna A.S., Gunduz M. 2005. Early warning signs for distressed projects. *Canadian Journal of Civil Engineering* 32(5): 796-802.

Hon-Siang L., Somarajan C. 1995. A proposal on improved procedures for estimating task-time distribution in PERT. *European Journal of Operational Research* 85: 39-52.

Jaworski K.M., Biruk S. 2000. A model of construction project based on Petri nets theory. *Archives of Civil Engineering* XLVI: 71-82.

Jaselskis E.J., Ashley D.B. 1991. Optimal allocation of project management resources for achieving success. *Journal of Construction Engineering and Management* 117(2): 321-340.

Jaskowski P. 2008. Designing the structure of a construction project operating system using evolutionary algorithm. *Archives of Civil Engineering* LIV: 371-394.

Jaskowski P., Biruk S., Bucoń R. 2010. Assessing contractor selection criteria weights with fuzzy AHP method application in group decision environment. *Automation in Construction* 19: 120-126.

Jergeas G., McTague R. 2002. Construction productivity: an auditing and measuring tool. *AACE International Transactions* CS91-CS104.

Keefer D.L., Verdini W.A. 1993. Better estimation of PERT activity time parameters. *Management Science* 39: 1086-1091.

Kog Y.C., Chua D.K.H., Loh P.K., Jaselskis E.J. 1999. Key determinants for construction schedule performance. *International Journal of Project Management* 17(6): 351-359.

Lee S., Halpin D.W. 2003. Predictive tool for estimating accident risk. *Journal of Construction Engineering and Management* 129(4): 431-436.

Lichtenstein S., Fischhoff B., Philips L. 1982. *Calibration of probabilities: the state of the art to 1980*. In: Kahneman D., Slovic P., Tversky A. (ed.). *Judgement under uncertainty: heuristics and biases*. New York: Cambridge University Press.

Littlefield T.K., Randolph P.H. 1987. Reply an answer to Sasieni's question on PERT times. *Management Science* 33: 1357–1359.

MacCrimmon K. R., Ryavec C. 1964. An analytical study of PERT assumptions. *Operational Research* 12: 16-37.

Nasir D., McCabe B., Hartono L. 2003. Evaluating risk in construction-schedule model (ERIC-S): construction schedule risk model. *Journal of Construction Engineering and Management* 129(5):518-527.

Neil J.M., Knack L.E. 1984. Predicting Productivity. *AACE International Transactions* H.3.1-H.3.8.

Ovararin N., Popescu C. 2001. Field factors affecting masonry productivity. *AACE International Transactions* ES91-ES97.

Pearson E.S., Tukey J.W. 1965. Approximate means and standard deviations based on distances between percentage points of frequency curves. *Biometrics* 52: 533-546.

Perera A., Imriya K. 2003. Knowledge-based system for construction cost control. *AACE International Transactions* IT101-108.

Schatteman D., Herroelen W., Van de Vonder S., Boone A. 2008. Methodology for integrated risk management and proactive scheduling of construction projects. *Journal of Construction Engineering and Management* 134(11): 885-893.

Shi J. J. 1999. A neural network based system for predicting earthmoving production. *Construction Manngement and Economics* 17: 463-471.

Sonmez R., Rowings J.E. 1998. Construction labor productivity modeling with neural networks. *Journal of Construction Engineering and Management* 124(6): 498-504.

Woodward C. 2003. Project productivity analysis: what is 1.0? *AACE International Transactions* ES11-ES15.

Zayed T.M., Halpin D.W. 2005. Pile Construction Productivity Assessement. *Journal of Construction Engineering and Management* 131(6): 705-714.

ASSESSMENT OF THE EFFECT OF LARGE - CAPACITY UNITS ON RELIABILITY OF RUSSIA'S UNIFIED POWER SYSTEM

G.F. Kovalev, L.M. Lebedeva
•
Energy Systems Institute, Siberian of the Russian Academy of Sciences,
Irkutsk, 130, Lermontov Street, 664033, Russia
e-mail: kovalev@isem.sei.irk.ru

ABSTRACT

Methodical approaches to study on the problem of using large-capacity units are substantiated. Based on the multi-variant calculations of adequacy of Russia's Unified power system (UPS), that were carried out by the software package "YANTAR", the conclusions were drawn that the use of large-capacity units is feasible in terms of capacity increase and admissible in terms of system reliability.

Problem characteristics

The major factor that fosters the use of generation units of increasingly larger capacity in electric power systems is cost effectiveness which implies a decrease of specific construction and operation costs due to the improvement of efficiency at electricity generation, reduction of specific consumption of primary energy resource and decrease in the number of personnel per unit of installed capacity [1–3]. However, objectively there are factors that reduce to a certain extent the economic benefits of large-capacity units. These are:

- the increase of negative consequences due to security-related failures, since the units of large and super large capacity contain much greater potential energy reserves that can be released and do harm during emergencies. Neutralizing the negative impacts naturally requires additional efforts and expenses;
- the statistical data on operation of units of various capacities shows that the capacity growth raises the probability of emergency downtime q:

$$q = \frac{\tau_r}{T_o + \tau_r},$$

largely due to increase of time for unit restoration after failures τ_r; T_o – operating time between failures. Figure 1 presents graphically the dependence $q = f(P_{unit})$, where P_{unit} is capacity of a unit (based on [1]);

- the rise in capacity of generation units is also accompanied by decrease in their availability factor K_a:

$$K_a = \frac{T_{cal} - \tau_r - \tau_{pl}}{T_{cal}}$$

due to increase of both duration of restoration time τ_r, and duration of downtime in the planned maintenances τ_{pl} over the considered calendar period T_{cal} (normally a year). For example, K_a for 100–150 MW units makes up 0.85–0.9, and for 1000 MW units – 0.7–0.75;

– the capacity increase of every generation unit causes rise in the required generation capacity reserves [1].

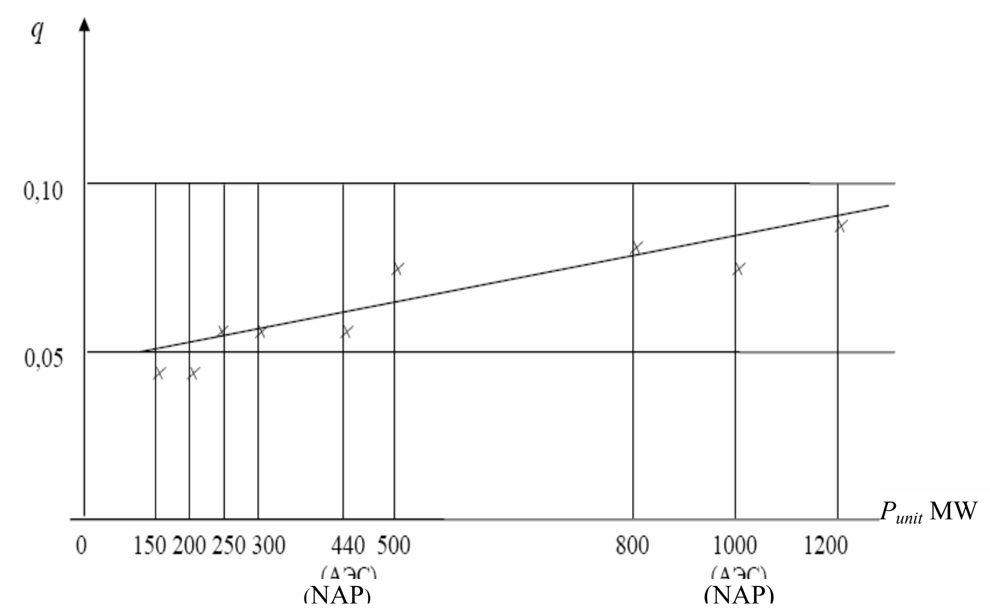


Fig. 1. Emergency rate indices for units of various capacities

Technical and economic conditions for reliable operation of electric power systems are such that the question of appropriate capacity of every generation unit directly depends on capacity of the entire system. It is known that the larger the generation unit capacity the greater the reserve capacity is necessary to provide the required reliability of power supply. This can be shown by a simple example.

Assume that the power required to cover the load is 100 MW. The reliability level is standardized by the deficit-free operation probability equal to 0.999. There is a possibility to install 10, 25, 50 and 100 MW units. The calculated values of the required installed capacity for these conditions and available capacities of every generation unit are summarized in Table 1. It is assumed that the emergency rate of units q=0.1 and no less than one unit should be periodically removed from service for maintenance (current or capital) [4].

As seen from Table 1 rise in the unit capacity from 10 to 100 MW calls for increase in reserve capacity by 300–70 = 230 MW in order to maintain the required level of reliable system operation.

The reliability analysis also shows that an increase in power system capacity leads to rise in the rational capacity of every generation unit. However, it should be understood that this analysis is much more complicated than that demonstrated above by the elementary example. It requires employment of the entire set of negative and positive, technical and economic factors related to the capacity growth of every generation unit in a system.

Table 1. Calculated values of the required number of units at load P_l=100 MW, reliability level **P**≥0.999 and various capacities of units

CAPACITY OF GENERATION UNITS P_{UNIT}, MW	REQUIRED NUMBER OF UNITS N, PCS.	INSTALLED CAPACITY P_{INS}, MW	DESIGN RELIABILITY INDEX P*	VALUE OF RESERVE $P_{res} = P^g_{ins} - P^l_{\max}$, MW
10	**17**	**170**	**0.99950**	**70**
25	**9**	**225**	**0.99962**	**125**
50	**6**	**300**	**0.99954**	**200**
100	**4**	**400**	**0.99900**	**300**

*Deviations from **P**=0.999 are related to the integer nature of the problem solved.

In the past two decades in power systems of Russia and other countries along with a tendency towards increase in the capacity of generation units an opposite tendency has emerged towards construction of the so called distributed generation in large power systems, i.e. small-capacity generation which is placed at load nodes. The dialectical combination of the two tendencies makes it possible to maintain alone with economical efficiency a high level of power supply reliability and thus, to a great extent, mitigates the negative impacts of using large-capacity generation units. However, based on the expert estimates [6] the total capacity of distributed generation will not exceed 7–8 % of the total capacity in the system, i.e. the larger part of system capacity will consist of generators of medium, large and extra-large (above 1000–1500 MW) capacity.

The level of system reliability that depends, as was already mentioned, on the generation and network reserves of power systems, in many countries is standardized as a reliability index , i.e. the probability of deficit-free power system operation. In the former USSR this value was equal to 0.996 which corresponded to 35 hours of power system operation a year with power deficit $(P^l > P^g_{ay})$. In developed Western countries this value is assumed to be 0.9996 (3.5 *h*/year). In Russia, in the context of unfolding the "Concept…" [5] there are suggestions to use this value in the UPS of Russia at the level of 0.9991 (7.9 *h*/year).

The results of reliability calculations for Russia's UPS with large-capacity generation units

Initial calculated variant of Russia's UPS expansion, 2020.

The basic variant for 2020 [6] was assumed to be the initial variant. The considered scheme consists of 7 interconnected power systems (IPSs) and 9 tie lines connecting them, Fig.2. The reliability calculations were made by the software package "YANTAR" [7]. The software package "YANTAR" allows a more detailed representation and consideration of power system but at this stage of work we will confine ourselves to the level of interconnected power system.

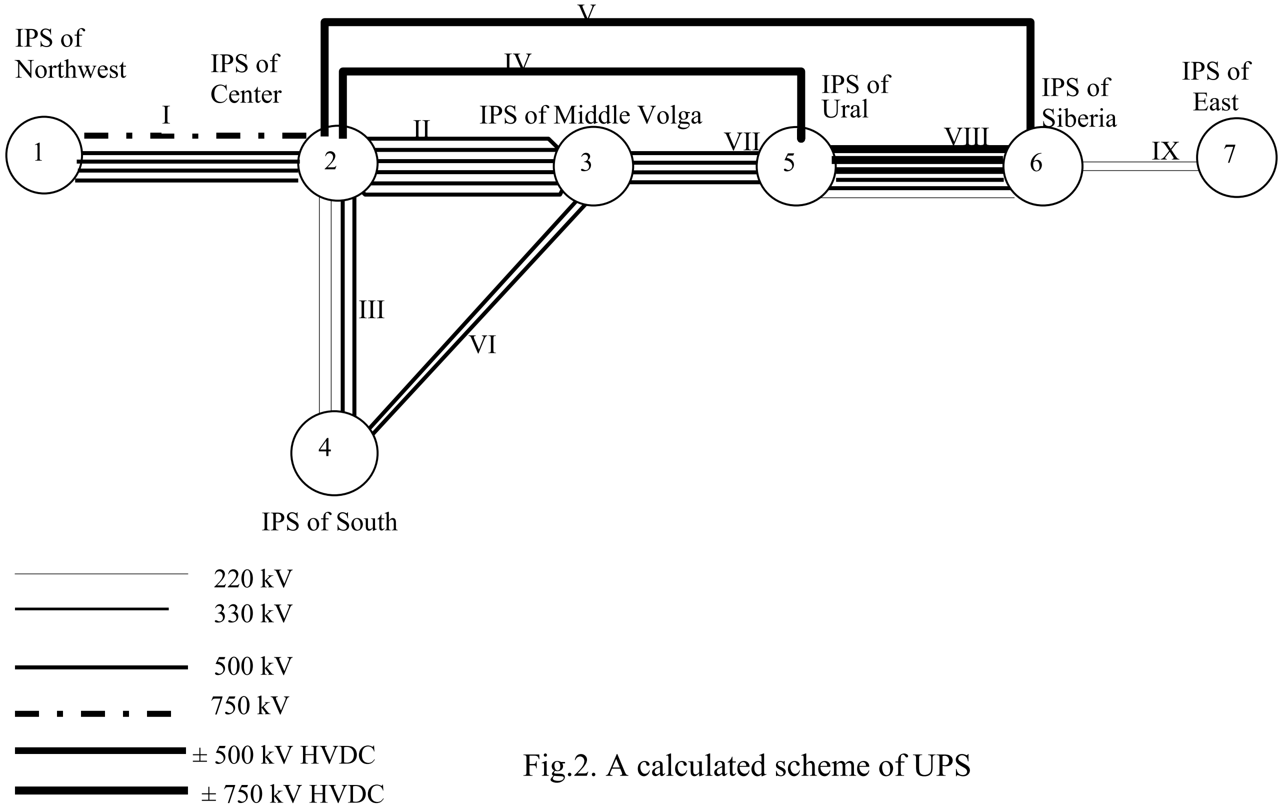


Fig.2. A calculated scheme of UPS

The major parameters of IPSs are presented in Table 2.

The transfer capabilities of tie lines connecting the interconnected power systems are presented in Table 3.

The load of nodes includes auxiliaries, export and trans-boundary power exchanges. The installed generation capacity of nodes differs from the available one by the value of underused power plant capacities and technology constraints.

The results of reliability assessment of the basic variant of Russia's UPS expansion till 2020, suggested in [6], are presented in Table 4.

Analysis of the results shows that the basic variant supposes a high margin of system reliability which is determined by the rated reserve of generation capacity and transfer capabilities of tie lines.

There are good grounds to suppose that the UPS expansion strategy was created by supporters of self-balancing in regional IPSs, therefore, some benefits of the UPS as a single electric power space of the country were ignored. One of the benefits is, first of all, a decrease in generation capacity reserves at a set (standard) level of power supply reliability.

Table 4 shows that in all interconnected power systems the reliability indices **P** in the suggested variant of expansion considerably exceed the standard value (0.9996) assumed in developed countries.

Table 2. Main parameters of IPSs, 2020

NODE NUMBER	IPS	REQUIRED ELECTRICITY OUTPUT E_R, BILLION KWH	LOAD MAXIMUM $P^l_{\max}$, MW	INSTALLED CAPACITY P_{INS}, MW	AVAILABLE CAPACITY, P_{AV}, MW	FULL SYSTEM RESERVE, R_{FULL}, MW
1	NORTHWEST	177.8	29960	35400	33130	3170
2	CENTER	409.1	72000	83500	80560	8560
3	MIDDLE VOLGA	115.9	19470	27100	24170	4700
4	SOUTH	120.2	20665	26100	23850	3185
5	URAL	415.4	60730	65400	62510	1780
6	SIBERIA	376.4	55835	79400	72000	16165
7	EAST	84.3	13850	15780	14864	1014
UPS		1699.1	267967	332680	311084	43117

The study on Russia's UPS reliability with a 1800 MW pilot unit installed in the IPS of Ural, 2020 (for* P = 0.9996*).

For this case in the initial variant of expansion part of capacity of newly constructed power plants with units of relatively small capacity, was replaced by a 1800 MW double-unit installed at one of the Ural nuclear power plants. This unit was assumed to be a pilot one and according to the recommendations [1] should be characterized by higher unreliability as compared to the large-scale production of equipment. Besides, it was assumed in the calculations that reliability characteristic of the double-unit is represented by the distribution series of three unit states with their probabilities (Table 5).

Table 3. Transfer capabilities of tie lines, 2020

CONNECTED NODES (IPS) NUMBER (NAME)	TRANSFER CAPABILITIES (MW), DIRECTION	
	DIRECT	REVERSE
1 (NORTHWEST) – 2 (CENTER)	3600	3600
2 (CENTER) – 3 (MIDDLE VOLGA)	3500	3500
2 (CENTER) – 4 (SOUTH)	2000	2000

2 (Center) – 5 (Ural)	**6000**	**6000**
2 (Center) – 6 (Siberia)	**5700**	**5700**
3 (Middle Volga) – 4 (South)	**1500**	**1500**
3 (Middle Volga) – 5 (Ural)	**2500**	**2500**
5 (Ural) – 6 (Siberia)	**12850**	**12850**
6 (Siberia) – 7 (East)	**900**	**900**

Table 4. Calculated reliability of the initial UPS expansion variant, 2020

Node number	**IPS**	**Probability of deficit-free operation P, p.u**	**Coefficient of consumer provision with electricity π^{*}, p.u.**	**Electricity undersupply E_{und}, MWh**	**Total system reserve in % of load maximum $P^{l}_{\max}$, IPS**
1	**Northwest**	**0.999966**	**0.999999**	**193.2**	**10.58**
2	**Center**	**0.999999**	**0.999999**	**1.5**	**11.89**
3	**Middle Volga**	**0.999999**	**0.999999**	**0**	**24.14**
4	**South**	**0.999977**	**0.999999**	**84.4**	**15.41**
5	**Ural**	**0.999999**	**0.999999**	**4.3**	**2.93**
6	**Siberia**	**0.999999**	**0.999999**	**0**	**28.95**
7	**East**	**0.999983**	**0.999999**	**0**	**7.3**
UPS (without IPS of East)		**0.999942**	**0.999999**	**283.4**	**16.06**

* $\pi = E_a / E_r = (E_r - E_{und}) E_r$.

Table 5. Probability distribution series of the 1800 MW unit states

Production	**Full failure, 0 MW**	**Failure of either half of the unit, 900 MW**	**Full availability, 1800 MW**
Pilot unit	**0.035**	**0.090**	**0.875**
Commercial units	**0.025**	**0.075**	**0.900**

The resulting reliability calculations for this variant of UPS expansion are presented in Table 6.

The specific feature of the calculations made is the fact that the compared variants differ only in the parameters of a small part of generation capacity (in this very case 1800 MW out of 62510 MW in Ural, i.e. only 2.88 %). The analysis can reveal only whether the calculated reliability is higher or lower than the rated level. Changes in the indices of fault-free operation in the 5th – 6th digit after the point and mathematical expectation of undersupply at the level of hundreds of megawatt- hours are comparable with an error in calculations (3–5 %) that are determined on the basis of Monte Carlo method for choosing the system states by the random number generator. Calculation of operation conditions with the accuracy up to 1 MW, the computer and algorithmic rounding of calculation results, etc. do not naturally allow a quantitative conclusion on higher or lower reliability of compared variants based only on the difference in the last two-three significant figures of the results (including calculated electricity undersupply).

In addition to this fact it should be noted that the probability of deficit-free operation of UPS as a whole that represents a sum of deficit-free states of individual IPSs incurs little information. In this context the probability of deficit-free state of UPS $\boldsymbol{P}_{\text{UPS}}$ will always be no less than the minimum probability among all probabilities for IPSs, i.e.

$$\boldsymbol{P}_{\text{UPS}} \le \boldsymbol{P}_{\text{IPS}\,min}.$$

One should bear in mind the presented comments when analyzing the obtained results of reliability calculations.

Based on the above comments Tables 4 and 6 show that commissioning of the unit 2×900 = 1800 MW does not cause a noticeable decrease of reliability: probabilities of deficit-free operation change in the 5th – 6th digit after the point and still remain much higher than the standard value equal to 0.9996.

Moreover, if the 1800 MW unit is represented as a single-unit with the emergency rate q=0.125, calculations of UPS reliability have not resulted in essential decrease of system reliability, i.e. the probability of deficit-free operation of all IPSs remained above 0.9996. The system reliability was also calculated for the initial conditions of UPS expansion, when the 3000 MW single-unit with q_{unit} = 0.135 was installed in IPS of Ural. In this case the design reliability index was not below 0.9996. (The calculation results of reliability for the variants with the single-units of 1800 and 3000 MW are not given in the paper by virtue of obvious impossibility to manufacture units with such characteristics by 2020).

Table 6. Calculation results of reliability of Russia's UPS expansion variant at installation of the 1800 MW unit in IPS of Ural, 2020.

Node number	IPS	Probability of deficit-free operation P, p.u.	Coefficient of consumer provision with electricity π, p.u.	Electricity undersupply $Э_{нед}$, MWh	Full system reserve in % of maximum load $P^{l}_{\max}$, IPS
1	North-West	0.999964	0.999999	182.0	10.58
2	Center	0.999999	0.999999	0	11.89
3	Middle Volga	0.999999	0.999999	0	24.14

4	**SOUTH**	**0.999976**	**0.999999**	**96.7**	**15.41**
5	**URAL**	**0.999996**	**0.999999**	**87.4**	**2.93**
6	**SIBERIA**	**0.999999**	**0.999999**	**0**	**28.95**
7	**EAST**	**0.999980**	**0.999999**	**0**	**7.30**
UPS (WITHOUT IPS OF EAST)		**0.999936**	**0.999999**	**366.1**	**16.06**

From the reliability standpoint the problem of sudden failure of the whole 1800 MW unit by some reason is of interest. The main criteria for admissibility of such a failure are:

– frequency decrease not below an admissible level for the emergency situation in the system;

– inadmissibility of overloading the tie lines at redistribution of power flows in the network because of abrupt tripping of the unit;

– probability of the event occurrence at the period most dangerous for system operation.

Analysis of the considered situation leads to the following conclusions. Since for UPS the droop of load with respect to frequency $K_f = \Delta P / \Delta f$ lies in the range 1–2, i.e. generation decrease (load growth) by 1–2 % leads to a 1 % frequency decrease [8], then at failure of the whole unit (1800 MW) a relative value of decrease in load covering during its maximum will make up $P_{unit} / P^{l}_{\max} = (1800/267967)\cdot 100 = 0.67$ %.

In this case a relative frequency decrease in UPS will reach at the initial instant of sudden tripping of the 1800 MW unit:

$$\overline{\Delta f} = \frac{\Delta P}{K_f} = \frac{0.67}{1 \div 2} = 0.670 \div 0.335 \text{ \%},$$

which corresponds to the frequency decrease by

$$\Delta f = (0.670 \div 0.335)\frac{50}{100} = 0.335 \div 0.168 \text{ Hz}.$$

As is known, at system failure the frequency decrease is assumed to be up to 49.5 Hz, i.e. $\Delta f_{dec} = 0.5$ Hz. Hence, an abrupt tripping of the whole 1800 MW unit is admissible. Since the control range of power plants supporting frequency in UPS should not be lower than 1–2 % (the so-called spinning reserve) during the maximum load, which exceeds the relative unit capacity 0.67 %, the frequency will decrease for a rather short term.

Frequency variation in UPS by 0.05–0.1 Hz and more (see [9]) changes the backbone network operation so much that it leads, as a rule, to a dangerous change in power flows over the majority of tie lines between IPSs and possible splitting of UPS by weak ties. In the case of ineffective operation of emergency control devices parallel operation will also be violated over the relatively strong tie lines.

Calculation of load flow for the event of the 1800 MW unit tripping in IPS of Ural has shown that transfer capabilities of tie lines accepted in "The General Scheme of development" [6] ensure an admissible distribution of flows for the studied conditions.

In accordance with the basic concepts of the probability theory the probability of the whole unit tripping at the most critical time of UPS operation, namely during the maximum load without capacity reserves in the system is determined as follows

$$\boldsymbol{P}_{dang} = \boldsymbol{P}_{unit} \cdot \boldsymbol{P}_{\max} \cdot \boldsymbol{P}_{def},$$

where $\boldsymbol{P}_{unit} = 0.035$ – emergency probability with complete failure of the unit (see Table 5); $\boldsymbol{P}_{\max}$ –

probability for UPS to be under maximum daily load (for 1 hour a day) $\boldsymbol{P}_{\max} = 1/24 = 0.042$; $\boldsymbol{P}_{def}$ – probability of a deficit state of UPS:

$$\boldsymbol{P}_{def} = 1 - \boldsymbol{P}_{norm} \leq 1 - 0.9996 = 0.0004.$$

Then $\boldsymbol{P}_{dang}$, i.e. the probability of a *dangerous* state, is very low (at a level of probability of a sudden natural disaster):

$$\boldsymbol{P}_{dang} = 0.035 \cdot 0.042 \cdot 0.0004 = 0.0000006.$$

Thus, it is safe to assume that the use of 1800 MW units is quite admissible in terms of reliability at the current stage of Russia's UPS expansion (even without consideration of its joint operation with other EPSs of the NIS and European countries).

Calculation results of Russia's UPS reliability for particular conditions of system expansion.

The above analysis was an official variant of Russia's UPS expansion to be considered as an optimistic variant. The crisis conditions, however, can essentially influence a development pattern of the national economy as a whole and electric power industry, in particular. Therefore, it seems appropriate to analyze admissibility of putting large units into operation during the period 2020–2030, supporting power supply reliability at the lower level $\mathbf{P} = 0.996$. Consider the most severe conditions, when power consumption levels remain at the former level, but the available generation capacity considerably reduces from 311084 MW (see Table 2) to 287380 MW. In this case the capacity reserve to maintain $\mathbf{P} = 0.996$ will be equal to 19413 MW.

For these heavier conditions different variants for commissioning of large units in different regions of UPS were studied:

1. Commissioning of a 3500 MW single-unit in IPS of Ural.
2. Commissioning of one 1800 MW double-unit in IPS of Ural and one – in IPS of Center and two double-units in IPS of North-West.
3. Commissioning of one 1800 MW double-unit in IPS of Ural and two double-units in IPS of North-West and three – in IPS of Center.

The variants were compared with reliability of the initial variant (without commissioning of large units). The calculation results have shown that the full reserve available in UPS at a level of 7.6 % of the coincident annual maximum of load in the considered variant proves to be sufficient for UPS reliability support at the given level, when in accordance with variants 1–3 large units are put into operation instead of traditional ones of lower capacity. Hence, it is possible to conclude that for Russia's UPS use of the units from 1800 to 3500 MW does not cause an essential reliability decrease.

General conclusions on the results of studies on system reliability of Russia's UPS at commissioning of the units 1800–3000 MW for 2020 and 2030.

1. The calculations have shown that the presented variants of using large units in the schemes of Russia's UPS expansion for the time period till 2020 (one pilot unit in IPS of Ural), four and even six units after 2020 in different IPSs virtually do not decrease an assumed system reliability in the General Scheme [6].
2. It should be noted that in reliability calculations account was taken first of all of unfavorable factors of using large units. At first an "isolated" operation of Russia's UPS was studied. Based on the parallel work of UPS with power systems of Baltic states, Belarus, Ukraine, Kazakhstan, Tajikistan, etc. conditions for using large units would be even more favorable by virtue of both an essential growth of system capacity and a weak effect of random failure of the whole unit capacity on UPS.
3. The study also shows that failure of the 1800 MW unit at the most unfavorable time of UPS operation (at maximum load with no generation capacity reserves in the system) has a

probability of about 10^{-7}, which corresponds to probability of a rare natural disaster, such as earthquake, volcanic eruption, hurricane, etc. A simultaneous failure of two and more units is practically excluded as an improbable event.

4. Additional calculations have also revealed that the use of single-units with the capacity up to 3500 MW is admissible in Russia's UPS in the years 2020–2030.

* * *

Thus, from the system reliability considerations the use of large units up to 3500 MW in Russia's UPS for the time horizon 2020–2030 is surely admissible and expedient. Moreover, for economic efficiency reasons it can be recommended with confidence to design both double-units and single-units with a capacity of 3000–3500 MW for their application during the period 2030–2050.

The study performed assesses only system adequacy of UPS. However, later on the study on operating condition reliability for Russia's UPS should be carried out in terms of stability of parallel operation and transients [10].

The suggested technique and model can be applied for similar studies in other systems.

References

[1] Manual on power system design. / Ed. by S.S. Rokotyan and P.M. Shapiro. – M.: Energoatomizdat, 1985. – 352 p. (in Russian)

[2] Kinney R. Siting energy facilities. Translation from English. – M.: Energoatomizdat, 1983. – 320 p. (in Russian)

[3] Sullivan R. Power system planning. Translation from English. – M.: Energoizdat, 1982. – 360 p. (in Russian)

[4] Recommended practices in design of energy system expansion. Approved by Order No. 281 of the Russian Ministry of Energy of 30.06.2003. – 39 p. (in Russian)

[5] The concept of reliability support in electric power industry. Adopted by RAO EES Rossii of 27.12. 2004. – 48 p. (in Russian)

[6] The general scheme of electric power objects placement up to 2020. – M.: Minpromenergo, 2007. − 240 p. (in Russian)

[7] Kovalev G.F., Lebedeva L.M. A model for reliability estimation of electric power systems for long-term planning of their operation. // Elektrichestvo. 2000. No. 11. P. 17–24. (in Russian)

[8] Markovich I.M. Energy system operating conditions. M.-L.: Gosenergoizdat, 1969. – 352 p. (in Russian)

[9] Sovalov S.A. Operating conditions of Unified energy system. – M.: Energoatomizdat, 1983. – 384 p. (in Russian)

[10] Reliability of energy systems (Collection of recommended terms). – M.: Information-Analytical Center "Energiya", 2007. – 192 p. (in Russian)

A RELIABILITY MODEL FOR "SAFETY SYSTEM-PROTECTED OBJECT" COMPLEX WITH MULTIPLE SAFETY SYSTEMS

A. I. Pereguda, D. A. Timashov

•

Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia

e-mail: pereguda@iate.obninsk.ru

ABSTRACT

The paper presents a new reliability model for "safety system-protected object" complex with multiple safety systems. It is supposed that the complex consists of one protected object and multiple independent safety systems with complex structures. Scheduled periodic inspections of safety systems are also taken into account. Asymptotic estimates of the mean time to accident and the probability of the accident prior to time t are obtained under some assumptions on operation process of the complex.

1 INTRODUCTION

Hazardous facilities use a variety of systems concerned with safety, with safety systems being the most important of those. Safety systems are provided to detect potentially dangerous protected object failures or conditions and to implement appropriate safety actions. Protected object may have several types of hazardous deviations of protected object operation process that require their own safety systems. Some reliability models for the elements of safety systems were introduced by Hansen and Aarø (Aarø & Hansen 1997), Corneliussen and Hokstad (Corneliussen & Hokstad 2003), Høyland and Rausand (Høyland & Rausand 2004). In this paper we propose a different approach to reliability assessment of "safety system-protected object" complex based on asymptotic properties of alternating renewal processes.

In the present study we set out to analyze the reliability of the automated "safety system-protected object" complex with multiple safety systems. Systems of such kind are quite common in the nuclear power engineering, because safety systems of nuclear power plant should employ diversity in the detection of fault sequences and in the initiation of the safety system action to terminate the sequences. We follow Pereguda (Pereguda 2001) in assuming that the operation of the complex can be described using a superposition of alternating renewal processes. Our objective is to provide an asymptotic estimation for such reliability indices as the mean time to accident and the probability of the accident prior to time t.

2 MODEL DESCRIPTION

Let us consider an automated complex of protected object and N safety systems. Safety systems and the protected object are repairable. They are restored to an as-good-as-new state. All failures are supposed to be independent. Let j-th safety system consists of M_j subsystems and k-th subsystem of j-th safety system consists of $C_{j,k}$ elements.

By $\chi_{i,j}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$ denote the time to the i-th protected object failure detected by j-th safety system. Let $\chi_{i,j}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$ be independent random variables and for each fixed j let $\chi_{i,j}$, $i=1,2,\ldots$ be identically distributed random variables with CDF $F_{\chi_j}(t)$. By $\gamma_{i,j}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$ denote the time to the protected object repair after it's i-th failure detected by j-th safety system. Let $\gamma_{i,j}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$ be independent random variables and for each fixed j let $\gamma_{i,j}$, $i=1,2,\ldots$ be identically distributed random variables with CDF $F_{\gamma_j}(t)$. Suppose that moments of the protected object repair are renewal points of the operation process of the complex. Suppose that $F_{\chi_j}(t)$ and $F_{\gamma_j}(t)$ are nonlattice distributions with finite mean. By $\xi_{i,j,k,l}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$, $k=1,2,\ldots,M_j$, $l=1,2,\ldots,C_{j,k}$ denote the time to the i-th failure of the l-th element of the k-th subsystem of the j-th safety system. Let $\xi_{i,j,k,l}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$, $k=1,2,\ldots,M_j$, $l=1,2,\ldots,C_{j,k}$ be independent random variables and for each fixed j, k, l let $\xi_{i,j,k,l}$, $i=1,2,\ldots$ be identically distributed random variables with CDF $F_{\xi_{j,k,l}}(t)$. Suppose that safety system elements are repaired only after corresponding safety subsystem failure is detected. By $\eta_{i,j,k}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$, $k=1,2,\ldots,M_j$ denote the time to repair of the k-th subsystem of the j-th safety system after it's i-th failure. Let $\eta_{i,j,k}$, $i=1,2,\ldots$, $j=1,2,\ldots,N$, $k=1,2,\ldots,M_j$ be independent random variables and for each fixed j, k let $\eta_{i,j,k}$, $i=1,2,\ldots$ be identically distributed random variables with CDF $F_{\eta_{j,k}}(t)$. Suppose that moments of the safety subsystem repair are renewal points of the operation process of the safety subsystem. Suppose that $F_{\xi_{j,k,l}}(t)$ and $F_{\eta_{j,k}}(t)$ are nonlattice distributions with finite mean. A failure of the safety subsystem may be detected immediately or only during scheduled periodic inspections of the safety subsystem. By $T_{j,k}$ denote the period of scheduled inspections of the k-th subsystem of the j-th safety system. By $\theta_{j,k}$ denote the duration of scheduled inspections of the k-th subsystem of the j-th safety system. The safety subsystem may be active or inactive during the inspection. Suppose that each safety system is coherent system (Høyland & Rausand 2004) and each safety subsystem is coherent system. Let $\varphi_{j,k}(x_{j,k,1}, x_{j,k,2}, \ldots x_{j,k,C_{j,k}})$ denote the system structure function of the k-th subsystem of the j-th safety system and let $\psi_j(x_{j,1}, x_{j,2}, \ldots, x_{j,M_j})$ denote the system structure function of the j-th safety system. Let ν be a random number of renewal intervals of the operation process of the complex before an accident. By ω denote the time to accident. An accident takes place when safety systems are unable to detect the protected object failure. Our aim is to estimate the mean time to accident $M\omega$ and the probability $\Pr(\omega \le t)$ of the accident prior to time t.

2 MAIN RESULTS

2.1 Mean time to failure and reliability function

Since the operation process of the complex is a superposition of alternating renewal processes, it follows that

$$\omega = \sum_{i=1}^{\nu-1}\Big(\min(\chi_{i,1}, \chi_{i,2}, \ldots, \chi_{i,N}) + \gamma_{i,1} J_{\chi_{i,1} < \min(\chi_{i,2}, \chi_{i,3} \ldots, \chi_{i,N})} + \gamma_{i,2} J_{\chi_{i,2} < \min(\chi_{i,1}, \chi_{i,3} \ldots, \chi_{i,N})} + \ldots + \gamma_{i,N} J_{\chi_{i,N} < \min(\chi_{i,1}, \chi_{i,2} \ldots, \chi_{i,N-1})}\Big) + \min(\chi_{\nu,1}, \chi_{\nu,2}, \ldots, \chi_{\nu,N}),$$

where J_A is an indicator function of the event A. By α_i denote the time to i-th failure of the protected object. By β_i denote the time to i-th repair of the protected object. We obviously have

$$\alpha_i = \min(\chi_{i,1}, \chi_{i,2}, \ldots, \chi_{i,N})$$

and

$$\beta_i = \gamma_{i,1} J_{\chi_{i,1} < \min(\chi_{i,2}, \chi_{i,3} \ldots, \chi_{i,N})} + \gamma_{i,2} J_{\chi_{i,2} < \min(\chi_{i,1}, \chi_{i,3} \ldots, \chi_{i,N})} + \ldots + \gamma_{i,N} J_{\chi_{i,N} < \min(\chi_{i,1}, \chi_{i,2} \ldots, \chi_{i,N-1})}.$$

Therefore

$$F_\omega(t) = \Pr(\omega \le t) = \Pr\left(\sum_{i=1}^{\nu-1}(\alpha_i + \beta_i) + \alpha_\nu \le t\right)$$

and

$$\Pr(\nu = n) = q(1-q)^{n-1},$$

where q is the probability of accident during a renewal interval $\left[\sum_{i=1}^{r}(\alpha_i + \beta_i), \sum_{i=1}^{r+1}(\alpha_i + \beta_i)\right)$, $\forall r \in \{0,1,2,\ldots\}$. Applying the Laplace-Stieltjes transform to $F_\omega(t)$, we obtain

$$\widetilde{F}_\omega(s) = E\left[e^{-s\omega}\right] = \sum_{n=1}^{\infty} E\left[e^{-s\omega} \mid \nu = n\right]\Pr(\nu = n)$$

where $\widetilde{F}_\omega(s) = \int_0^\infty e^{-st} dF_\omega(t) = E\left[e^{-s\omega}\right]$. We see that

$$E\left[e^{-s\omega} \mid \nu = n\right] = E\left[e^{-s\left(\sum_{i=1}^{\nu-1}(\alpha_i+\beta_i)+\alpha_\nu\right)} \middle| \nu = n\right] = \left(\widetilde{F}_\alpha(s)\right)^n \left(\widetilde{F}_\beta(s)\right)^{n-1}.$$

Note that

$$F_\alpha(t) = 1 - \prod_{j=1}^{N}\left(1 - F_{\chi_j}(t)\right)$$

and

$$F_\beta(t) = \sum_{j=1}^{N} F_{\gamma_j}(t) \int_0^\infty \left(\prod_{\substack{r=1 \\ r\ne j}}^{N}\left(1 - F_{\chi_r}(x)\right)\right) dF_{\chi_j}(x).$$

Finally,

$$\widetilde{F}_\omega(s) = \sum_{n=1}^{\infty}\left(\widetilde{F}_\alpha(s)\right)^n\left(\widetilde{F}_\beta(s)\right)^{n-1} q(1-q)^{n-1} = \frac{q\widetilde{F}_\alpha(s)}{1-(1-q)\widetilde{F}_\alpha(s)\widetilde{F}_\beta(s)}.$$

Since $E[\omega] = -\left.\frac{d\widetilde{F}_\omega(s)}{ds}\right|_{s=0}$, it follows that

$$E[\omega] = E[\alpha] + \frac{1-q}{q}\left(E[\alpha] + E[\beta]\right),$$

where

$$E[\alpha] = \int_0^\infty \left(\prod_{j=1}^{N}\left(1 - F_{\chi_j}(t)\right)\right) dt$$

and

$$E[\beta] = \sum_{j=1}^{N}\int_0^\infty \left(1 - F_{\gamma_j}(t)\right)dt \int_0^\infty \left(\prod_{\substack{r=1 \\ r\ne j}}^{N}\left(1 - F_{\chi_r}(t)\right)\right) dF_{\chi_j}(t).$$

Applying a limit theorem for recurrent point processes with a fixed interarrival time distribution (Kovalenko, Kuznetsov & Pegg 1997) we obtain

$$\Pr\left(\frac{q\omega}{E[\alpha] + E[\beta]} > t\right) \xrightarrow[q \to 0]{} e^{-t}.$$

Therefore

$$\Pr(\omega \le t) \xrightarrow[q \to 0]{} 1 - e^{-\frac{qt}{E[\alpha]+E[\beta]}}.$$

Note that $q \to 0$ for a highly reliable safety system which is the case for most of hazardous facilities.

2.2 Probability of accident during a renewal interval

Applying the law of total probability we obtain

$$q = \sum_{j=1}^{N} q_j \Pr\left(\chi_j < \min\left(\chi_1, \chi_2, \dots, \chi_{j-1}, \chi_{j+1}, \dots, \chi_N\right)\right) = \sum_{j=1}^{N} q_j \int_0^\infty \left(\prod_{\substack{r=1 \\ r \ne j}}^{N} \left(1 - F_{\chi_r}(t)\right) \right) dF_{\chi_j}(t),$$

where q_j is the probability of accident during a renewal interval due to j-th safety system failure. The accident takes place during i-th renewal interval due to j-th safety system failure if and only if $\chi_{i,j} \in Q_j^-$, where Q_j^- is the set of intervals where the j-th safety system is inactive. Therefore

$$q_j = \int_0^\infty \Pr\left(t \in Q_j^-\right) dF_{\chi_j}(t).$$

It is difficult, if at all possible, to obtain explicit relation for $\Pr(t \in Q_j^-)$. Here we use the following approximate relation:

$$q_j \approx \int_0^\infty \tilde{q}_j dF_{\chi_j}(t),$$

where

$$\tilde{q}_j = \lim_{t \to \infty} \Pr(t \in Q_j^-).$$

It is known (Høyland & Rausand 2004) that the j-th safety system availability at time t is

$$p_j(t) = E\left[\psi_j\left(x_{j,1}(t), x_{j,2}(t), \dots, x_{j,M_j}(t)\right)\right] = h_j\left(p_{j,1}(t), p_{j,2}(t), \dots, p_{j,M_j}(t)\right),$$

where $p_{j,k}(t)$ is the availability of the k-th subsystem of the j-th safety system. It can be easily shown that

$$\Pr(t \in Q_j^-) = 1 - h_j\left(\Pr\left(t \in Q_{j,1}^+\right), \Pr\left(t \in Q_{j,2}^+\right), \dots, \Pr\left(t \in Q_{j,M_j}^+\right)\right),$$

where $Q_{k,j}^+$ is the set of intervals where the k-th subsystem of the j-th safety system is active. Therefore

$$q_j \approx 1 - h_j\left(\tilde{p}_{j,1}, \tilde{p}_{j,2}, \dots, \tilde{p}_{j,M_j}\right),$$

where

$$\tilde{p}_{j,k} = \lim_{t \to \infty} \Pr\left(t \in Q_{j,k}^+\right).$$

Applying the law of total probability we obtain

$$p_{j,k}(t) = \Pr\left(t \in Q_{j,k}^+\right) = \int_0^\infty \int_0^\infty \Pr\left(t \in Q_{j,k}^+ \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y) dF_{\xi_{j,k}}(x),$$

where $\xi_{i,j,k}$ is the time to i-th failure of the k-th subsystem of the j-th safety system. Obviously, $\xi_{i,j,k}$, i=1,2,… are identically distributed random variables with CDF $F_{\xi_{j,k}}(t)$ for each fixed j, k. It can be easily shown that

$$F_{\xi_{j,k}}(t) = 1 - h_{j,k}\left(1 - F_{\xi_{j,k,1}}(t), 1 - F_{\xi_{j,k,2}}(t), \dots, 1 - F_{\xi_{j,k,C_{j,k}}}(t)\right),$$

where

$$h_{j,k}\left(p_{j,k,1}(t), p_{j,k,2}(t), \dots, p_{j,k,C_{j,k}}(t)\right) = E\left[\varphi_{j,k}\left(x_{j,k,1}(t), x_{j,k,2}(t), \dots x_{j,k,C_{j,k}}(t)\right)\right].$$

2.3 Safety system without inspections

By definition $p_{j,k}(t)$ is the availability of the k-th subsystem of the j-th safety system. We obviously have

$$p_{j,k}(t) = \iint\limits_{x+y\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) +$$

$$+ \iint\limits_{x+y>t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = I_1 + I_2.$$

It can be easily shown that

$$I_2 = \iint\limits_{x+y>t} J_{t\in[0,x]}\, dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = 1 - F_{\xi_{j,k}}(t).$$

Since the operation process of the safety system is an alternating renewal process, it follows that

$$I_1 = \iint\limits_{x+y\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) =$$

$$= \iint\limits_{x+y\le t} p_{j,k}(t-x-y)\, dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = \int\limits_{0}^{t} p_{j,k}(t-z)\, dF_{\xi_{j,k}+\eta_{j,k}}(z),$$

where

$$F_{\xi_{j,k}+\eta_{j,k}}(z) = \int\limits_{0}^{z} F_{\xi_{j,k}}(z-y)\, dF_{\eta_{j,k}}(y).$$

Finally,

$$p_{j,k}(t) = 1 - F_{\xi_{j,k}}(t) + \int\limits_{0}^{t} p_{j,k}(t-z)\, dF_{\xi_{j,k}+\eta_{j,k}}(z).$$

This equation is well known as the fundamental renewal equation (Høyland & Rausand 2004). The application of Laplace-Stieltjes transform and tauberian theorems yields

$$\hat{p}_{j,k} = \lim_{t\to\infty} p_{j,k}(t) = \frac{E[\xi_{j,k}]}{E[\xi_{j,k}] + E[\eta_{j,k}]},$$

where

$$E[\xi_{j,k}] = \int\limits_{0}^{\infty} \left(1 - F_{\xi_{j,k}}(t)\right) dt$$

and

$$E[\eta_{j,k}] = \int\limits_{0}^{\infty} \left(1 - F_{\eta_{j,k}}(t)\right) dt.$$

Again, this is the well known equation for the limiting availability (Høyland & Rausand 2004).

2.4 Safety system with inspections, safety system is inactive during inspection

Let us again write the availability of the k-th subsystem of the j-th safety system as the sum of the following two expressions:

$$p_{j,k}(t) = \iint\limits_{\tau_{j,k}(x,y)\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) +$$

$$+ \iint\limits_{\tau_{j,k}(x,y)>t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = I_1 + I_2,$$

where $\tau_{j,k}(\xi_{1,j,k},\eta_{1,j,k}) = \left(\left\langle \frac{\xi_{1,j,k}}{T_{j,k}+\theta_{j,k}} \right\rangle + 1\right)\left(T_{j,k}+\theta_{j,k}\right) + \eta_{1,j,k}$ is the length of the renewal interval of the k-th subsystem of the j-th safety system operation process and $\langle x \rangle$ is an integer part of x. We see that

$$I_2 = \iint\limits_{\tau_{j,k}(x,y)>t} \left(\sum_{r=0}^{\left\langle \frac{x}{T_{j,k}+\theta_{j,k}} \right\rangle - 1} J_{t\in\left[r\left(T_{j,k}+\theta_{j,k}\right),\, r\left(T_{j,k}+\theta_{j,k}\right)+T_{j,k}\right)} + J_{t\in\left[\left\langle \frac{x}{T_{j,k}+\theta_{j,k}} \right\rangle \left(T_{j,k}+\theta_{j,k}\right),\, x\right)} \right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x).$$

It can be easily shown that

$$I_2 = \left(1 - F_{\xi_{j,k}}(t)\right) - \sum_{r=1}^{\infty}\left(1 - F_{\xi_{j,k}}\left(r\left(T_{j,k}+\theta_{j,k}\right)\right)\right)\left(J_{(r-1)\left(T_{j,k}+\theta_{j,k}\right)+T_{j,k}\le t} - J_{r\left(T_{j,k}+\theta_{j,k}\right)\le t}\right) = F_{\zeta_{j,k}}(t) - F_{\xi_{j,k}}(t),$$

where

$$F_{\zeta_{j,k}}(t) = 1 - \sum_{r=1}^{\infty}\left(1 - F_{\xi_{j,k}}\left(r\left(T_{j,k}+\theta_{j,k}\right)\right)\right)\left(J_{(r-1)\left(T_{j,k}+\theta_{j,k}\right)+T_{j,k}\le t} - J_{r\left(T_{j,k}+\theta_{j,k}\right)\le t}\right).$$

Note that

$$I_1 = \iint\limits_{\tau_{j,k}(x,y)\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) =$$

$$= \iint\limits_{\tau_{j,k}(x,y)\le t} p_{j,k}\left(t - \tau(x,y)\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = \int_0^t p_{j,k}(t-z)\, dF_{\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)}(z),$$

where $F_{\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)}(z) = \Pr\left(\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right) \le t\right)$. Therefore

$$p_{j,k}(t) = F_{\zeta_{j,k}}(t) - F_{\xi_{j,k}}(t) + \int_0^t p_{j,k}(t-z)\, dF_{\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)}(z).$$

Applying the same technique as above we get the following estimation:

$$\hat{P}_{j,k} = \lim_{t\to\infty} p_{j,k}(t) = \frac{E\left[\xi_{j,k}\right] - E\left[\zeta_{j,k}\right]}{E\left[\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)\right]},$$

where

$$E\left[\zeta_{j,k}\right] = \theta_{j,k} E\left[\left\langle \frac{\xi_{j,k}}{T_{j,k}+\theta_{j,k}} \right\rangle\right] = \theta_{j,k} \sum_{r=1}^{\infty} r\left(F_{\xi_{j,k}}\left((r+1)\left(T_{j,k}+\theta_{j,k}\right)\right) - F_{\xi_{j,k}}\left(r\left(T_{j,k}+\theta_{j,k}\right)\right)\right),$$

$$E\left[\xi_{j,k}\right] = \int_0^{\infty}\left(1 - F_{\xi_{j,k}}(t)\right)dt,$$

$$E\left[\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)\right] = \int_0^{\infty}\left(1 - F_{\eta_{j,k}}(t)\right)dt +$$

$$+ \left(T_{j,k}+\theta_{j,k}\right)\left(1 + \sum_{r=1}^{\infty} r\left(F_{\xi_{j,k}}\left((r+1)\left(T_{j,k}+\theta_{j,k}\right)\right) - F_{\xi_{j,k}}\left(r\left(T_{j,k}+\theta_{j,k}\right)\right)\right)\right).$$

2.5 Safety system with inspections, safety system is active during inspection

Using the same method as above we obtain

$$p_{j,k}(t) = \iint\limits_{\tau_{j,k}(x,y)\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) +$$

$$+ \iint\limits_{\tau_{j,k}(x,y)> t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = I_1 + I_2,$$

where $\tau_{j,k}(\xi_{1,j,k},\eta_{1,j,k}) = \left(\left\langle \dfrac{\xi_{1,j,k}}{T_{j,k}+\theta_{j,k}} \right\rangle + 1\right)\left(T_{j,k}+\theta_{j,k}\right) + \eta_{1,j,k}$ is the length of the renewal interval of the *k*-th subsystem of the *j*-th safety system operation process. It is clear that

$$I_2 = \iint\limits_{\tau_{j,k}(x,y)> t} J_{t\in[0,x]}\, dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = 1 - F_{\xi_{j,k}}(t)$$

and

$$I_1 = \iint\limits_{\tau_{j,k}(x,y)\le t} \Pr\left(t \in Q^{+}_{j,k} \mid \xi_{1,j,k} = x, \eta_{1,j,k} = y\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) =$$

$$= \iint\limits_{\tau_{j,k}(x,y)\le t} p_{j,k}\left(t - \tau(x,y)\right) dF_{\eta_{j,k}}(y)\, dF_{\xi_{j,k}}(x) = \int_0^t p_{j,k}(t-z)\, dF_{\tau_{j,k}(\xi_{j,k},\eta_{j,k})}(z),$$

where $F_{\tau_{j,k}(\xi_{j,k},\eta_{j,k})}(z) = \Pr\left(\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right) \le t\right)$. And once again we obtain fundamental renewal equation

$$p_{j,k}(t) = 1 - F_{\xi_{j,k}}(t) + \int_0^t p_{j,k}(t-z)\, dF_{\tau_{j,k}(\xi_{j,k},\eta_{j,k})}(z).$$

Therefore

$$\tilde{p}_{j,k} = \lim_{t\to\infty} p_{j,k}(t) = \frac{E\left[\xi_{j,k}\right]}{E\left[\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)\right]},$$

where

$$E\left[\xi_{j,k}\right] = \int_0^\infty \left(1 - F_{\xi_{j,k}}(t)\right) dt,$$

$$E\left[\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)\right] = \int_0^\infty \left(1 - F_{\eta_{j,k}}(t)\right) dt +$$

$$+ (T_{j,k}+\theta_{j,k})\left(1 + \sum_{r=1}^{\infty} r\left(F_{\xi_{j,k}}\left((r+1)\left(T_{j,k}+\theta_{j,k}\right)\right) - F_{\xi_{j,k}}\left(r\left(T_{j,k}+\theta_{j,k}\right)\right)\right)\right).$$

3 CASE STUDY

Consider the following example. Suppose that complex consists of 5 safety systems and one protected object.

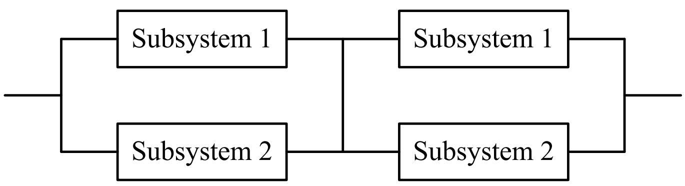


Figure 1. Reliability block diagram of the first safety system.

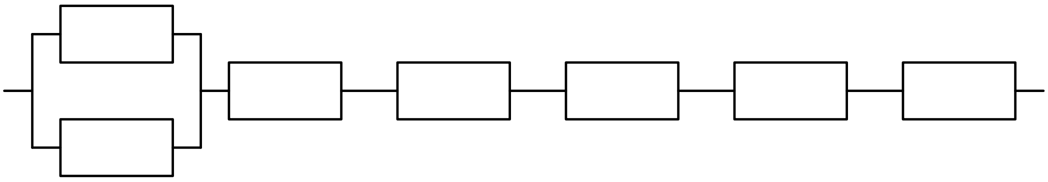


Figure 2. Reliability block diagram of Subsystem 1.

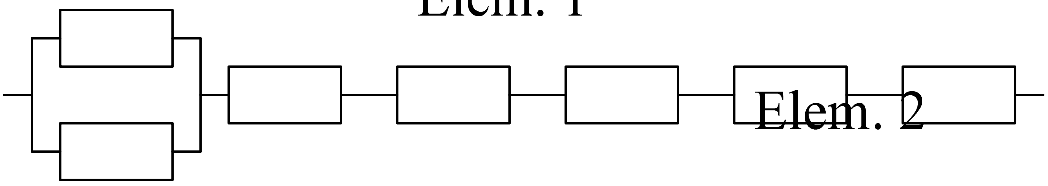


Figure 3. Reliability block diagram of Subsystem 2.

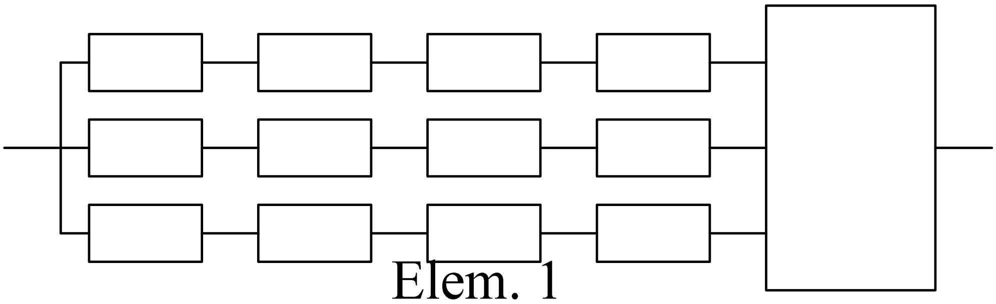


Figure 4. Reliability block diagram of the second safety system.

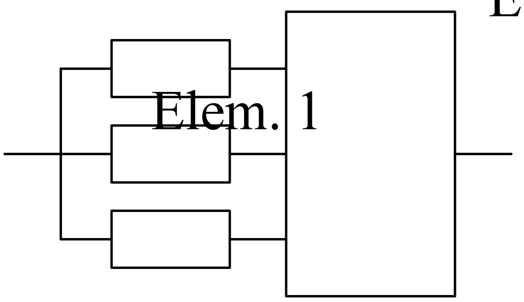


Figure 5. Reliability block diagram of the third safety system.

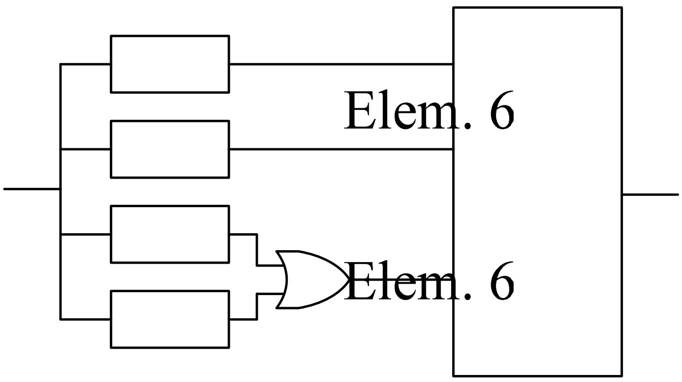


Figure 6. Reliability block diagram of the fourth safety system.

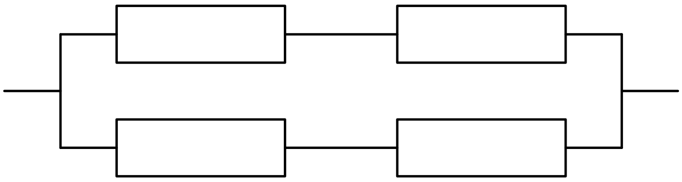


Figure 7. Reliability block diagram of the fifth safety system.

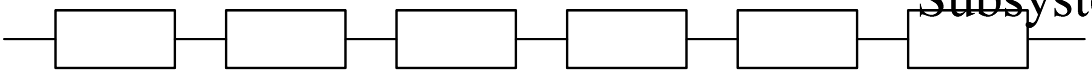


Figure 8. Reliability block diagram of Subsystem 3.

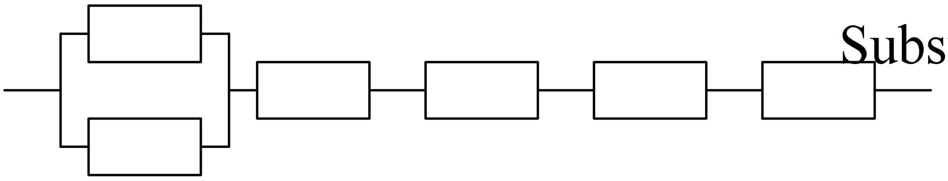


Figure 9. Reliability block diagram of Subsystem 4.

Reliability block diagrams of safety systems are shown on Figures 1 through 9. We obviously have N=5, M_1=2, M_2=1, M_3=1, M_4=1, M_5=2. It can be easily shown that

$$h_1(t) = \left(p_{1,1}(t) + p_{1,2}(t) - p_{1,1}(t)p_{1,2}(t)\right)^2,$$

$$h_2(t) = 3\left(p_{2,1}(t)\right)^2 - 2\left(p_{2,1}(t)\right)^3, \quad h_3(t) = 3\left(p_{3,1}(t)\right)^2 - 2\left(p_{3,1}(t)\right)^3,$$

$$h_4(t) = \left(p_{4,1}(t)\right)^2 + 2p_{4,1}(t)\left(2p_{4,1}(t) - \left(p_{4,1}(t)\right)^2\right)\left(1 - p_{4,1}(t)\right),$$

$$h_5(t) = 1 - \left(1 - p_{5,1}(t)p_{5,2}(t)\right)^2.$$

Therefore $C_{1,1}$=4, $C_{1,2}$=4, $C_{2,1}$=4, $C_{3,1}$=1, $C_{4,1}$=1, $C_{5,1}$=6, $C_{5,2}$=3. We see that

$$h_{1,1}(t) = \left(2p_{1,1,1}(t) - \left(p_{1,1,1}(t)\right)^2\right)\left(p_{1,1,2}(t)\right)^3 p_{1,1,3}(t)p_{1,1,4}(t),$$

$$h_{1,2}(t) = \left(2p_{1,2,1}(t) - \left(p_{1,2,1}(t)\right)^2\right)\left(p_{1,2,2}(t)\right)^3 p_{1,2,3}(t)p_{1,2,4}(t),$$

$$h_{2,1}(t) = p_{2,1,1}(t)p_{2,1,2}(t)p_{2,1,3}(t)p_{2,1,4}(t),$$

$$h_{3,1}(t) = p_{3,1,1}(t), \quad h_{4,1}(t) = p_{4,1,1}(t),$$

$$h_{5,1}(t) = p_{5,1,1}(t)p_{5,1,2}(t)p_{5,1,3}(t)p_{5,1,4}(t)p_{5,1,5}(t)p_{5,1,6}(t),$$

$$h_{5,2}(t) = \left(2p_{5,2,1}(t) - \left(p_{5,2,1}(t)\right)^2\right)\left(p_{5,2,2}(t)\right)^3 p_{5,2,3}(t).$$

Let $F_{\chi_j}(t) = EXP\left(t;\lambda_{\chi_j}\right)$, j=1,2,…,N, $F_{\gamma_j}(t) = EXP\left(t;\lambda_{\gamma_j}\right)$, j=1,2,…,N, $F_{\xi_{j,k,l}}(t) = EXP\left(t;\lambda_{\xi_{j,k,l}}\right)$, j=1,2,…,N, k=1,2,…,M_j, l=1,2,…,$C_{j,k}$ and $F_{\eta_{j,k}}(t) = EXP\left(t;\lambda_{\eta_{j,k}}\right)$, j=1,2,…,N, k=1,2,…,M_j, where

$$EXP(t;\lambda) = \begin{cases} 1 - e^{-\lambda t}, \text{ if } t \ge 0 \\ 0, \text{ otherwise.} \end{cases}$$

Suppose that failures of all safety subsystem are detected only during scheduled periodic inspections of the safety subsystem and safety subsystems are active during an inspection. Therefore

$$E[\omega] = E[\alpha] + \frac{1-q}{q}\left(E[\alpha] + E[\beta]\right)$$

and

$$\Pr(\omega \le t) \xrightarrow[q \to 0]{} 1 - e^{-\frac{qt}{E[\alpha]+E[\beta]}},$$

where

$$E[\alpha] = \frac{1}{\lambda_{\chi_1} + \lambda_{\chi_2} + \lambda_{\chi_3} + \lambda_{\chi_4} + \lambda_{\chi_5}},$$

$$E[\beta] = \frac{1}{\lambda_{\chi_1} + \lambda_{\chi_2} + \lambda_{\chi_3} + \lambda_{\chi_4} + \lambda_{\chi_5}} \left(\frac{\lambda_{\chi_1}}{\lambda_{\gamma_1}} + \frac{\lambda_{\chi_2}}{\lambda_{\gamma_2}} + \frac{\lambda_{\chi_3}}{\lambda_{\gamma_3}} + \frac{\lambda_{\chi_4}}{\lambda_{\gamma_4}} + \frac{\lambda_{\chi_5}}{\lambda_{\gamma_5}} \right),$$

$$q = \frac{q_1\lambda_{\chi_1} + q_2\lambda_{\chi_2} + q_3\lambda_{\chi_3} + q_4\lambda_{\chi_4} + q_5\lambda_{\chi_5}}{\lambda_{\chi_1} + \lambda_{\chi_2} + \lambda_{\chi_3} + \lambda_{\chi_4} + \lambda_{\chi_5}},$$

$$q_1 \approx 1 - \left(\tilde{p}_{1,1} + \tilde{p}_{1,2} - \tilde{p}_{1,1}\tilde{p}_{1,2}\right)^2,$$

$$q_2 \approx 1 - 3\tilde{p}_{2,1}^2 + 2\tilde{p}_{2,1}^3, \quad q_3 \approx 1 - 3\tilde{p}_{3,1}^2 + 2\tilde{p}_{3,1}^3,$$

$$q_4 \approx 1 - \tilde{p}_{4,1}^2 - 2\tilde{p}_{4,1}\left(2\tilde{p}_{4,1} - \tilde{p}_{4,1}^2\right)\left(1 - \tilde{p}_{4,1}\right), \quad q_5 \approx \left(1 - \tilde{p}_{5,1}\tilde{p}_{5,2}\right)^2,$$

$$\tilde{p}_{j,k} = \frac{E\left[\xi_{j,k}\right]}{E\left[\tau_{j,k}\left(\xi_{j,k},\eta_{j,k}\right)\right]}, \; j=1,2,\ldots,N, \; k=1,2,\ldots,M_j,$$

$$E\left[\xi_{1,1}\right] = \frac{2}{\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}} - \frac{1}{2\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}},$$

$$E\left[\xi_{1,2}\right] = \frac{2}{\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}} - \frac{1}{2\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}},$$

$$E\left[\xi_{2,1}\right] = \frac{1}{\lambda_{\xi_{2,1,1}} + \lambda_{\xi_{2,1,2}} + \lambda_{\xi_{2,1,3}} + \lambda_{\xi_{2,1,4}}}, \quad E\left[\xi_{3,1}\right] = \frac{1}{\lambda_{\xi_{3,1,1}}}, \quad E\left[\xi_{4,1}\right] = \frac{1}{\lambda_{\xi_{4,1,1}}},$$

$$E\left[\xi_{5,1}\right] = \frac{1}{\lambda_{\xi_{5,1,1}} + \lambda_{\xi_{5,1,2}} + \lambda_{\xi_{5,1,3}} + \lambda_{\xi_{5,1,4}} + \lambda_{\xi_{5,1,5}} + \lambda_{\xi_{5,1,6}}},$$

$$E\left[\xi_{5,2}\right] = \frac{2}{\lambda_{\xi_{5,2,1}} + 3\lambda_{\xi_{5,2,2}} + \lambda_{\xi_{5,2,3}}} - \frac{1}{2\lambda_{\xi_{5,2,1}} + 3\lambda_{\xi_{5,2,2}} + \lambda_{\xi_{5,2,3}}},$$

$$E\left[\tau_{1,1}\left(\xi_{1,1},\eta_{1,1}\right)\right] = \frac{1}{\lambda_{\eta_{1,1}}} + \left(T_{1,1} + \theta_{1,1}\right)\left(1 + \frac{2e^{-\left(\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}\right)\left(T_{1,1}+\theta_{1,1}\right)}}{1 - e^{-\left(\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}\right)\left(T_{1,1}+\theta_{1,1}\right)}} - \right.$$

$$\left. - \frac{e^{-\left(2\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}\right)\left(T_{1,1}+\theta_{1,1}\right)}}{1 - e^{-\left(2\lambda_{\xi_{1,1,1}} + 3\lambda_{\xi_{1,1,2}} + \lambda_{\xi_{1,1,3}} + \lambda_{\xi_{1,1,4}}\right)\left(T_{1,1}+\theta_{1,1}\right)}}\right),$$

$$E\left[\tau_{1,2}\left(\xi_{1,2},\eta_{1,2}\right)\right] = \frac{1}{\lambda_{\eta_{1,2}}} + \left(T_{1,2} + \theta_{1,2}\right)\left(1 + \frac{2e^{-\left(\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}\right)\left(T_{1,2}+\theta_{1,2}\right)}}{1 - e^{-\left(\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}\right)\left(T_{1,2}+\theta_{1,2}\right)}} - \right.$$

$$\left. - \frac{e^{-\left(2\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}\right)\left(T_{1,2}+\theta_{1,2}\right)}}{1 - e^{-\left(2\lambda_{\xi_{1,2,1}} + 3\lambda_{\xi_{1,2,2}} + \lambda_{\xi_{1,2,3}} + \lambda_{\xi_{1,2,4}}\right)\left(T_{1,2}+\theta_{1,2}\right)}}\right),$$

$$E\left[\tau_{2,1}\left(\xi_{2,1},\eta_{2,1}\right)\right] = \frac{1}{\lambda_{\eta_{2,1}}} + \left(T_{2,1} + \theta_{2,1}\right)\left(1 + \frac{e^{-\left(\lambda_{\xi_{2,1,1}} + \lambda_{\xi_{2,1,2}} + \lambda_{\xi_{2,1,3}} + \lambda_{\xi_{2,1,4}}\right)\left(T_{2,1}+\theta_{2,1}\right)}}{1 - e^{-\left(\lambda_{\xi_{2,1,1}} + \lambda_{\xi_{2,1,2}} + \lambda_{\xi_{2,1,3}} + \lambda_{\xi_{2,1,4}}\right)\left(T_{2,1}+\theta_{2,1}\right)}}\right),$$

$$E\left[\tau_{3,1}\left(\xi_{3,1},\eta_{3,1}\right)\right] = \frac{1}{\lambda_{\eta_{3,1}}} + \left(T_{3,1} + \theta_{3,1}\right)\left(1 + \frac{e^{-\lambda_{\xi_{3,1,1}}\left(T_{3,1}+\theta_{3,1}\right)}}{1 - e^{-\lambda_{\xi_{3,1,1}}\left(T_{3,1}+\theta_{3,1}\right)}}\right),$$

$$E\left[\tau_{4,1}\left(\xi_{4,1},\eta_{4,1}\right)\right]=\frac{1}{\lambda_{\eta_{4,1}}}+\left(T_{4,1}+\theta_{4,1}\right)\left(1+\frac{e^{-\lambda_{\xi_{4,1,1}}\left(T_{4,1}+\theta_{4,1}\right)}}{1-e^{-\lambda_{\xi_{4,1,1}}\left(T_{4,1}+\theta_{4,1}\right)}}\right),$$

$$E\left[\tau_{5,1}\left(\xi_{5,1},\eta_{5,1}\right)\right]=\frac{1}{\lambda_{\eta_{5,1}}}+\left(T_{5,1}+\theta_{5,1}\right)\left(1+\frac{e^{-\left(\lambda_{\xi_{5,1,1}}+\lambda_{\xi_{5,1,2}}+\lambda_{\xi_{5,1,3}}+\lambda_{\xi_{5,1,4}}+\lambda_{\xi_{5,1,5}}+\lambda_{\xi_{5,1,6}}\right)\left(T_{5,1}+\theta_{5,1}\right)}}{1-e^{-\left(\lambda_{\xi_{5,1,1}}+\lambda_{\xi_{5,1,2}}+\lambda_{\xi_{5,1,3}}+\lambda_{\xi_{5,1,4}}+\lambda_{\xi_{5,1,5}}+\lambda_{\xi_{5,1,6}}\right)\left(T_{5,1}+\theta_{5,1}\right)}}\right),$$

$$E\left[\tau_{5,2}\left(\xi_{5,2},\eta_{5,2}\right)\right]=\frac{1}{\lambda_{\eta_{5,2}}}+\left(T_{5,2}+\theta_{5,2}\right)\left(1+\frac{2e^{-\left(\lambda_{\xi_{5,2,1}}+3\lambda_{\xi_{5,2,2}}+\lambda_{\xi_{5,2,3}}\right)\left(T_{5,2}+\theta_{5,2}\right)}}{1-e^{-\left(\lambda_{\xi_{5,2,1}}+3\lambda_{\xi_{5,2,2}}+\lambda_{\xi_{5,2,3}}\right)\left(T_{5,2}+\theta_{5,2}\right)}}-\right.$$

$$\left.-\frac{e^{-\left(2\lambda_{\xi_{5,2,1}}+3\lambda_{\xi_{5,2,2}}+\lambda_{\xi_{5,2,3}}\right)\left(T_{5,2}+\theta_{5,2}\right)}}{1-e^{-\left(2\lambda_{\xi_{5,2,1}}+3\lambda_{\xi_{5,2,2}}+\lambda_{\xi_{5,2,3}}\right)\left(T_{5,2}+\theta_{5,2}\right)}}\right).$$

4 CONCLUSIONS

The proposed model permits to assess the reliability of the "safety system-protected object" complex with multiple safety systems. In particular the suggested approach allows to evaluate such reliability indices as the mean time to accident and the probability of the accident prior to time *t*. The proposed approach allows to take into account the structure of safety systems and scheduled periodic inspections of safety systems. The solution obtained is useful for reliability assessment of nuclear power plants and similar dangerous technological objects.

REFERENCES

Corneliussen, K. & Hokstad, P. 2003. *Reliability Prediction Method for Safety Instrumented Systems; PDS Method Handbook, 2003 Edition.* SINTEF report STF38 A02420, SINTEF, Trondheim, Norway.

Hansen, G.K. & Aarø, R. 1997. *Reliability Quantification of Computer-Based Safety Systems. An Introduction to PDS.* SINTEF report STF38 A97434, SINTEF, Trondheim, Norway.

Kovalenko, I.N., Kuznetsov, N.Yu. & Pegg, P.A. 1997. *Mathematical Theory of Reliability of Time Dependent Systems with Practical Applications.* John Wiley & Sons.

Pereguda, A.I. 2001. Calculation of the Reliability Indicators of the System Protected Object-Control and Protection System. *Atomic Energy* 90: 460-468.

Rausand, M. & Høyland, A. 2004. *System Reliability Theory: Model, Statistical Methods and Applications.* 2nd ed. John Wiley & Sons.

ESTIMATION THE SHAPE, LOCATION AND SCALE PARAMETERS OF THE WEIBULL DISTRIBUTION

Dr. Zouaoui Chikr el-Mezouar

•

University of Bechar, Algeria

E-mail: Chikrtime@yahoo.fr

ABSTRACT

In this paper we propose a new estimators of the shape, location and scale parameters of the weibull distribution.

Keyword: Weibull Distribution, Cran's method and method of moments.

1.INTRODUCTION

The shape and scale parameter estimation of weibull distribution within the traditional methods and standard Bayes from work has been studied by Tummala (1980)[5], Ellis and Tummala (1983)[4], Cran (1988)[3], Al-Fawzan (2000)[2], and Al-Nasir (2002)[1].

This paper considers an estimation procedure based on the coefficient of variation, C.V. The recommended use of such estimators, is to provide quick, preliminary estimators of the parameters. Computational experiments on the presented method and comparison with Cran's method are reported.

2- The three-parameter weibull:

Whenever there is a minimum life (a) such that $(T > a)$, the three-parameter weibull may be appropriate. This distribution assumes that no failures will take place to time (a). For this distribution, the cumulative distribution function. C.D.F is given by:

$$F(t) = 1 - \exp\left[-\left(\frac{t-a}{b}\right)^{c}\right] \quad , t \geq a \quad , a \geq 0 \qquad (2-1)$$

The parameter (a) is called the location parameter. And the (k^{th}) moment is defined by :

$$\mu'_k = a + \frac{b\Gamma\left(1+\frac{1}{c}\right)}{k^{\frac{1}{c}}} \qquad (2-2)$$

In particular, when $k = 1$,

$$\mu_1' = a + b\Gamma\left(1+\frac{1}{c}\right) \qquad (2-3)$$

is the mean time to failure, MTTF of the distribution, and when $k = 2$

$$\mu_2' = a + \frac{b\Gamma\left(1+\frac{1}{c}\right)}{2^{\frac{1}{c}}} \qquad (2-4),$$

and so the variance of this distribution is defined by

$$\sigma^2 = b^2\left\{\Gamma\left(1+\frac{2}{c}\right) - \left[\Gamma\left(1+\frac{1}{c}\right)\right]^2\right\} \qquad (2-5)$$

which is the same as that in the two-parameter model.

3- Estimation of the parameters:

Given the ordered random samples : $t_{(1)} \le t_{(2)} \le \cdots \le t_{(n)}$, the cumulative distribution function .C.D.F can be estimated by :

$$\begin{aligned} S_n(t) &= 0, \quad t < t_{(1)} \\ &= \frac{r}{n}, \quad t_{(r)} \le t \le t_{(r+1)} \quad , r = 1,2,\cdots,n-1 \qquad (3-1) \\ &= 1 \ , \quad t_{(n)} \le t \end{aligned}$$

Ten the population moment, μ_k' is estimated by:

$$\begin{aligned} m_k' &= \int_0^\infty \{1 - S_n(t)\}^k dt \\ &= \sum_{r=0}^{n-1}\left(1-\frac{r}{n}\right)^k \left\{t_{(r+1)} - t_{(r)}\right\} \quad , \quad t_{(0)} = 0 \qquad (3-2) \end{aligned}$$

In particular,

$m_1' = \bar{t}$, the sample mean.

Cran (1988)[3] expressed the parameters in terms of the lower order moments as follows:

$$\left.\begin{aligned} a &= \frac{\mu_1'\mu_4' - \mu_2'^2}{\mu_1' + \mu_4' - 2\mu_2'} \ , \\ b &= \frac{\mu_1' - a}{\Gamma\left(1 + \frac{1}{c}\right)} \\ &\text{and} \\ c &= \frac{\ln(2)}{\ln(\mu_1' - \mu_2') - \ln(\mu_2' - \mu_4')} \end{aligned}\right\} \qquad (3-3)$$

Therefore, the moment estimators of $(a),(b)$ *and* (c) can be obtained from $(3-3)$ by substituting m_1', m_2' *and* m_4' for μ_1', μ_2' *and* μ_4' respectively and solving.

Since the estimator of (a) is inadmissible by being negative or by exceeding $t_{(1)}$, hence we can use the alternative estimator:

$$\hat{a} = t_{(1)} - \frac{\hat{b}\Gamma\left(1 + \frac{1}{\hat{c}}\right)}{n^{\frac{1}{\hat{c}}}} \qquad (3-4)$$

We propose, the coefficient of variation, to get an expression which is a function of (c) only , i.e,

$$C.V. = \frac{\sqrt{\mu_2 - \mu_1^2}}{\mu_1 - t_{(1)}} = \frac{\sqrt{\Gamma\left(1 + \frac{2}{c}\right) - \left[\Gamma\left(1 + \frac{1}{c}\right)\right]^2}}{\Gamma\left(1 + \frac{1}{c}\right)\left(1 - \frac{1}{n^{\frac{1}{c}}}\right)} \qquad (3-5)$$

Now, we can form a table for various $(C.V.)$ by using $(3-5)$ for different (c) values.

In order to estimate (c) *and* (b) , we calculate the coefficient of variation $(C.V.)$ of the data and comparing with $(C.V.)$ using the table to estimate the shape parameter (c) , i.e

$$C.\hat{V}. = \frac{\sqrt{\Gamma\left(1 + \frac{2}{\hat{c}}\right) - \left[\Gamma\left(1 + \frac{1}{\hat{c}}\right)\right]^2}}{\Gamma\left(1 + \frac{1}{\hat{c}}\right)\left(1 - \frac{1}{n^{\frac{1}{\hat{c}}}}\right)} \qquad (3-6)$$

substituting , the scale parameter (b) can then be estimated.

4- simulation results:

The objective of our experiments is to compare the proposed estimators with Cran's estimators. We have generated random samples with known parameters for different sample sizes. To be able to compare, we calculated the mean-squared-error (MSE) for each method , and the table 1, shows the complete results.

Table (1) : Comparison between proposed method and Cran's method (R=1000)

Sample size (n)	parameters	proposed	Cran	The Best
		MSE	MSE	
10	$a=2$	15.9134	333.2995	proposed
	$b=4$	17.4373	333.1223	Proposed
	$c=2$	10.3747	237.5663	Proposed
25	$a=2$	1.3287	10.8445	Proposed
	$b=4$	1.8016	11.3442	Proposed
	$c=2$	1.0492	8.5543	Proposed
50	$a=2$	0.2506	0.3278	Proposed
	$b=4$	0.4193	0.5162	Proposed
	$c=2$	0.2041	0.3486	Proposed
100	$a=2$	0.0806	0.0914	Proposed
	$b=4$	0.1543	0.1678	Proposed
	$c=2$	0.0706	0.1173	proposed

5-Conclusion:

In this paper, we have presented both Cran's method and proposed method (using the coefficient of variation) for estimating the three-parameter weibull distribution. It has been shown from the computational results that the method which gives the best estimates is the proposed method.

References:

1. Al-Fawzan , M.A (2000) : "Methods for Estimating parameters of the Weibull distribution" King Abdulaziz city for science and technology Saudi Arabia.
2. Cran G.W. (1988) : "Moment Estimators for the 3-parameter Weibull Distribution" IEEE TRANSACTIONS ON RELIABILITY , vol. 37, N^0.4.

3. Ellis , W.C. and Tummala, V.M.R (1986) : “Minimum Expected Loss Estimators of the shape and scale parameters of the Weibull Distribution” IEEE TRANSACTIONS ON RELIABILITY , vol. R-35, N^0.2.
4. Tummala, V.M.R (1980) : “Minimum Expected loss estimators of reliability and shape parameter of Weibull distibution” Industrial Mathematics , the Industrial Mathematics Sciety, vol. 30, part I pp.61-67.

IMITATIAL MODELING OF CONDITION THE POWER BLOCK.

Farhadzadeh E.M., Muradaliyev A.Z., Rafiyeva T.K.

Azerbaijan Scientific-Research and Design-Prospecting Institute of Energetic
AZ1012, Ave. H.Zardabi-94
●
e-mail:fem1939@rambler.ru

ABSTRACT

The new method modeling of condition power block, based on joint application a method of modeling of casual events and method modeling of casual processes is developed.

The automated decision of some practical problems, as forecasting of the basic industrial parameters of power station as a whole and separate power units (PB) on various intervals of time (year, quarter, month), an estimation of probability of performance of a production schedule and necessary size of an operative reserve of power, the substantiation of requirements to deduced in cold reserve PB, provides an opportunity of adequate modeling conditions PB.

The basic method used at modeling of conditions энергооборудования, the method of statistical tests [1] is. Its essence consists that various conditions played by casual image on the basis functions of distribution. Modeling of conditions PB by analytical methods meets the serious difficulties caused by set of possible conditions and their complex interrelation. Statistical modeling can be organized both at a level of casual events, and at a level of casual processes. The initial information at modeling at a level of casual events (conditions PB) probabilities of display of these events, and result of calculation - casual sequence of events. The initial information at modeling at a level of casual processes functions of distribution of intervals between the same events and functions of distribution of duration of course of these events, and result of calculation - casual sequence of intervals between events. If modeled events are dependent, this dependence should reflect in modeling algorithm. The variety and interrelation of events, dynamics of change of the parameters describing events, in time not only create significant difficulties in algorithmization of real laws, but also cause, as a rule, private character of developed programs. Many noted difficulties it is possible to avoid if to use both of a method of modeling. At a level of casual events to model type of a condition, and at a level of casual processes - duration of a condition.

Statistical estimations of relative values of total duration of conditions and statistical functions of distribution of realizations of duration of conditions can calculated according to operating experience for a number of years of supervision. Their designations, accordingly, through $\delta\tau^*_{\Sigma,i}$ and $F^*(\tau_i)$ with i=1,m_s, where m_s - number of conditions PB. As $\sum_{i=1}^{m_S}\delta\tau^*_{\Sigma,i}=1$, set $\delta\tau^*_{\Sigma,i}\geq 0$ with i=1, can be presented as a number of frequencies of conditions PB. For fixed though also any sequence of conditions (SC), we shall calculate an integrated number of distribution of total duration of conditions F($\delta\tau^*_{\Sigma,i}$).

Thus size $F_i(\delta\tau^*_{\Sigma,i})$ we shall define under the formula:

$$F_i(\delta\tau^*_{\Sigma})=\sum_{j=1}^{i}\delta\tau^*_{\Sigma,j} \qquad (1)$$

$$F_1(\delta\tau^*_{\Sigma})=\delta\tau^*_{\Sigma,1}$$

$$F_{m_S}(\delta\tau^*_{\Sigma})=1$$

As an example in table 1 estimations of relative duration of conditions PB 300MBт, working on gas-black oil fuel are resulted.

Table 1

Estimation of relative duration of conditions PB 300 MBт

N	Type conditions	Relative duration (%)	Number of distribution	Average duration conditions (h.)
1.	Working	73,9	0,739	543
2.	Emergency idle time	0,1	0,740	16
3.	Refusal at start-up	0,8	0,748	189
4.	Repeated refusal	0,5	0,753	48
5.	Sudden refusal	1,8	0,771	43
6.	Emergency application	4,9	0,820	103
7.	Cold reserve	9,3	0,913	185
8.	Average repair	2,7	0,940	2344
9.	Major overhaul	6,0	1,0	3362

Necessity of differentiation of emergency switching-off caused by their distinction and the requirement of adequacy of modeled process of change of conditions PB. The condition of emergency idle time (at system failures) characterizes switching-off PB basically influence of a power supply system, sudden refusal leads to necessity of use of a hot reserve, damages PB eliminated by switching-off PB under the emergency application, - to use of a cold reserve, refusals at start-up (from a condition of a cold reserve and emergency repair) - operative opportunities of translation PB from non-working conditions in working, repeated refusal (refusal on an interval less than 24 hour) - quality of the control of results after emergency repair.

On fig. 1 some histograms of duration of conditions are resulted. Character of distribution of duration of conditions, is defined numerous, but not always by equivalent factors.

The method of statistical tests with reference to modeling of conditions PB is realized in following sequence:

1. Random variable X with uniform distribution to interval [0,1] is modeled
2. We define an interval of some F($\delta\tau^*_\Sigma$) in which size X gets, by consecutive comparison of borders of intervals. If

$$F_{i-1}(\delta\tau^*_\Sigma) > x > F_i(\delta\tau^*_\Sigma) \tag{2}$$

That corresponds to size X i-th condition PB.

3. Again realization of random variable X is modeled;
4. The interval of function $F^*(\tau_i)$ in which size X gets is defined, i.e. the interval for which is satisfied a condition

$$F_{j-1}(\tau_i) > x > F^*_j(\tau_i) \tag{3}$$

5. Under the formula

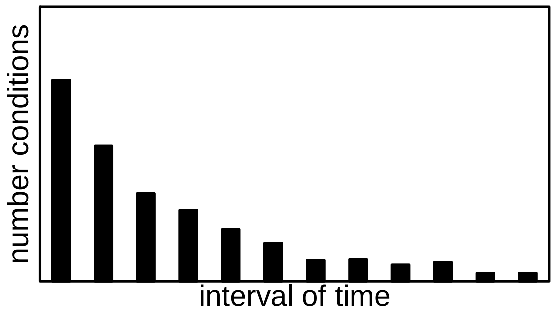
$$\tau_i = \tau_{i,j-1} + \frac{(\tau_{i,j} - \tau_{i,j-1})[X - F_{j-1}(\tau_i)]}{F_j(\tau_i) - F_{j-1}(\tau_i)} \tag{4}$$

realization of duration i-го conditions is calculated. Having repeated n.1-5 before performance of a condition

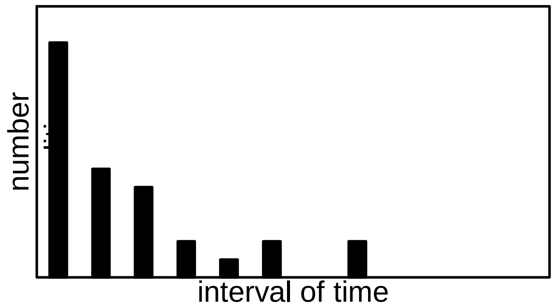
$$\sum_{i=1}^{m_S}\sum_{j=1}^{m_i}\tau_{i,j} \geq \Delta T$$

where m_s - number of conditions; m_i - number of realizations conditions i-го type; $\tau_{i,j}$ - j-th realization of duration i-го conditions; ΔT - an interval of time for which the sequence of conditions PB is modeled.

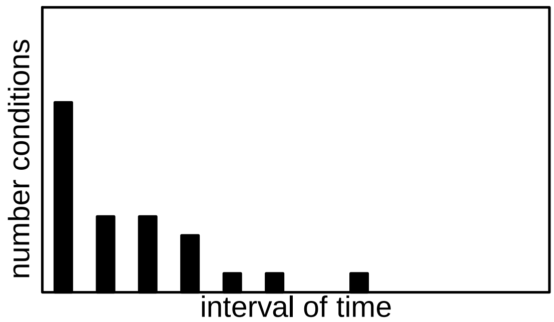
We shall receive realization of conditions PB. The information file of conditions includes date and time of the beginning and the end of a condition, duration of a condition, a kind of switching-off, type of a condition. This realization of conditions, reflecting the general laws of number and duration of conditions, nevertheless, can is essential differ from concrete laws of change of conditions in time. Difference reduced not only to a divergence of the moments of occurrence of conditions. It is natural, since it is necessary to operate with random variables, and is inevitable.



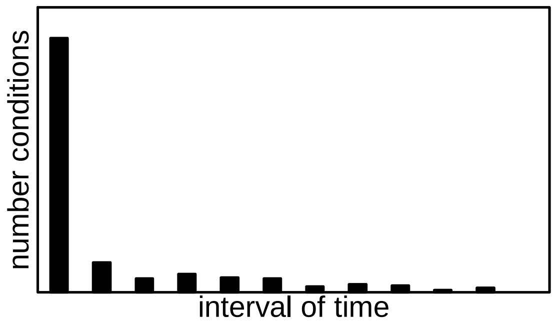
a)



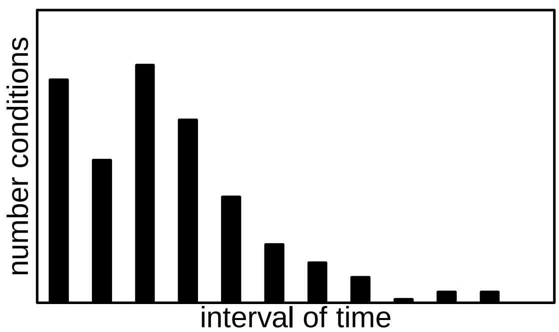
b)



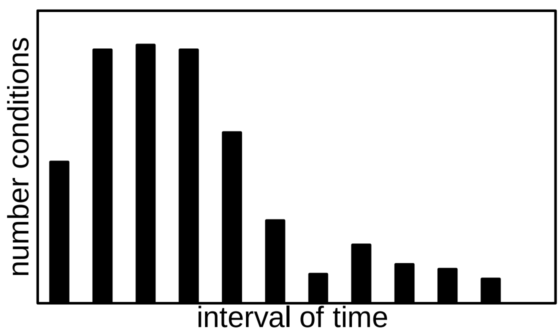
c)



d)



e)



f)

Fig. 1. Histograms of duration conditions.
a - working condition; b - emergency idle time; c - refusal at start-up; d - sudden switching-off;
e - switching-off under the emergency application; f - cold reserve.

In modeled realizations are possible:

- same joint conditions. For example, consistently two working conditions.
- practically impossible conditions. For example, at finding PB in a condition of a cold reserve of occurrence of a condition of emergency idle time
- conditions which are impossible in the set interval of time. For example, capital and average repair during an autumn-winter maximum of loading are not spent.

Principal causes of inadequacy of modeled realizations of sequence of conditions PB of real sequence of conditions are initial preconditions (accident and independence of conditions) when are not considered:

- the determined character scheduled (average and capital) repairs;
- dependence of probability of conditions on parameters of individual reliability PB;
- interrelation of conditions PB;
- dependence of probability of conditions on a season.

Let us consider methods of the account of these features. At the automated forecasting basic industrial parameters PB, which scheduled repair, is not stipulated, a number of distribution of probabilities of conditions can be received by transition to conditional probabilities of conditions.

Conditional probability i-го conditions provided that the condition j is impossible, pays off under the formula:

$$\delta\tau^{**}_{\Sigma,i} = \frac{\delta\tau^{*}_{\Sigma,i}}{\sum\limits_{\substack{\nu=1 \\ \nu\neq j}}^{m_S} \tau^{*}_{\Sigma,\nu}} \tag{5}$$

$$\delta\tau^{**}_{\Sigma,j} = 0$$

And a number of distribution of conditional probabilities of conditions - under the formula (1)

If on considered PB carrying out of scheduled repair work modeling SC is spent on intervals of time before repair is provided. Otherwise (scheduled repair is not stipulated) - on all set interval of time. Objective character of realizations in this model entirely concerns only to full conformity to real statistical data. However, still, SC insufficiently full reflects distinction of parameters of reliability PB. Reflection of this distinction can be reached by transition from the average values of relative total duration of conditions of all PB $\delta\tau^{*}_{\Sigma,i}$, to relative total duration of conditions of everyone PB and from the average distributions of duration of conditions of all PB $F(\tau_i)$ to distributions of duration of conditions of everyone PB.

As an example confirming necessity of the account of individual reliability PB, in table 2 estimations of probability of finding PB in various conditions are resulted. Despite of casual character of emergency conditions, and conditions of a cold reserve concrete PB (the probability of finding PB in a condition of a cold reserve depends on its technical condition, the specific charge of fuel, an opportunity of decrease in number of start-up and so forth), probability of transition from a working condition in a condition of restoration at sudden refusals, or in a condition of a cold reserve are various. From a condition of a reserve transition in a condition of restoration is impossible at sudden refusals, and furthermore - again in a condition of a reserve. These and a number of other features real SC PB could not be considered in the algorithm considered above, assuming mutual independence of adjacent conditions PB. The interrelation conditions be considered by conditional probabilities of occurrence of conditions.

Table 2

Probabilities of conditions PB

Number the block	Type of condition						
	Working	Emergency idle time	Sudden refusal	Emergency application	Cold reserve	Average repair	Major overhaul
1	0,748	0,001	0,043	0,046	0,06	0,088	0
2	0,752	0	0,016	0,057	0,095	0	0,073
3	0,662	0	0,005	0,054	0,121	0,037	0,070
4	0,642	0,001	0,026	0,063	0,102	0	0,145

5	0,631	0	0,028	0,068	0,172	0,065	0,025
6	0,83	0,002	0,011	0,040	0,055	0	0,062
7	0,783	0	0,009	0,033	0,092	0	0,081
8	0,86	0,001	0,012	0,040	0,047	0	0,03

The estimation of conditional probabilities spent on statistical data SC under enough simple formula which looking like:

$$Q^*_{i,j} = \frac{m_{i,j}}{m_i} \tag{6}$$

where m_i - number of conditions i - го type; $m_{i,j}$ - the number of conditions j-го type provided that preceded this condition a condition i-го type.

Considering bulkiness and labour input of the statistical analysis of initial data real SC manually, possible subjective mistakes, have been developed algorithm and the program of calculation of conditional probabilities of occurrence of conditions. The essence of algorithm reduced to consecutive comparison of adjacent conditions PB. Necessity of such comparison is caused by a significant share of non-working conditions (on the average 20 %) in which PB it is translated formally from a non-working condition. Such translations, reducing number of start-up PB, promote decrease in the charge of fuel. If the moments of end preceded and the beginnings of the subsequent of non-working conditions coincide, as the next condition the non-working condition is fixed. Otherwise - a working condition. Results of calculations are brought in a matrix of change of conditions which structure at m_s=5, is resulted in table 3.

It is necessary to have in view of, that a chance, when

$$\sum_{j=1}^{m_s} m_{i,j} \neq \sum_{j=1}^{m_s} m_{j,i} \tag{7}$$

and practically always: $$m_{i,j} \neq m_{j,i} \tag{8}$$

Table 3

Structure of a matrix of change of conditions

Conditional number (i) a previous condition	Conditional number (j) the subsequent condition				
	1	2	3	4	5
1	$m_{1,1}$	$m_{1,2}$	$m_{1,3}$	$m_{1,4}$	$m_{1,5}$
2	$m_{2,1}$	$m_{2,2}$	$m_{2,3}$	$m_{2,4}$	$m_{2,5}$
3	$m_{3,1}$	$m_{3,2}$	$m_{3,3}$	$m_{3,4}$	$m_{3,5}$
4	$m_{4,1}$	$m_{4,2}$	$m_{4,3}$	$m_{4,4}$	$m_{4,5}$
5	$m_{5,1}$	$m_{5,2}$	$m_{5,3}$	$m_{5,4}$	$m_{5,5}$

The parity (7) speaks initial and final conditions SC PB for which the previous (subsequent) condition is not known. In the ratio (8) finds the reflection as interrelation of conditions PB, and formal character of change of some non-working conditions. Here $m_{i,j}$ - the number of preceded conditions of i-th type from which PB has been translated in a condition of j-th type; $m_{j,i}$ - number of the subsequent conditions of j-th type in which PB has been translated from a condition of i-th type; $m_{i,j}$ - the general number of conditions of i-th type.

It is obvious, that $m_{i,j}$ - number of switching-off (start-up) PB, and $m_{1,j}$ - number of switching-off PB in j-th condition. Alongside with $m_{i,j}$ where i=1, m_s and j=1, m_s were calculated also total duration of finding PB in i-th condition provided that a preceded condition was j-th. The estimation of probability of translation PB from i-th condition in j-th condition calculated under the formula (6), and a number of probabilities of conditions, under the formula:

$$F_i(Q^*_{i,j})_\nu = \sum_{\substack{j=1 \\ j \neq i}}^{\nu} Q^*_{i,j} \tag{9}$$

$$F_i(Q^*_{i,j})_{m_S} = 1$$

The algorithm modeling condition PB thus transformed (regarding modeling type of a condition) a little. From average of some distribution of probabilities of conditions PB, we pass to a number of distribution conditional probabilities of occurrence of the subsequent condition (if a previous condition was a condition of the set type). For example, if to accept for a previous condition - working to this condition (i=1) there corresponds distribution $F_1(Q_{1,j})$. As a result, of playing type of a condition on $F_1(Q_{1,j})$ the subsequent condition there can be a reserve condition (i=7). To this condition, there correspond a number of distribution $F_7(Q^*_{7,j})$. As a result, of the next playing it is established, that at start-up PB there was damage PB and it is deduced in emergency repair, etc. Some experimental estimation of conditional probabilities of occurrence of conditions $Q^*_{i,j}$ and numbers of distribution of these probabilities $F_i(Q^*_{i,j})$ are resulted in table 4.

Greater advantage of application of distributions $F_i(Q^*_{i,j})$ is increase of objective character of realization SC. In particular, at modeling SC adjacent same and practically impossible conditions are excluded, and probabilities of transitions from one condition in another are adequate observable on practice. One of the most important and difficult questions at modeling SC is the account of dynamics of change of probability of conditions in time. Earlier the accepted assumption of uniform distribution of conditions on the set interval of time not always corresponds to practice.

Table 4

Estimations of conditional probabilities of conditions

The subsequent condition (j)	Previous conditions (i)							
	Working		Sudden refusal		Emergency application		Cold reserve	
	$Q^*_{i,j}$	$F_i(Q^*_{i,j})$	$Q^*_{i,j}$	$F_i(Q^*_{i,j})$	$Q^*_{i,j}$	$F_i(Q^*_{i,j})$	$Q^*_{i,j}$	$F_i(Q^*_{i,j})$
Working	-	0	0.86	0.86	0.81	0.81	0.96	0.96
Emergency idle time	0.04	0.04	0	0.86	0	0.81	0	0.96
Sudden refusal	0.33	0.37	-	0.86	0	0.81	0	0.96
Emergency application	0.35	0.72	0	0.86	-	0.81	0	0.96
Refusal at start-up	0	0.72	0.02	0.88	0.01	0.82	0.04	1.0
Repeated refusal	0	0.72	0.09	0.97	0.05	0.87	0	1.0
Cold reserve	0.28	1.0	0.03	1.0	0.13	1.0	-	1.0

As an example on fig. 2 realizations of law of change of factor of technical use (K_{tu}) PB a state district power station within a year are resulted. As relative duration of a finding in working order PB during the winter period approximately twice less, than during the years period follows from fig.2.

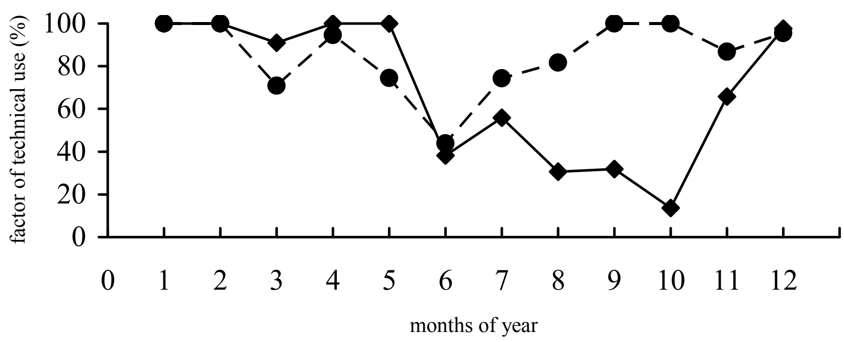


Fig.2. Laws of change of factor of technical use separate PB on months of year.

To consider non-uniformity of occurrence of conditions PB in current of year, numbers of distribution of probabilities of conditions in each month, which used at modeling type of a condition, are made. However, thus the discrepancies connected with an opportunity of modeling of adjacent same and practically impossible conditions kept.

To calculate matrixes of estimations of conditional probabilities of occurrence of conditions PB for each month, in view of sharp decrease in number of conditions PB, is connected with the big uncertainty of estimations. To exclude the specified discrepancies of modeling, we shall take advantage of that part of the information of a matrix of change of conditions which does not depend on number of conditions. Namely - the instruction on possible adjacent conditions. If adjacent conditions are possible, in a cell of a matrix we shall put down 1, otherwise - 0. We shall name this matrix - a matrix of transitions (MT). For the conditions entered into consideration (see table 1) (MT) shown in table 5.

The further increase of adequacy modeled SC is reached by use of the mechanism of specification of probabilities of occurrence of conditions after each playing type of a condition. An essence of the mechanism of specification we shall consider on a following example.

Table 5

Matrix of transitions

Conditional number of a previous condition	Conditional number of the subsequent condition								
	1	2	3	4	5	6	7	8	9
1	0	1	0	1	1	1	1	1	1
2	1	0	1	0	0	1	1	1	1
3	1	0	0	0	0	1	1	1	1
4	1	0	1	1	0	1	1	1	1
5	1	0	1	0	0	1	1	1	1
6	1	0	1	0	0	0	1	1	1
7	1	0	1	0	0	1	0	1	1
8	1	0	0	0	0	0	1	0	0
9	1	0	0	0	0	0	1	0	0

Let's assume, that relative duration of a working condition is equal $\delta\tau^*_{\Sigma wor} = 0{,}6$ considered month of year, conditions of a cold reserve- $\delta\tau^*_{\Sigma res} = 0{,}3$, conditions of emergency repair $\delta\tau^*_{\Sigma em} = 0{,}1$. At playing type and duration of a condition it has appeared, that PB is in working order, with relative duration $\delta\tau^*_{\Sigma wor} = 0{,}40$. From this condition according to conditions of example PB can pass both in a condition of a cold reserve, and in a condition of emergency repair.

Conditional probabilities of these conditions (a preceded condition the working condition is) will be equal:

$$\delta\tau^{**}_{\Sigma res} = \frac{\delta\tau^{*}_{\Sigma,res}}{\delta\tau^{*}_{\Sigma,res} + \delta\tau^{*}_{\Sigma,em}} = 0{,}75$$

$$\delta\tau^{**}_{\Sigma,em} = \frac{\delta\tau^{*}_{\Sigma,em}}{\delta\tau^{*}_{\Sigma,res} + \delta\tau^{*}_{\Sigma,em}} = 0{,}25$$

Further, if as a result of playing the next type of a condition and its duration, it is established, that next condition PB is emergency repair with relative duration $\delta\tau_{em} = 0{,}15$ it has appeared, that $\delta\tau^{*}_{em} > \delta\tau^{*}_{\Sigma em}$. In it finds the reflection a natural parity of average sizes and separate realizations. As the sum relative длительностей arisen conditions PB does not exceed unit ($(\delta\tau^{*}_{wor} + \delta\tau^{*}_{em} = 0{,}55 < 1)$ process of modeling proceeds. During the considered moment of time, (emergency repair is completed) PB can pass both in a working condition, and in a condition of a cold reserve. However, conditional probabilities of transition in these conditions will not be equal any more

$$\delta\tau^{**}_{\Sigma,wor} = \frac{\delta\tau^{*}_{\Sigma wor}}{1 - \delta\tau^{*}_{\Sigma em}} = 0{,}67$$

$$\delta\tau^{**}_{\Sigma,res} = \frac{\delta\tau^{*}_{\Sigma res}}{1 - \delta\tau^{*}_{\Sigma em}} = 0{,}33$$

As $\delta\tau_{\Sigma wor}$ is partially spent. We shall lead current correction of conditional probabilities under the formula

$$\delta\tau^{**}_{\Sigma,wor} = \frac{\delta\tau^{*}_{\Sigma wor} - \delta\tau^{*}_{wor}}{\delta\tau^{*}_{\Sigma wor} + \delta\tau^{*}_{\Sigma res} - \delta\tau^{*}_{wor}} = 0{,}4$$

$$\delta\tau^{**}_{\Sigma,res} = \frac{\delta\tau^{*}_{\Sigma res}}{\delta\tau^{*}_{\Sigma wor} - \delta\tau^{*}_{wor} + \delta\tau^{*}_{\Sigma res}} = 0{,}6$$

Comparison of results of calculation testifies to essential change of sizes $\delta\tau_{\Sigma wor}$ and $\delta\tau^{**}_{\Sigma wor}$. If as a result of playing type and duration of a condition it has appeared, that the next condition is working, and realization of duration of a working condition exceeds $\delta\tau^{**}_{\Sigma wor} = 0.2$, in the remained interval of time of the considered period probably only reserve condition and consequently process of modeling of conditions comes to the end

CONCLUSION

1. Process of change of conditions of power units characterized by an opportunity of formal transition from one non-working condition in another that promotes decrease in number of switching-off (start-up). The number of such changes of conditions, on the average, makes about 20 % from number of non-working conditions. Application of known methods of modeling of conditions does not allow consider these features.
2. The new method of modeling of a condition of the power units, based on joint application of a method of modeling of casual events and a method of modeling of casual processes is developed. The method allows:
- exclude modeling adjacent same conditions and impossible combinations of adjacent conditions;
- consider statistical interrelation of conditions;
- consider laws of change of conditions in a season.
1. Modeling of inadmissible combinations of adjacent conditions is prevented on the basis of a matrix of transitions

2. The interrelation of conditions displayed by transition to conditional probabilities of conditions and correction of relative duration of conditions on a residual interval of modeling.
3. Dependence probability occurrence of conditions time is considered by consecutive modeling conditions on intervals for which this dependence can be neglected
4. On the basis algorithm, modeling conditions power units as a whole, and the algorithm and the program of forecasting of the guaranteed estimations of the basic industrial parameters both for a state district power station developed for separate power units.

REFERENCES

1. Rudenko J.N., Ushakov I.A. Reliability of systems of power. M.: Science, 1986.

ON TOTAL TIME ON TEST TRANSFORM ORDER

V. M. Chacko
Department of Statistics, St. Thomas College
Thrissur, Kerala-680001
●
Email: chackovm@gmail.com

ABSTRACT

In this paper, ordering of two lifetime random variable based on convex Total Time on Test (CXTTT) transform and increasing convex Total Time on Test (ICXTTT) transform of their distributions are introduced and, their implication with stochastic ordering and hazard rate ordering are proved.

1 INTRODUCTION

Stochastic orders and inequalities are being used at an accelerated rate in much diverse area of probability and statistics. This paper introduces the stochastic ordering of two life distributions based on convex Total Time on Test (CXTTT) transform and increasing convex Total Time on Test (ICXTTT) transform.

The simplest way of comparing two distribution functions is by comparison of associated means. However, such a comparison is based on only two single number (the means), and therefore it is often not very informative. When one wishes to compare two distribution functions that have the same mean (or that are centered about the same value), one is usually interested in the comparison of the dispersion of these distributions. In many situations in applications, one has more detailed information, for the comparison of two distribution functions, that take in account various forms of possible knowledge about the two underlying distributions, see Shaked and Shanthikumar (1994).

Total Time on Test (TTT) transform plots are useful for analyzing non-negative data. The plots help in choosing a mathematical model for the data and provide information about failure rate. Also incomplete data can be analyzed and there is a theoretical basis for such an analysis, see Barlow and Campo (1975). As TTT is useful in analyzing incomplete data, we can order the distributions according to TTT of respective distributions. Kochar et al. (2002) defined TTT transform order and Shaked and Shanthikumar (2007) studied it explicitly. Nair et al. (2008) provided applications of TTT of order n in reliability analysis.

But if the mean values of the two distributions are same, we need to go for variability measures for ordering. Convex and increasing convex ordering is usually used to order two distributions according to the variability of their random variables. In this paper, we introduce the ordering of two distributions based on convex TTT and increasing convex TTT, which can be used to order two distributions according to the TTT of the convex and increasing convex functions of the respective random variables. When we consider censored data, CXTTT and ICXTTT is more suitable for ordering two distributions according to the variability.

In section 2, the notions of usual stochastic ordering and TTT are briefly recalled. In section 3, the definition of TTT ordering is given. In section 4, the concept of CXTTT ordering and ICXTTT ordering are provided and some implications between stochastic ordering and hazard rate ordering with CXTTT and ICXTTT ordering are proved. Conclusions are given at last section.

2. STOCHASTIC , HAZARD RATE AND MEAN RESIDUAL LIFE ORDER

Let X and Y be two random variables such that

$$P(X > u) \leq P(Y > u), \forall u \in (-\infty, \infty).$$

Then X is said to be smaller than Y in the usual stochastic order (denoted by $X \leq_{st} .Y$). It means that X is less likely than Y to take large values, where "large" means the value greater than u, and that this is the case for all u's. (2.1) is same as

$$P(X \leq u) > P(Y \leq u), \forall u \in (-\infty, \infty).$$

Let X and Y has distributions F and G respectively independent of each other. Let $h_f(x) = \frac{f(x)}{1-F(x)}$ and $h_g(x) = \frac{g(x)}{1-G(x)}$ be the hazard rate functions of F and G where f(x) and g(x) are the probability density functions of F and G respectively. Clearly higher the hazard rate smaller the X should be stochastically.

Definition 2.1 Let X and Y are two non-negative random variables with absolutely continuous distributions F and G respectively independent of each other. X is said to be smaller than Y in hazard rate order (denoted by $X \leq_{hr} .Y$) if $h_f(x) \geq h_g(x)$, $x \geq 0$.

Another important order is mean residual life order. The definition of mean residual life is given below.

Definition 2.2 If X is a non-negative random variable with a survival function $\overline{F}(x)$ and a finite mean μ, the mean residual life of X at x is defined as

$$m(x) = E(X - x \mid X > x), \forall x \in [0, \infty] \text{ and 0 otherwise.}$$

Clearly, the smaller the mean residual life function is the smaller X should be in some stochastic sense. Let $m_f(x)$ and $m_g(x)$, $x \geq 0$ be the mean residual life functions of X and Y respectively.

Definition 2.3 Let X and Y be two non-negative random variables with absolutely continuous distributions F and G respectively independent of each other. X is said to be smaller than Y in mean residual life order if $m_f(x) \leq m_g(x)$, $x \geq 0$ (denoted by $X \leq_{mrl} Y$).

More details of stochastic orders can be seen in Shaked and Shanthikumar (1994). Now we recall the TTT order in the following section.

3. TOTAL TIME ON TEST TRANSFORM

Let X and Y have distributions F and G respectively independent of each other. Given a sample of size n from the non-negative random variables X and Y, let $X_{(1)} \leq X_{(2)} \leq ... \leq X_{(k)} \leq ... \leq X_{(n)}$ and $Y_{(1)} \leq Y_{(2)} \leq ... \leq Y_{(k)} \leq ... \leq Y_{(n)}$ be the order statistics corresponding to the samples. TTT to the rth failure from distributions F and G are, respectively,

$$T(X_{(r)}) = nX_{(1)} + (n-1)(X_{(2)} - X_{(1)}) + ... + (n-r+1)(X_{(r)} - X_{(r-1)}) = \sum_{i=1}^{r} X_{(i)} + (n-r)X_{(r)}$$

$$T(Y_{(r)}) = nY_{(1)} + (n-1)(Y_{(2)} - Y_{(1)}) + ... + (n-r+1)(Y_{(r)} - Y_{(r-1)}) = \sum_{i=1}^{r} Y_{(i)} + (n-r)Y_{(r)}.$$

Define

$$H_n^{-1}(r/n) = \frac{1}{n}T(X_{(r)}) \text{ and } K_n^{-1}(r/n) = \frac{1}{n}T(Y_{(r)})$$

$$H_n^{-1}(r/n) = \int_0^{F_n^{-1}(r/n)} (1-F_n(u))du,\ K_n^{-1}(r/n) = \int_0^{G_n^{-1}(r/n)} (1-G_n(u))du$$

where $F_n(u) = \begin{cases} 0 & u < X_{(i)} \\ i/n & X_{(i)} \le u < X_{(i+1)} \\ 1 & X_{(n)} > u \end{cases}$ and $G_n(u) = \begin{cases} 0 & u < Y_{(i)} \\ i/n & Y_{(i)} \le u < Y_{(i+1)} \\ 1 & Y_{(n)} > u \end{cases}$

$F_n^{-1}(x) = \inf\{x : F_n(x) \ge u\}$ and $G_n^{-1}(x) = \inf\{x : G_n(x) \ge u\}$.

The fact that $F_n(u) \to F(x)$ a.s. and $G_n(u) \to G(x)$ a.s. implies, by Glivenko Cantelli Theorem, $\lim_{n\to\infty, r/n \to t} \int_0^{F_0^{-1}(r/n)} (1-F_n(u))du = \int_0^{F^{-1}(t)} (1-F(u))du$ and

$\lim_{n\to\infty, r/n \to t} \int_0^{G_0^{-1}(r/n)} (1-G_n(u))du = \int_0^{G^{-1}(t)} (1-G(u))du$ uniformly in $t \in [0,1]$.

We define TTT transform of F as

$$H_F^{-1}(t) = \int_0^{F^{-1}(t)} (1-F(u))du \quad t \in [0,1].$$

and TTT transform of G as

$$H_G^{-1}(t) = \int_0^{G^{-1}(t)} (1-G(u))du \quad t \in [0,1].$$

We define the following order of two random variables with absolute continuous distribution functions F and G respectively. Clearly lower the empirical TTT of X is lower the that of Y only when the value of $X_{(1)} \le X_{(2)} \le ... \le X_{(k)} \le ... \le X_{(n)}$ and are lower than that of $Y_{(1)} \le Y_{(2)} \le ... \le Y_{(k)} \le ... \le Y_{(n)}$. That is, $T(X_{(n)}) \le T(Y_{(r)})$.

Now we recall the following.

Definition 3.1 Let X and Y be two non-negative random variables with absolute continuous distributions F and G respectively. X is said to be smaller than that of Y in the Total Time on Test Transform order if $H_F^{-1}(t) \le H_G^{-1}(t), \quad \forall t \in [0,1]$.

We denote the TTT order as $X \le_{TTT} Y$. More details of TTT ordering can be seen in Shaked and Shanthikumar (2007) and its application in Chacko et al. (2010).

In the following section, we introduce the Convex TTT order and Increasing convex TTT order which take an account of variability of random variables.

4 CONVEX AND INCREASING CONVEX TTT

Let

$$T^g(X_{(r)}) = ng(X_{(1)}) + (n-1)(g(X_{(2)}) - g(X_{(1)})) + ... + (n-r+1)(g(X_{(r)}) - g(X_{(r-1)})) = \sum_{i=1}^{r} g(X_{(i)}) + (n-r)g(X_{(r)})$$

where g is a convex function. Then define, for $g(x) = x^2$,

$$(H_n^{-1})^2(r/n) = \int_0^{(F_n^{-1}(r/n))^2} (1-F_n(u))du = \frac{T_n^{x^2}(X_{(r)})}{n}$$

where

$$\frac{T_n^{x^2}(X_{(r)})}{n}=\sum_{i=1}^{r}(X_{(i)})^2+(n-r)(X_{(r)})^2 \quad \frac{T_n^{x^2}(X_{(r)})}{n}=\sum_{i=1}^{r}(X_{(i)})^2+(n-r)(X_{(r)})^2$$

$$\lim_{n\to\infty, r/n\to t}\int_0^{(F_0^{-1}(r/n))^2}(1-F_n(u))du=\int_0^{(F^{-1}(t))^2}(1-F(u))du=(H_F^{-1})^2(t), say.$$

More generally, define for every convex function $g: R\to R$

as $g(H_n^{-1})(r/n)=\int_0^{g(F_n^{-1}(r/n))}(1-F_n(u))du=\frac{T_n^g(X_{(r)})}{n}$

$$\lim_{n\to\infty, r/n\to t}\int_0^{g(F_0^{-1}(r/n))}(1-F_n(u))du=\int_0^{g(F^{-1}(t))}(1-F(u))du=g(H_F^{-1})(t), say.$$

Similarly we can define

$$g(K_n^{-1})(r/n)=\int_0^{g(G_n^{-1}(r/n))}(1-G_n(u))du=\frac{T_n^g(Y_{(r)})}{n}$$

$$\lim_{n\to\infty, r/n\to t}\int_0^{g(G_0^{-1}(r/n))}(1-G_n(u))du=\int_0^{g(G^{-1}(t))}(1-G(u))du=g(K_F^{-1})(t), say.$$

Let X and Y be two random variables such that $T^g(X_{(n)})\le T^g(Y_{(r)})$ for all convex functions $g: R\to R$ and all samples of size n. Then X is smaller than Y in some stochastic sense, since $T^g(X_{(n)})$ is average of total observed convex transformed time of a test. The X values are less likely to take larger values than Y values. Therefore we define the following convex TTT ordering.

Definition 4.1 Let X and Y be two non-negative random variables with absolutely continuous distribution functions F and G respectively. If

$$(H_F^{-1})^g(t)\le(H_G^{-1})^g(t), \quad \forall t\in[0,1],$$

and g is convex function, then X is smaller than Y in convex TTT order (denoted as $X\le_{CXTTT} Y$).

Roughly speaking, convex functions are functions that take on them (relatively) larger values over region of the form $(-\infty,a)\cup(b,\infty)$ for a < b.

Now we introduce the increasing convex TTT ordering.

Definition 4.2 Let X and Y be two non-negative random variables with absolutely continuous distribution functions F and G respectively. If

$$(H_F^{-1})^g(t)\le(H_G^{-1})^g(t), \quad \forall t\in[0,1]$$

and g is increasing convex function, then X is smaller than Y in increasing convex TTT order (denoted $X\le_{ICXTTT} Y$).

Roughly speaking X is both 'smaller' and 'less variable' than Y in some stochastic sense.

Example 4.1 Let $X\sim Exp(\lambda)$ and $Y\sim Exp(\theta)$ and g(x) = x, a convex function.

$H_F^{-1}(t)=\lambda t$ and $H_G^{-1}(t)=\theta t$, $t\in[0,1]$. $\therefore \hat{\lambda}=\frac{T(X_{(r)})}{n}\le\hat{\theta}=\frac{T(Y_{(r)})}{n}$ when $T(X_{(r)})\le T(Y_{(r)})$.

Hence we can conclude that $X\le_{TTT} Y$ and $X\le_{CXTTT} Y$, if $\hat{\lambda}\le\hat{\theta}$. Again

$$\int_0^{(F^{-1}(t))^2}(1-F(u))du=\int_0^{(F^{-1}(t))^2}e^{-x/\lambda}dx=\lambda(1-e^{-(x_*)^2/\lambda})$$

and

$$\int_0^{(G^{-1}(t))^2}(1-G(u))du=\int_0^{(G^{-1}(t))^2}e^{-x/\theta}dx=\theta(1-e^{-(x_{**})^2/\theta})$$

where

$x_*=\inf\{x:F(x)\geq t\}$ and $x_{**}=\inf\{x:G(x)\geq t\}$ Then $(H_F^{-1})^2(t)\leq(H_G^{-1})^2(t),\quad\forall t\in[0,1]$ if $\lambda<\theta$ and $x_*<x_{**}$.

Now we prove the following theorem, which gives the implication of stochastic ordering and convex TTT ordering, if the expectations of random variables are finite.

Theorem 4.1 Let X and Y be two non-negative random variables having absolutely continuous distribution functions F and G respectively. Let g be an convex function $g:R\to R$. If $F^{-1}(t)\leq G^{-1}(t)$, $EX<\infty$ and $EY<\infty$ then $X\leq_{st}Y$ implies $X\leq_{CXTTT}Y$.

Proof: Clearly, under the stated conditions, $\forall u\in(0,\infty)$ and $\forall t\in[0,1]$,

$$P(X>u)\leq P(Y>u)\Rightarrow\int_0^{(F^{-1}(t))^g}P(X>u)du\leq\int_0^{(G^{-1}(t))^g}P(Y>u)du$$

where g is a convex function. Therefore $X\leq_{CXTTT}Y$. Hence the proof.

Now we prove the following theorem, which gives the implication of hazard rate ordering and convex TTT ordering, if the expectations of random variables are finite.

Theorem 4.2 Let X and Y be two non-negative random variables having absolutely continuous distribution functions F and G respectively. Let g be and convex function $g:R\to R$ If $F^{-1}(t)\leq G^{-1}(t)$, $EX<\infty$ and $EY<\infty$ then $X\leq_{hr}Y$ implies $X\leq_{CXTTT}Y$.

Proof: Clearly, under the stated conditions,

$$h_f(u)\geq h_g(u),\quad\forall u>0\Rightarrow P(X>u)=e^{-\int_0^u h_f(x)dx}\leq P(Y>u)=e^{-\int_0^u h_g(x)dx}$$

Then by above theorem, $X\leq_{CXTTT}Y$. Hence the proof.

In a similar way, we can prove the implications of stochastic ordering and increasing convex TTT ordering, and hazard rate ordering and increasing convex TTT ordering, be replacing the function g by an increasing convex function. The results are stated below without proof.

Theorem 4.3 Let X and Y be two non-negative random variables having absolutely continuous distribution functions F and G respectively. Let g be an increasing convex function $g:R\to R$. If $F^{-1}(t)\leq G^{-1}(t)$, $EX<\infty$ and $EY<\infty$ then $X\leq_{st}Y$ implies $X\leq_{CXTTT}Y$.

Theorem 4.4 Let X and Y be two non-negative random variables having absolutely continuous distribution functions F and G respectively. Let g be an increasing convex function $g:R\to R$ If $F^{-1}(t)\leq G^{-1}(t)$, $EX<\infty$ and $EY<\infty$ then $X\leq_{hr}Y$ implies $X\leq_{ICXTTT}Y$.

5. CONCLUSIONS

The main advantage of convex and increasing convex TTT order relation is to order two random variables according to their variability and closeness to 0, even when censored data is available. It needs further study to explore the closure properties as in other ordering behaviors. The concave and increasing concave TTT ordering can be defined easily. Analogous results are straight forward. The results have theoretical and practical applications in reliability theory.

REFERENCES

1. Barlow, R. E. and Campo, R. A. (1975) Total time on test processes and application to failure data analysis , *Research report No. ORC 75-8, University of California.*
2. Klefsjo, B. (1981) On ageing properties and total time on test transform, *Scand. Jr. Statistics*., 9, 37-41
3. Chacko, V.M., Praveena, P.C., and M. Manoharan (2010) Ageing properties of semi-Markov system and Total time on test transform, *Proc. International Congress of Mathematicians Abstract< Hindustan Books (434-435)*, Hyderbad, Aug 19-27.
4. Kochar, S. C., Li., X. and Shaked, M. (2002) The total time on test transform and the excess wealth stochastic orders of distributions, *Adv. Appl. Prob*., 34, 826-845.
5. Shaked, M. and Shanthikumar, J. G., (1994*) Stochastic Orders and their applications,* Academic Press NewYork.
6. Shaked, M. and Shanthikumar, J. G., (2007) *Stochastic Orders*, Springer, NewYork.
7. Nair., U., Sankaran, P. G. and Vinesh Kumar, B. (2008) TTT transforms of order n and their implications in reliability analysis, *J. Appl. Prob,* , 46, 1127-1139.

Red box rules are for proof stage only. Delete before final printing.

Operational Risk Management
A practical approach to intelligent data analysis

Editors
RON S. KENETT, *KPA Ltd., Raanana, Israel; University of Turin, Italy; and NYU-Poly, Center for Risk Engineering, New York, USA*

YOSSI RAANAN, *KPA Ltd., Raanana, Israel; and College of Management, Academic Studies, Rishon Lezion, Israel*

Models and methods for operational risks assessment and mitigation are gaining importance in financial institutions, healthcare organizations, industry, businesses and organizations in general. This book introduces modern Operational Risk Management (OpR) and describes how various data sources of different types, both numeric and semantic sources such as text can be integrated and analyzed. It also demonstrates how OpR is synergetic to other risk management activities such as Financial Risk Management and Safety Management. Many real life examples are presented, mostly based on the MUSING project co-funded by the EU FP6 Information Society Technology Programme. This book provides a unique multidisciplinary perspective on the important and evolving topic of Operational Risk Management.

Operational Risk Management: A practical approach to intelligent data analysis provides practical and tested methodologies for combining structured and unstructured, semantic-based data, and numeric data, in OpR data analysis.

Key Features:

- Explores integration of semantic, unstructured textual data, in OpR.
- Provides novel techniques for combining qualitative and quantitative information to assess risks and design mitigation strategies.
- Presents a comprehensive treatment of 'near-misses' data and incidents in OpR.
- Looks at case studies in the financial and industrial sector.
- Discusses application of ontology engineering to model knowledge used in OpR.

The book will be useful to operational risk practitioners, risk managers in banks, hospitals and industry looking for modern approaches to risk management that combine an analysis of structured and unstructured data. It will also benefit academics interested in research in this field, looking for techniques developed in response to real world problems.

STATISTICS IN PRACTICE

A series of practical books outlining the use of statistical techniques in a wide range of applications areas:

- HUMAN AND BIOLOGICAL SCIENCES
- EARTH AND ENVIRONMENTAL SCIENCES
- INDUSTRY, COMMERCE AND FINANCE

Cover design by www.theoakstudio.co.uk

ISBN [illegible]

WILEY
wiley.com

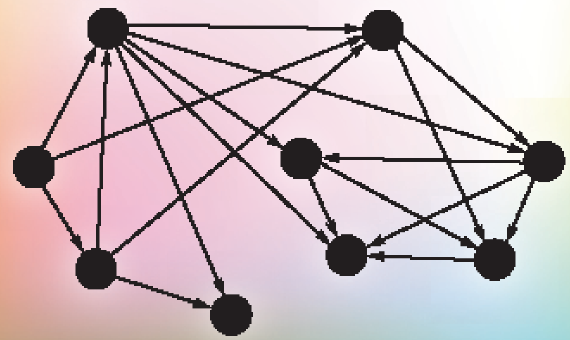
Editors
KENETT
RAANAN

Operational Risk Management
A practical approach to intelligent data analysis

WILEY

Editors
RON S. KENETT
YOSSI RAANAN

Operational Risk Management
A practical approach to intelligent data analysis



WILEY

STATISTICS IN PRACTICE

Operational Risk Management:
a practical approach to intelligent data analysis

ISBN 9780470517666

http://eu.wiley.com/WileyCDA/WileyTitle/productCd-047074748X.html
http://onlinelibrary.wiley.com/book/10.1002/9780470972571

Publisher: John Wiley and Sons, Chichester
Editors: Ron S. Kenett and Yossi Raanan

http://xrl.us/bh8c2v

Introduction to the book

Operational Risk Management is becoming a key competency for organisations in all industries. Financial institutions, regulated by the Basel II accord, need to address it systematically since their level of implementation affects their capital requirements, one of their major operational expenses. Health organisations have been tackling this challenge for many years. The Institute of Medicine reported in 2000 that 44,000 - 98,000 patients die each year in the US as a result of medication errors, surgical errors and missed diagnoses, at an estimated cost to the US economy of $17-$29 billion. Operational risks affect large organisations as well as Small and Medium-sized Enterprises (SMEs) in virtually all industries, from the oil and gas industry, to hospitals, from education to public services.

This multi-author book is about tracking and managing operational risks using state-of-the-art technology that combines the analysis of qualitative, semantic, unstructured data with quantitative data. The examples used are mostly from information technology but the approach is general. As such, the book provides knowledge and methods that can have a substantial impact on the economy and quality of life.

The book has four main parts. Part I is an introduction to Operational Risk Management, Part II deals with data for Operational Risk Management and its handling, Part III covers operational risks analytics and Part IV concludes the book with several applications and a discussion on how Operational Risk Management integrates with other disciplines. The fourteen chapters and the book layout are listed below with short descriptions.

Part I: Introduction to Operational Risk Management

This first part of the book is introductory with a review of modern risk management in general and a presentation of specific aspects of Operational Risk Management issues.

Chapter 1: *Risk Management: A general view* (R. Kenett, R. Pike and Y. Raanan)
The chapter introduces the concepts of risk management and positions Operational Risk Management within the overall risk management landscape. The topics covered include definitions of risks, aspects of information quality and a discussion of state of the art Enterprise Risk Management. The organizations we have in mind are financial institutions implementing Basel II regulations, industrial companies developing, manufacturing and delivering products and services, health care services and others with exposure to risks with potential harmful effects. The chapter is meant to be a general introduction to risk management and a context setting background for the thirteen other chapters of the book.

Chapter 2: *Operational Risk Management: An overview* (Y. Raanan, R. Kenett and R. Pike)
The chapter introduces the general concepts of Operational Risk Management in the context of the overall risk management landscape. Section 2 provides a definition of Operational Risk Management, Section 3 covers the key techniques of this important topic, Section 4 discusses Statistical models and Section 5 covers several measurement techniques for assessing operational risks. The final section summarizes the chapter and provides a roadmap for the book.

Part II: Data for Operational Risk Management and its Handling

Operational Risk Management relies on diverse data sources, and the handling and management of this data requires novel approaches, methods and implementations. This part is devoted to these concepts and their practical applications. The applications are based on case studies that provide practical, real examples for the practitioners of Operational Risk Management.

Chapter 3: *Ontology based modelling and reasoning in operational risks* (C. Leibold, H-U. Krieger and M. Spies)
The chapter discusses design principles of operational risk ontologies for handling semantic unstructured data in Operational Risk Management (OpR). In particular, we highlight the contribution of ontology modelling to different levels of abstraction in OpR. Realistic examples from the MUSING project (MUSING, 2006) and application domain specific ontologies are provided. We draw a picture of axiomatic guidelines that provides a foundation for the ontological framework and refers to relevant reporting and compliance standards and generally agreed best practices.

Chapter 4: *Semantic analysis of textual input* (H. Saggion, T. Declerck, and K. Bontcheva)
Information Extraction is the process of extracting from text specific facts in a given target domain. The chapter gives an overview of the field covering components involved in the development and evaluation of information extraction system such as parts of speech tagging or named entity recognition. The chapter introduces available tools such as the GATE system and illustrate rule-based approaches to information extraction. An illustration of information extraction in the context of the MUSING project is presented.

Chapter 5: *A case study of ETL for operational risks* (V. Grossi and A. Romei)
Integrating both internal and external input sources, filtering them according to rules, and finally merging the relevant data are all critical aspects of business analysis and risk assessment. This is especially critical when internal loss data is not sufficient for effective calculation of risk indicators. The class of tools responsible for these tasks is known as *Extract, Transform* and *Load (ETL)*. The chapter reviews state-of-the-art techniques in ETL and describes an application of a typical ETL processes in the analysis of causes of operational risk failures. In particular, it presents a case study in information technology operational risks in the context of a telecommunication network, highlighting the data sources, the problems encountered during the data merging, and finally the solution proposed and implemented by means of ETL tools.

Chapter 6: *Risk based testing of web services* (X. Bai and R. Kenett)
A fundamental strategy for mitigating operational risks in Web Services and software systems in general is testing. Exhaustive testing of Web Services is usually impossible due to unavailable source code, diversified user requirements and the large number of possible service combinations delivered by the open platform. The chapter presents a risk-based approach for selecting and prioritizing test cases to test service-based systems. The problem addressed is in the context of semantic web services. Such services introduce semantics to service integration and interoperation using ontology models and specifications like OWL-S. They are considered to be the future in WWW evolution. However, due to typically complex ontology relationships, semantic errors are more difficult to detect, as compared to syntactic errors. The models describe in the chapter analyze semantics from various perspectives such as ontology dependency, ontology usage and service workflow, in order to identify factors that contribute to risks in the delivery of these services. Risks are analyzed from two aspects: failure probability and importance, and three layers: ontology data, specific services and composite services. With this approach, we associate test cases to the semantic features and schedule test execution on the basis of risks of their target features. Risk assessment is then used to control the process of Web Services progressive group testing, including test case ranking, test case selection and service ruling out. The chapter presents key techniques used to enable an effective adaptation mechanism: adaptive measurement and adaptation rules. As a statistical testing technique, the approach aims to detect, as early as possible, the problems with highest impact on the users. A number of examples are used to illustrate the approach.

Part III: Operational Risks Analytics

The data described in Part II requires specialized analytics in order to become information and in order for that information to be turned, in a subsequent phase of its analysis, into knowledge. These analytics will be described here.

Chapter 7: *Scoring models for operational risks* (P. Giudici)
The chapter deals with the problem of analyzing and integrating qualitative and quantitative data. In particular it shows how, on the basis of the experience and opinions of internal company “experts”, a scorecard is derived producing a ranking of different risks and a prioritized list of improvement areas and related controls. Scorecard models represent a first step in risk analysis. The chapter presents advanced approaches and statistical models for implementing such models.

Chapter 8: *Bayesian merging and calibration for operational risks* (S. Figini)
According to the Basel II accord, banks are allowed to use the Advanced Measurement Approach (AMA) option for the computation of their capital charge covering operational risks. Among these methods, the Loss Distribution Approach (LDA) is the most sophisticated one. It is highly risk sensitive as long as internal data is used in the calibration process. Given that, LDA is more closely related to the actual risks of each bank. However it is now widely recognized that calibration on internal data only is not enough for computing accurate capital requirements. In other words, internal data should be supplemented with external data. The goal of the chapter is to provide a rigorous statistical method for combining internal and external data and ensure that merging both databases results in unbiased estimates of the severity distribution.

Chapter 9: *Measures of association applied to operational risks* (R. Kenett and S. Salini)
Association rules are a basic analysis tools for unstructured data such as accident reports, call centres recordings and CRM logs. Such tools are commonly used in basket analysis of shopping carts for identifying patterns in consumer behaviour. The chapter shows how association rules are used to analyze unstructured operational risk data in order to provide risk assessments and diagnostic insights. We present a new graphical display of association rules that permits effective clustering of associations with a novel interest measure of association rule called the Relative Linkage Disequilibrium.

Part IV: Operational Risk Applications and its Integration with other Disciplines

Operational Risk Management is not a stand-alone management discipline. This part of the book demonstrates how Operational Risk Management relates to other management issues and Intelligent Regulatory Compliance.

Chapter 10: *Operational Risk Management beyond AMA: New ways to quantify non recorded losses* (G. Aprile, A. Pippi and S. Visinoni)
A better understanding of the impact of IT failures on the overall process of Operational Risk Management can be achieved not only by looking at the risk events with a bottom line effect, but also drilling down to consider the potential risks in terms of missed business opportunities and/or near losses. Indeed, for banking regulatory purposes, only events which are formally accounted for in the books are considered when computing the operational capital at risk. Yet, the "hidden" impact of operational risks is of paramount importance under the implementation of the Pillar 2 requirements of Basel II which expands the scope of the analysis to include reputation and business risk topics. This chapter presents a new methodology in Operational Risk Management that addresses these issues. It helps identify multiple losses, opportunity losses and near misses, and quantifies their potential business impact. The main goals are: 1) to reconstruct multiple-effect losses, which is compliant with Basel II requirements and 2) to quantify their potential impact due to reputation and business risks (opportunity losses) and low level events (near misses), which is indeed a possible extension to Basel II Advanced Measurement Approach (AMA). As a consequence, the proposed methodology has an impact both on daily operations of a bank and at the regulatory level, by returning early warnings on degraded system performance and by enriching the analysis of the risk profile beyond Basel II compliance.

Chapter 11: *Combining operational risks in financial risk assessment scores* (M. Munsch, S. Rohe and M. Jungemann-Dorner)
The chapter's central thesis is that efficient financial risk management must be based on an early warning system monitoring risk indicators. Rating and scoring systems are tools of high value for proactive credit risk management and require solid and carefully planned data management. We introduce a business retail rating system based on the Creditreform solvency index which allows a fast evaluation of a firm's credit worthiness. Furthermore we evaluate the ability of quantitative financial ratings to predict fraud and prevent crimes like money laundering. This practice oriented approach identifies connections between typical financing processes, operational risks and risk indicators, in order to point out negative developments and trends, enabling those involved to take remedial actions in due time and thereby reverse these trends.

Chapter 12: *Intelligent Regulatory Compliance* (M. Spies, R. Gubser and M. Schacher)
In view of the increasing needs for regulation of international markets many regulatory frameworks are being defined and enforced. However, the complexity of the regulation rules, frequent changes and differences in national legislations make it extremely complicated to implement, check or even prove regulatory compliance of company operations or processes in a large number of instances. In this context, the Basel II framework for capital adequacy (soon to evolve to Basel III) is currently being used for defining internal assessment processes in banks and other financial services providers. The chapter shows how recent standards and specifications related to business vocabularies and rules enable Intelligent Regulatory Compliance (IRC). By IRC, we mean semi-automatic or fully automated procedures that can check business operations of relevant complexity for compliance against a set of rules that express a regulatory standard. More specifically, the BMM (Business Motivation Model) and SBVR (Semantics of Business Vocabularies and business Rules) specifications by the Object Management Group (OMG) provide a formal basis for representing regulation systems in a sufficiently formal way to enable IRC of business processes. Besides the availability of automatic reasoning systems, IRC also requires semantics enabled analysis of business service and business

performance data such as process execution logs or trace data. The MUSING project contributed several methods of analysis to the emerging field of IRC (MUSING, 2006). The chapter discusses standards and specifications for business governance and IRC based on BMM and SBVR.

Chapter 13: *Democratization of enterprise risk management* (P. Lombardi, S. Piscuoglio, R. Kenett, Y. Raanan and M. Lankinen)
The chapter highlights the interdisciplinary value of the methodologies and solutions developed for semantically-enhanced handling of operational risks. The three domains dealt with are Operational Risk Management, Financial Risk Management and Internationalisation. These areas are usually treated as 'worlds apart' because of the distance of the players involved, from financial institutions to Public Administrations, to specialised consultancy companies. This proved to be a fertile common ground, not only for generating high value tools and services, but also for a "democratised" approach to risk management, a technology of great importance to SMEs worldwide.

Chapter 14: *Operational risks, quality, accidents and incidents* (R. Kenett and Y. Raanan)
This concluding chapter presents challenges and directions for Operational Risk Management. The first section provides an overview of a possible convergence between risk management and quality management. The second section is based on a mapping of uncertainty behaviour and decision making processes due to Taleb (2007). This classification puts into perspective so called "Black Swans", rare events with significant impact. The third section presents a link between management maturity and the application of quantitative methods in organisations. The fourth section discusses the link between accidents and incidents and the fifth section is a general case study from the oil and gas industry. This illustrates the applicability of Operational Risk Management to a broad range of industries. A final summary section discusses challenges and opportunities in operational risks. Throughout Chapter 14 we refer to previous chapters in order to provide an integrated view of the material contained in the book.

The book presents state of the art methods and technology and concrete implementation examples. Our main objective is to push forward the Operational Risk Management envelope in order to improve the handling and prevention of risks. We hope that this work will contribute, in some way, to organisations who are motivated to improve their Operational Risk Management practices and methods with modern technology. The potential benefits of such improvements are immense.

Part I

INTRODUCTION TO OPERATIONAL RISK MANAGEMENT

Operational Risk Management: A Practical Approach to Intelligent Data Analysis
Edited by Ron S. Kenett and Yossi Raanan
 ISBN: 978-0-470-74748-3

1

Risk management: a general view

Ron S. Kenett, Richard Pike and Yossi Raanan

1.1 Introduction

Risk has always been with us. It has been considered and managed since the earliest civilizations began. The Old Testament describes how, on the sixth day of creation, the Creator completed his work and performed an *ex post* risk assessment to determine if further action was needed. At that point in time, no risks were anticipated since the 31st verse of Genesis reads ‘And God saw every thing that he had made, and, behold, it was very good’ (Genesis 1: 31).

Such evaluations are widely conducted these days to determine risk levels inherent in products and processes, in all industries and services. These assessments use terms such as ‘probability or threat of a damage’, ‘exposure to a loss or failure’, ‘the possibility of incurring loss or misfortune’. In essence, risk is linked to uncertain events and their outcomes. Almost a century ago, Frank H. Knight proposed the following definition:

> Risk is present where future events occur with measureable probability.

Quoting more from Knight:

> Uncertainty must be taken in a sense radically distinct from the familiar notion of risk, from which it has never been properly separated . . . .

Operational Risk Management: A Practical Approach to Intelligent Data Analysis
Edited by Ron S. Kenett and Yossi Raanan
 ISBN: 978-0-470-74748-3

> The essential fact is that 'risk' means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is really present and operating . . . . It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an unmeasurable one, that it is not in effect an uncertainty at all'.
>
> (Knight, 1921)

According to Knight, the distinction between risk and uncertainty is thus a matter of knowledge. Risk describes situations in which probabilities are available, while uncertainty refers to situations in which the information is too imprecise to be summarized by probabilities. Knight also suggested that uncertainty can be grasped by an 'infinite intelligence' and that to analyse these situations theoreticians need a continuous increase in knowledge. From this perspective, uncertainty is viewed as a lack of knowledge about reality.

This separates 'risk' from 'uncertainty' where the probability of future events is not measured. Of course what are current uncertainties (e.g. long-range weather forecasts) may some day become risks as science and technology make progress.

The notion of risk management is also not new. In 1900, a hurricane and flood killed more than 5000 people in Texas and destroyed the city of Galveston in less than 12 hours, materially changing the nature and scope of weather prediction in North America and the world. On 19 October 1987, a shock wave hit the US stock market, reminding all investors of the inherent risk and volatility in the market. In 1993, the title of 'Chief Risk Officer' was first used by James Lam, at GE Capital, to describe a function to manage 'all aspects of risk' including risk management, back-office operations, and business and financial planning. In 2001, the terrorism of September 11 and the collapse of Enron reminded the world that nothing is too big to collapse.

To this list, one can add events related to 15 September 2008, when Lehman Brothers announced that it was filing for Chapter 11 bankruptcy protection. Within days, Merrill Lynch announced that it was being sold to rival Bank of America at a severely discounted price to avert its own bankruptcy. Insurance giant AIG, which had previously received an AAA bond rating (one of only six US companies to hold an AAA rating from both Moody's and S&P) stood on the brink of collapse. Only an \$85 billion government bailout saved the company from experiencing the same fate as Lehman Brothers. Mortgage backers Fannie Mae and Freddie Mac had previously been put under federal 'governorship', to prevent the failure of two major pillars in the US mortgage system. Following these events, close to 1000 financial institutions have shut down, with losses up to \$3600 billion.

The car industry has also experienced such events. After Toyota announced a recall of 2.3 million US vehicles on 21 January 2010, its shares dropped 21%, wiping out $33 billion of the company's market capitalization. These widely publicized events keep reinvigorating risk management.

The Food and Drug Administration, National Aeronautics and Space Administration, Department of Defense, Environmental Protection Agency, Securities and Exchange Commission and Nuclear Regulatory Commission, among others, have all being implementing risk management for over a decade. Some basic references that form the basis for these initiatives include: Haimes (2009), Tapiero (2004), Chorafas (2004), Ayyub (2003), Davies (1996) and Finkel and Golding (1994).

Risk management, then, has long been a topic worth pursuing, and indeed several industries are based on its successful applications, insurance companies and banks being the most notable. What gives this discipline enhanced attention and renewed prominence is the belief that nowadays we can do a better job of it. This perception is based on phenomenal developments in the area of data processing and data analysis. The challenge is to turn 'data' into information, knowledge and deep understanding (Kenett, 2008). This book is about meeting this challenge. Many of the chapters in the book are based on work conducted in the MUSING research project. MUSING stands for MUlti-industry, Semantic-based next generation business INtelliGence (MUSING, 2006). This book is an extended outgrowth of this project whose objectives were to deliver next generation knowledge management solutions and risk management services by integrating Semantic Web and human language technologies and to combine declarative rule-based methods and statistical approaches for enhancing knowledge acquisition and reasoning. By applying innovative technological solutions in research and development activities conducted from 2006 through 2010, MUSING focused on three application areas:

1. *Financial risk management.* Development and validation of next generation (Basel II and beyond) semantic-based business intelligence (BI) solutions, with particular reference to credit risk management and access to credit for enterprises, especially small and medium-sized enterprises (SMEs).
2. *Internationalization.* Development and validation of next generation semantic-based internationalization platforms supporting SME internationalization in the context of global competition by identifying, capturing, representing and localizing trusted knowledge.
3. *Operational risk management.* Semantic-driven knowledge systems for operational risk measurement and mitigation, in particular for IT-intensive organizations. Management of operational risks of large enterprises and SMEs impacting positively on the related user communities in terms of service levels and costs.

Kenett and Shmueli (2009) provide a detailed exposition of how data quality, analysis quality and information quality are all required for achieving knowledge with added value to decision makers. They introduce the term InfoQ to assess the quality of information derived from data and its analysis and propose several practical ways to assess it. The eight InfoQ dimensions are:

1. *Data granularity.* Two aspects of data granularity are measurement scale and data aggregation. The measurement scale of the data must be adequate for the purpose of the study and. The level of aggregation of the data should match the task at hand. For example, consider data on daily purchases of over-the-counter medications at a large pharmacy. If the goal of the analysis is to forecast future inventory levels of different medications, when restocking is done on a weekly basis, then we would prefer weekly aggregate data to daily aggregate data.

2. *Data structure.* Data can combine structured quantitative data with unstructured, semantic-based data. For example, in assessing the reputation of an organization one might combine data derived from balance sheets with data mined from text such as newspaper archives or press reports.

3. *Data integration.* Knowledge is often spread out across multiple data sources. Hence, identifying the different relevant sources, collecting the relevant data and integrating the data directly affects information quality.

4. *Temporal relevance.* A data set contains information collected during a certain period of time. The degree of relevance of the data to the current goal at hand must be assessed. For instance, in order to learn about current online shopping behaviours, a data set that records online purchase behaviour (such as Comscore data, www.comscore.com) can be irrelevant if it is even one year old, because of the fast-changing online shopping environment.

5. *Sampling bias.* A clear definition of the population of interest and how a sample relates to that population is necessary in both primary and secondary analyses. Dealing with sampling bias can be proactive or reactive. In studies where there is control over the data acquisition design (e.g. surveys), sampling schemes are selected to reduce bias. Such methods do not apply to retrospective studies. However, retroactive measures such as post-stratification weighting, which are often used in survey analysis, can be useful in secondary studies as well.

6. *Chronology of data and goal.* Take, for example, a data set containing daily weather information for a particular city for a certain period as well as information on the air quality index (AQI) on those days. For the United States such data is publicly available from the National Oceanic and Atmospheric Administration website (www.noaa.gov). To assess the quality of the information contained in this data set, we must consider the purpose of the analysis. Although AQI is widely used (for instance, for issuing a ‘code red’ day), how it is computed is not easy to figure out. One analysis goal might therefore be to find out how AQI is computed

from weather data (by reverse engineering). For such a purpose, this data is likely to contain high-quality information. In contrast, if the goal is to predict future AQI levels, then the data on past temperatures contains low-quality information.

7. *Concept operationalization.* Observable data is an operationalization of underlying concepts. 'Anger' can be measured via a questionnaire or by measuring blood pressure; 'economic prosperity' can be measured via income or by unemployment rate; and 'length' can be measured in centimetres or in inches. The role of concept operationalization is different for explanatory, predictive and descriptive goals.

8. *Communication and data visualization.* If crucial information does not reach the right person at the right time, then the quality of information becomes poor. Data visualization is also directly related to the quality of information. Poor visualization can lead to degradation of the information contained in the data.

Effective risk management necessarily requires high InfoQ. For more on information quality see Guess (2000), Redman (2007) and Kenett (2008).

We are seeking knowledge and require data in order to start the chain of reasoning. The potential of data-driven knowledge generation is endless when we consider both the increase in computational power and the decrease in computing costs. When combined with essentially inexhaustible and fast electronic storage capacity, it seems that our ability to solve the intricate problems of risk management has stepped up several orders of magnitude higher.

As a result, the position of chief risk officer (CRO) in organizations is gaining popularity in today's business world. Particularly after the 2008 collapse of the financial markets, the idea that risk must be better managed than it had been in the past is now widely accepted (see Kenett, 2009). Still, this position is not easy to handle properly. In a sense it is a new version of the corporate quality manager position which was popular in the 1980s and 1990s. One of the problems inherent in risk management is its almost complete lack of glamour. Risk management done well is treated by most people like electric power or running water – they expect those resources to be ever present, available when needed, inexpensive and requiring very little management attention. It is only when they are suddenly unavailable that we notice them. Risks that were well managed did not materialize, and their managers got little attention. In general, risk management positions provide no avenues to corporate glory. Indeed, many managers distinguish themselves in times of crisis and would have gone almost completely unnoticed in its absence. Fire fighting is still a very prevalent management style. Kenett *et al*. (2008) formulated the Statistical Efficiency Conjecture that stipulates that organizations exercising fire fighting, as opposed to process improvement of quality by design, are less effective in their improvement initiatives. This was substantiated with 21 case studies which were collected and analysed to try to convince management that prevention is carrying significant rewards.

An example of this phenomenon is the sudden glory bestowed on Rudy Giuliani, the former Mayor of New York City, because of his exceptional crisis management in the aftermath of the September 11 terrorist attack on the twin towers. It was enough to launch his bid for the presidency (although not enough, apparently, to get him elected to that office or even to the post of Republican candidate). Had the attacks been avoided, by a good defence intelligence organization, he would have remained just the Mayor of New York City. The people who would have been responsible for the prevention would have got no glory at all, and we might even never have heard about them or about that potential terrible threat that had been thwarted. After all, they were just doing their job, so what is there to brag about? Another reason for not knowing about the thwarted threat, valid also for business risk mitigation strategies, is not exposing the methods, systems and techniques that enabled the thwarting.

Nonetheless, risk management is a critically important job for organizations, much like vaccination programmes. It must be funded properly and given enough resources, opportunities and management attention to achieve concrete results, since it can be critical to the organization's survival. One should not embrace this discipline only after disaster strikes. Organizations should endeavour to prevent the next one by taking calculated, evidence-based, measured steps to avoid the consequences of risk, and that means engaging in active risk management.

1.2 Definitions of risk

As a direct result of risk being a statistical distribution rather than a discrete point, there are two main concepts in risk measurement that must be understood in order to carry out effective risk management:

1. *Risk impact*. The impact (financial, reputational, regulatory, etc.) that will happen should the risk event occur.
2. *Risk likelihood*. The probability of the risk event occurring.

This likelihood usually has a time period associated with it. The likelihood of an event occurring during the coming week is quite different from the likelihood of the same event occurring during the coming year. The same holds true, to some extent, for the risk impact since the same risk event occurring in two different points in time may result in different impacts. These differences between the various levels of impact may even owe their existence to the fact that the organization, realizing that the event might happen, has engaged actively in risk management and, at the later of the two time periods, was better prepared for the event and, although it could not stop it from happening, it succeeded in reducing its impact.

Other base concepts in the risk arena include:

- *Risk event*. An actual instance of a risk that happened in the past.
- *Risk cause*. The preceding activity that triggers a risk event (e.g. fire was caused by faulty electrical equipment sparking).

Risk itself has risk, as measures of risk often are subject to possible change and so measures of risk will often come with a confidence level that tells the reader what the risk of the risk measure is. That is, there may be some uncertainty about the prediction of risk but of course this should never be a reason to avoid the sound practice of risk management, since its application has generated considerable benefits even with less than certain predictions.

1.3 Impact of risk

In her book *Oracles, Curses & Risk Among the Ancient Greeks*, Esther Eidinow shows how the Greeks managed risk by consulting oracles and placing curses on people that affected their lives (Eidinow, 2007). She also posits that risk management is not just a way of handling objective external dangers but is socially constructed and therefore, information about how a civilization perceives risk, provides insights into its social dynamics and view of the world. The type of risks we are concerned with, at a given point in time, also provides insights into our mindset. Specifically, the current preponderance on security, ecological and IT risks would make excellent research material for an anthropologist in 200 years.

This natural tendency to focus on specific types of risk at certain times causes risk issues, as it is exactly the risks you have not been focusing on that can jump up and bite you. In his book *The Black Swan*, Nassim Nicholas Taleb describes events that have a very low probability of occurrence but can have a very great impact (Taleb, 2007). Part of the reasons he gives for these unexpected events is that we have not been focusing on them or their possibilities because of the underlying assumptions we made about our environment (i.e. all swans are white).

It is also true that the impact of many risk events is difficult to estimate precisely, since often one risk event triggers another, sometimes even a chain reaction, and then the measurements tend to become difficult. This distribution of the total impact of a compound event among its components is not of great importance during an initial analysis of risks. We would be interested in the whole, and not in the parts, since our purpose is to prevent the impact. Subsequent, finer, analysis may indeed assign the impacts to the component parts if their happening separately is deemed possible, or if it is possible (and desirable) to manage them separately. A large literature exists on various aspects or risk assessment and risk management. See for example Alexander (1998), Chorafas (2004), Doherty (2000), Dowd (1998), Embrecht *et al*. (1997), Engelmann and Rauhmeier (2006), Jorion (1997), Kenett and Raphaeli (2008), Kenett and Salini (2008), Kenett and Tapiero (2009), Panjer (2006), Tapiero (2004) and Van den Brink (2002).

1.4 Types of risk

In order to mitigate risks the commercial world is developing holistic risk management programmes and approaches under the banner of enterprise risk management (ERM). This framework aims to ensure that all types of risk are considered and attempts are made to compare different risk types within one overall risk measurement approach. There are many ERM frameworks available, but one of the most prevalent is the COSO ERM model created by the Committee of Sponsoring Organizations of the Treadway Commission. This framework categorizes risks within the following types: (1) financial, (2) operational, (3) legal/compliance and (4) strategic.

It is within this framework that this book approaches operational risks. This category is very broad and is present in, and relevant to, all industries and geographies. It covers such diverse topics as IT security, medical malpractice and aircraft maintenance. This diversity means that there are many approaches to measuring operational risk and all differ in terms of quantitative maturity and conceptual rigour. One important scope of the 'operational' category of risks deals with risks that are associated with the operations of information and communications technology (ICT). The reasons for this are that ICT is nowadays a critical component in all enterprises, forming a layer of the business infrastructure, that attracts over half the capital investments of business and thus deserves to be well managed. Moreover, ICT produces diagnostic data that makes tracking, analysing and understanding risk events easier. This encourages getting insights into the causes of risk events and improving their management. These aspects of risk were the focus of the MUSING European Sixth Framework Programme (MUSING, 2006).

1.5 Enterprise risk management

ERM is a holistic approach that views all the areas of risk as parts of an entity called risk. In addition to the fact that the division of risks across the various categories listed above requires tailored decisions, what one organization may call strategic, may be considered operational in another. The view is that the classification into such areas is an important tool to help decompose a very large problem into smaller pieces. However, all these pieces must be dealt with and then looked at by a senior manager in order to determine which risks are dealt with first, which later and which will currently be knowingly ignored or perhaps accepted without any action to manage them.

The basic creed of ERM is simple: 'A risk, once identified, is no longer a risk – it is a management problem.' Indeed, a telling phrase, putting the responsibility and the accountability for risk management and its consequences right where they belong – on the organization's management. It is based on the realization that the issue of what type a risk is – while relevant to the handling of that risk – is totally immaterial when it comes to damages resulting from that risk. Different types of risks may result in similar damages to the organization.

Therefore, the decomposition of risks into separate areas by their functional root causes is no more than a convenience and not an inherent feature of risk. As a result, all risk management efforts, regardless of their functional, organizational or geographical attributes, should be handled together. They should not be treated differently just because of expediency or because some functional areas have 'discovered' risk – sometime disguised by other terms – sooner than other areas. For example, just because accounting deals with financial exposure does not mean that risk management should be subjugated to that functional area. For example the fact that IT departments have been dealing with disaster recovery planning (DRP) to their own installations and services does not mean that risk management belongs in those departments. Risk management should be a distinct activity of the organization, located organizationally where management and the board of directors deem best, and this activity should utilize the separate and important skills deployed in each department – be it accounting, IT or any other department – as needed.

1.6 State of the art in enterprise risk management

A well-established concept that has been deployed across different industries and situations is the concept of three lines of defence. It consists of:

- *The business*. The day-to-day running of the operation and the front office.
- *Risk and compliance*. The continual monitoring of the business.
- *Audit*. The periodic checking of risk and compliance.

This approach has offered thousands of organizations a solid foundation upon which to protect themselves against a range of potential risks, both internal and external. Some organizations adopted it proactively on their own, as part of managing risk, and others may have had it forced upon them through regulators' insistence on external audits.

Regardless of circumstance, the three lines of defence concept is reliable and well proven, but it needs to be periodically updated. Otherwise, its ability to meet the rigours of today's market, where there is an increasing number of risks and regulations, and an ever-increasing level of complexity, becomes outdated.

For the three lines of defence to succeed, the communication and relationship between them needs to be well defined and coordination across all three lines must be clearly established. This is not easy to accomplish. In the majority of organizations, management of the various forms of risk – operational risk, compliance risk, legal risk, IT risk, etc. – is carried out by different teams, creating a pattern of risk silos. Each form of risk, or risk silo, is managed in a different way. This situation leads to a number of negative consequences described below.

1.6.1 The negative impact of risk silos

1.6.1.1 Inefficiency multiplies across silos

Silos may be very efficient at one thing, but that may be at the expense of the overall organization's efficiency. In the case of risk silos, each gathers the information it needs by asking the business managers to provide various information relating to their daily operations and any potential risks associated with them. Because of the silo structure, the business will find itself being asked for this same information on multiple occasions by a multiple of risk silos. These duplicative efforts are inefficient and counterproductive, and lead to frustrated front-office staff disinclined to engage with risk management in the future. The level of frustration is such today that when the recently appointed CEO of a large company asked his senior managers what single change would make their life easier, the reply was to do something to stop the endless questionnaires and check sheets that managers were required to fill out to satisfy risk managers and compliance officers. Frustration among business managers is never a positive development. But it can fully undermine a company's risk management programme as buy-in from the staff is essential.

1.6.1.2 Inconsistency adds to risks

Silos also tend to lead to inconsistency as the same information will be interpreted in different ways by different risk teams. This disparate relationship between risk teams can lead to the failure to recognize potential correlations between various risks. For example, the recent subprime mortgage crisis that has affected so many banks may have been partially avoided if there had been more coordination and communication between the banks' credit departments and those selling mortgages to people with bad credit. Or if the various regulators, whose function it is to reduce those risks, particularly catastrophic risks, were more forthcoming in sharing information with one another and preferred cooperation to turf protection. Similarly the ¤6.4 billion ($7 billion) loss at Société Générale was the result of several risk oversights, combining a lack of control on individual traders as well as a failure to implement various checks on the trading systems themselves. Also contributing was a negligence of market risk factors with risk management failing to highlight a number of transactions having no clear purpose or economic value.

1.6.1.3 Tearing down silos

Major risk events rarely result from one risk; rather they commonly involve the accumulation of a number of potential exposures. Consequently, companies need to coordinate better their risk management functions and establish consistent risk reporting mechanisms across their organizations. Applying this discipline to enterprise-wide risk management can be exceptionally difficult given that risk information is often delivered in inconsistent formats. For example, interest rate risk may be reported as a single value at risk (VaR) number, whereas regulatory compliance or operational risk may be expressed through a traffic-light format. This disparity can make it extremely difficult for a CRO, CEO or any senior executive accurately to rank risk exposures. As a result, organizations are now recognizing the need to establish a common framework for reporting risk. This is being undertaken through various initiatives across different industries – ICAS, Solvency II and the Basel II Accord. These initiatives have contributed to the growth of risk and compliance teams. However, the intent of these regulations is not simply to require firms to fulfil their most basic regulatory requirement and to set aside a defined sum of money to cover a list of risk scenarios. Instead, regulators want firms to concentrate on the methodology used to arrive at their risk assessments and to ensure that the risk management process is thoroughly embedded throughout the organization. This requires sound scenario analyses that bring together risk information from all of the various risk silos. It is worthwhile to note that silos do not exist only in the area of risk management. They tend to show up everywhere in organizations where lack of cooperation, competition among units and tunnel vision are allowed to rein unchecked. A notable example of silos is that of the development of separate information systems for the different functional business divisions in an organization, a phenomenon that until the advent and relatively widespread adoption of enterprise-wide computer systems (like ERP, CRM, etc.) caused business untold billions of dollars in losses, wasted and duplicated efforts and lack of coordination within the business. It is high time that risk management adopted the same attitude.

1.6.1.4 Improving audit coordination

Scenario analysis is very much based on the ability to collate and correlate risk information from all over the organization. This includes close coordination not just across the various risk areas, but also with the internal audit teams. This ensures they are more effective and not simply repeating the work of the risk and compliance teams, but rather adding value by rigorously testing this work. Such a task requires using the same common framework as the risk and compliance teams so that information can be seen in the correct context. When this occurs, everyone benefits. Companies are seeing much greater independence and objectivity in the internal audit role. In an increasing number of organizations the internal audit function is no longer confined to existing within a corner of the finance department and has more direct communication with senior management.

1.6.2 Technology's critical role

The use of integrated technology to facilitate the evolution of the three lines of defence is a relatively new development, but will become essential in ensuring coordination across the three lines. Because it has been hard to clarify the different lines of defence and their relationships, it has been difficult to build a business case for a new system and to build the necessary workflow around these different roles. However, the current technology situation, where completely separate legacy systems are used in the business, risk and audit departments, is becoming intolerable and simply contributing to risk. Everyone is aware of the weaknesses in their own systems, but this knowledge does not always translate across the three lines of defence. This leaves most companies with two choices. The first is to design a new all-encompassing system from scratch. The second is to deploy a system that supports common processes and reporting while allowing each function to continue using specialist solutions that suits its own needs. Successful firms will be those that recognize there are different functionalities in these different spaces, but they are all able to communicate with each other in a common language and through common systems. For example, observations can be shared and specific risk issues can then be discussed through an email exchange and summary reports can be automatically sent out to managers.

For internal auditors, a system that supports common processes and reporting improves efficiency and accuracy. The system can enable all lines of defence to establish risk and control libraries, so that where a risk is identified in one office or department, the library can then be reviewed to see if this risk has been recognized and if there are processes in place to manage this risk. Automating risk identification enables companies to take a smarter, more efficient and more global approach to the internal audit function. For business and risk managers, a system that supports common processes makes risk and compliance much simpler. Risk teams have a limited set of resources and must rely on the business to carry out much of the risk management process. This includes conducting risk and control self-assessments, and recording any losses and control breaches where these losses occur. Using a system that supports common processes means that business managers can accurately and efficiently contribute important information, while not being asked to duplicate efforts across risk silos. Risk managers also can then concentrate on the value-added side of their work and their role.

1.6.3 Bringing business into the fold

Beyond simply helping to get the work done, there are far wider benefits to the organization from using systems that support common processes and the principle behind them. For example, the more front-office staff are exposed to the mechanics of the risk management process (rather than being repeatedly petitioned for the same information from multiple parties), the more they are aware of its importance and their role in it.

A couple of decades ago, total quality management was a fashionable concept in many organizations. In some cases, a dedicated management team was assigned to this area, and the rest of the business could assume that quality was no longer their problem, but someone else’s. This same misconception applies to risk and compliance, unless all management and employees are kept well informed of such processes and their own active role in them.

Today, it is indeed critically important that everyone realizes that risk is their responsibility. This requires a clear and open line of communication and coordination between three lines of defence: business, risk and compliance, and audit. In order to implement ERM within an organization, the key challenge facing organizations and the CROs is the myriad of risk approaches and systems implemented throughout the modern large institution. Not only is there a huge amount of disparate data to deal with, but the basis on which this data is created and calculated is often different throughout the organization. As a result, it becomes almost impossible to view risks across units, types, countries or business lines.

Another side of the challenge facing CROs is that there are many disparate customers for ERM reporting and analysis. Reports need to be provided to senior business line management, directors and board committees, regulators, auditors, investors, etc. Quite often these customers have different agendas, data requirements, security clearances and format requirements. Often armies of risk analysts are employed within the ERM team whose task is to take information from business and risks systems and manually sort, review and merge this to attempt an overall view of the risk position of the company. This process is very resource and time consuming and extremely prone to error.

In other cases, CROs tackle ERM in a piecemeal fashion. They choose certain risk types or business lines that they feel can be successfully corralled and develop an ERM system to load data concerning those risk types or business lines, normalize that data so that it can be collated and then implement an analytic system to review the enterprise risk within the corral. The aim is to generate a quick win and then expand the framework as methodologies and resources become available. While this approach is a pragmatic one, and derives benefit for the organization, it has one major flaw. If you do not consider the entire picture before designing the approach, it can often be impossible to graft on further types of risk or business line in the future. Even if you manage to make the new addition, the design can fall into the 'I wouldn't have started from here' problem and therefore compromise the entire framework.

What is needed is an approach that implements a general ERM framework from the start that can be utilized as needed by the organization. This framework should cover all risk types and provide support for any business line type or risk measurement type. It should enable an organization to collate data in a standard format without requiring changes to specific lines of business or risk management systems. The 14 chapters of this book provide answers and examples for such a framework using state-of-the-art semantic and analytical technologies.

1.7 Summary

The chapter introduces the concept of risk, defines it and classifies it. We also show the evolution of risk management from none at all to today's heightened awareness of the necessity to deploy enterprise risk management approaches. Risk is now at the core of many applications. For example, Bai and Kenett (2009) propose a risk-based approach to effective testing of web services. Without such testing, we would not be able to use web applications reliably for ordering books or planning a vacation. Kenett *et al*. (2009) present a web-log-based methodology for tracking the usability of web pages. Risks and reliability are closely related. The statistical literature includes many methods and tools in these areas (see Kenett and Zacks, 1998; Hahn and Doganaksoy, 2008). Two additional developments of risks are worth noting. The first one is the introduction of Taleb's concept of black swans. A black swan is a highly improbable event with three principal characteristics: (1) it is unpredictable; (2) it carries a massive impact;

and (3) after the fact, we concoct an explanation that makes it appear less random, and more predictable, than it was (Taleb, 2007). Addressing black swans is a huge challenge for organizations of all size, including governments and not-for-profit initiatives. Another development is the effort to integrate methodologies from quality engineering with risk economics (Kenett and Tapiero, 2009). The many tools used in managing risks seek, de facto, to define and maintain the quality performance of organizations, their products, services and processes. Both risks and quality are therefore relevant to a broad number of fields, each providing a different approach to their measurement, their valuation and their management which are motivated by psychological, operational, business and financial needs and the need to deal with problems that result from the uncertainty and their adverse consequences. Both uncertainty and consequences may be predictable or unpredictable, consequential or not, and express a like or a dislike for the events and consequences induced. Risk and quality are thus intimately related, while at the same time each has, in some specific contexts, its own particularities. When quality is measured by its value added and this value is uncertain or intangible (as is usually the case), uncertainty and risk have an appreciable effect on how we deal, measure and manage quality. In this sense, both risk and quality are measured by ‘money’. For example, a consumer may not be able to observe directly and clearly the attributes of a product. And, if and when the consumer does so, this information might not be always fully known, nor be true. Misinformation through false advertising, unfortunate acquisition of faulty products, model defects, etc., have a ‘money effect’ which is sustained by the parties (consumers and firms) involved. By the same token, poor consumption experience in product and services can have important financial consequences for firms that can be subject to regulatory, political and social pressures, all of which have financial implications. Non-quality, in this sense, is a risk that firms assess, that firms seek to value and price, and that firms manage to profit and avoid loss. Quality and risk are thus consequential and intimately related. The level of delivered quality induces a risk while risk management embeds tools used to define and manage quality. Finally, both have a direct effect on value added and are a function of the presumed attitudes towards risk and the demands for quality by consumers or the parties involved in an exchange where it is quality or risk.

This introductory chapter lays the groundwork for the whole book that will move us from the general view of risk to specific areas of operational risk. In the following chapters the reader will be presented with the latest techniques for operational risk management coming out of active projects and research dedicated to the reduction of the consequences of operational risk in today’s highly complex, fast-moving enterprises. Many examples in the book are derived from work carried out within the MUSING project (MUSING, 2006). The next chapter provides an introduction to operational risk management and the successive 12 chapters cover advanced methods for analysing semantic data, combining qualitative and quantitative information and putting integrated risk approaches at work, and benefiting from them. Details on operational risk ontologies and data mining techniques for unstructured data and various applications are presented, including their implication to intelligent regulatory compliance and the analysis of near misses and incidents.

The overall objective of the book is to pave the way for next generation operational risk methodologies and tools.

References

Alexander, C.O. (1998) *The Handbook of Risk Management and Analysis*, John Wiley & Sons, Inc., New York.

Ayyub, B.M. (2003) *Risk Analysis in Engineering and Economics*, Chapman & Hall/CRC Press, Boca Raton, FL.

Bai, X. and Kenett, R.S. (2009) Risk-Based Adaptive Group Testing of Web Services, *Proceedings of the Computer Software and Applications Conference (COMPSAC'09)*, Seattle, USA.

Chorafas, D.N. (2004) *Operational Risk Control with Basel II: Basic Principles and Capital Requirements*, Elsevier, Amsterdam.

Davies, J.C. (Editor) (1996) *Comparing Environmental Risks: Tools for Setting Government Priorities*, Resources for the Future, Washington, DC.

Doherty, N.A. (2000) *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*, McGraw-Hill, New York.

Dowd, K. (1998) *Beyond Value at Risk: The New Science of Risk Management*, John Wiley &, Ltd, Chichester.

Eidinow, E. (2007) *Oracles, Curses & Risk Among the Ancient Greeks*, Oxford University Press, Oxford.

Embrecht, P., Kluppelberg, C. and Mikosch, T. (1997) *Modelling External Events*, Springer-Verlag, Berlin.

Engelmann, B. and Rauhmeier, R. (2006) *The Basel II Risk Parameters*, Springer, Berlin–Heidelberg, Germany.

Finkel, A.M. and Golding, D. (1994) *Worst Things First? The Debate over Risk-Based National Environmental Priorities*, Resources for the Future, Washington, DC.

Guess, F. (2000) Improving Information Quality and Information Technology Systems in the 21st Century, *International Conference on Statistics in the 21st Century*, Orino, ME.

Hahn, G. and Doganaksoy, N. (2008) *The Role of Statistics in Business and Industry*, Wiley Series in Probability and Statistics, John Wiley & Sons,Inc., Hoboken, NJ.

Haimes, Y.Y. (2009) *Risk Modeling, Assessment and Management*, third edition, John Wiley & Sons, Inc., Hoboken, NJ.

Jorion, P. (1997) *Value at Risk: The New Benchmark for Controlling Market Risk*, McGraw-Hill, Chicago.

Kenett, R.S. (2008) From Data to Information to Knowledge, *Six Sigma Forum Magazine*, pp. 32–33.

Kenett, R.S. (2009) Discussion of Post-Financial Meltdown: What Do the Services Industries Need From Us Now?, *Applied Stochastic Models in Business and Industry*, 25, pp. 527–531.

Kenett, R.S. and Raphaeli, O. (2008) Multivariate Methods in Enterprise System Imple- mentation, Risk Management and Change Management, *International Journal of Risk Assessment and Management* , 9, 3, pp. 258–276 (2008).

Kenett, R.S. and Salini, S. (2008) Relative Linkage Disequilibrium Applications to Air- craft Accidents and Operational Risks, *Transactions on Machine Learning and Data Mining* , 1, 2, pp. 83–96.

Kenett, R.S. and Shmueli, G. (2009) On Information Quality, University of Maryland, School of Business Working Paper RHS 06-100, http://ssrn.com/abstract=1464444 (accessed 21 May 2010).

Kenett, R.S. and Tapiero, C. (2009) Quality, Risk and the Taleb Quadrants, *Risk and Decision Analysis* , 4, 1, pp. 231–246.

Kenett, R.S. and Zacks, S. (1998) *Modern Industrial Statistics: Design and Control of Quality and Reliability* , Duxbury Press, San Francisco.

Kenett, R.S., de Frenne, A., Tort-Martorell, X. and McCollin, C. (2008) The Statistical Efficiency Conjecture, in *Statistical Practice in Business and Industry* , Coleman, S., Greenfield, T., Stewardson, D. and Montgomery, D. (Editors), John Wiley &Sons, Ltd, Chichester.

Kenett, R.S., Harel, A. and Ruggerri, F. (2009) Controlling the Usability of Web Services, *International Journal of Software Engineering and Knowledge Engineering* , 19, 5, pp. 627–651.

Knight, F.H. (1921) *Risk, Uncertainty and Profit* , Hart, Schaffner and Marx (Houghton Mifflin, Boston, 1964).

MUSING (2006) IST- FP6 27097, http://www.musing.eu (accessed 21 May 2010). Panjer, H.

(2006) *Operational Risks: Modelling Analytics* , John Wiley & Sons, Inc., Hoboken, NJ.

Redman, T. (2007) Statistics in Data and Information Quality, in *Encyclopedia of Statistics in Quality and Reliability* , Ruggeri, F., Kenett, R.S. and Faltin, F. (Editors in chief), John Wiley & Sons, Ltd, Chichester.

Taleb, N.N. (2007) *The Black Swan: The impact of the highly improbable*, Random House, New York.

Tapiero, C. (2004) *Risk and Financial Management: Mathematical and Computational Methods* , John Wiley & Sons, Inc., Hoboken, NJ.

Van den Brink, G. (2002) *Operational Risk: The New Challenge for Banks* , Palgrave, New York.

2

Operational risk management: an overview

Yossi Raanan, Ron S. Kenett and Richard Pike

2.1 Introduction

Operational risk management is a somewhat new discipline. While financial risks were recognized long ago, they are in fact part of everyday life and not just a business issue; operational risks and their management have been misdiagnosed frequently as human error, machine malfunction, accidents and so on. Often these risks were treated as disconnected episodes of random events, and thus were not managed. With the advancement of computerized systems came the recognition that operational mishaps and accidents have an effect, sometimes a very considerable one, and that they must be brought under control. Today, operational risk management is gaining importance within businesses for a variety of reasons. One of them is the regulatory demand to do so in important sectors of the economy like banking (Basel II, 2006), insurance (Solvency II, 2009) and the pharmaceutical industry (ICH, 2006). Another is the recognition that since operations are something that the business can control completely or almost completely, it ought also to manage the risk associated with these operations so that the controls are more satisfactory for the various stakeholders in the business. This chapter provides an overview of operational risk management (OpR) and enterprise risk management (ERM) as background material for the following chapters of the book.

Operational Risk Management: A Practical Approach to Intelligent Data Analysis
Edited by Ron S. Kenett and Yossi Raanan
 ISBN: 978-0-470-74748-3

2.2 Definitions of operational risk management

Operational risk has a number of definitions which differ mainly in details and emphasis. Although the proper definition of operational risk has often been the subject of past heated debate (International Association of Financial Engineers, 2010), there is general agreement among risk professionals that the definition should, at a minimum, include breakdowns or failures relating to people, internal processes, technology or the consequences of external events. The Bank for International Settlements, the organization responsible for the Basel II Accord regulating risk management in financial institutions, defines operational risk as follows:

> Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.
>
> (Basel II, 2006)

It is this latter definition that will be used here. In layman's terms, operational risk covers unwanted results brought about by people not following standard operational procedures, by systems, including computer-based systems, or by external events.

In the Basel II definition, 'inadequate or failed internal processes' encompass not only processes that are not suitable for their purpose, but also processes that failed to provide the intended result. These, of course, are not the same. Processes may become unsuitable for their purpose due to external events, like a change in the business environment over which the business has no control. Such change might have been so recent that the business or organization did not have the time to adjust itself. Failed processes, on the other hand, mean that the organization has fallen short in their design, implementation or control. Once we include internal auditing as one of the important business processes, it is seen that internal fraud and embezzlements are part of the definition.

The 'people' part covers both the case of human error or misunderstanding and the case of intentional actions by people – whether with intent to cause harm, defraud or cheat, or just innocently cutting corners, avoiding bureaucratic red tape or deciding that they know a better way of executing a certain action. 'Systems' covers everything from a simple printer or fax machine to the largest, most complicated and complex computer system, spread over many rooms, connecting many users and many other stakeholders located in every corner of the globe. Last in this shortlist of categories of operational risk is 'external events'. This innocently looking phrase covers a lot of possible causes for undesired outcomes – from hackers trying to disrupt computer systems, through labour strikes, to terrorist attacks, fires or floods.

Operational risks abound in every sector of the economy and in every human endeavour. Operational risks are found in the health sector, in the transportation sector, in the energy industry, in banking, in education and, indeed, in all activities. Some sectors, because of enhanced sensitivity to risks or because of government regulations, have implemented advanced processes for identifying the risks particular to their activities. However, operational risks exist when any activity occurs, whether we manage them or not. This recognition is beginning to reach the awareness of many management teams in a wide variety of activities (Doebli *et al*., 2003).

An example where operational risks are recognized as a source for large potential losses can be found in the report by the Foreign Exchange Committee (2004) that encourages best practices for the mitigation of operational risks in foreign exchange services. A detailed discussion of risk management in this industry, including an application of Bayesian networks used later in this book, can be found in Adusei-Poku (2005).

On 14 March 2010, the *Sunday Times* published a summary of a 2200-page report investigating the crash of Lehman Brothers on Wall Street described in Chapter 1 (*Sunday Times*, 2010). The report stated that, on May 2008, a senior vice president of Lehman Brothers wrote a memo to senior management with several allegations, all of which proved right. He claimed that Lehman had 'tens of billion of dollars of unsubstantiated balances, which may or may not be 'bad' or non-performing assets or real liabilities', and he was worried that the bank had failed to value tens of billion of dollars of assets in a 'fully realistic or reasonable way' and did not have staff and systems in place to cope with its rapid growth.

Lehman's auditors, Ernst & Young, were worried but did not react effectively. Time was not on Ernst & Young or Lehman Brother's side. By September, the 158-year-old bank was bust, thousands of people had lost their jobs and the world's economy was pitched into a black hole. The court-appointed bankruptcy examiner found Lehman used accounting jiggery-pokery to inflate the value of toxic real-estate assets it held, and chose to 'disregard or overrule the firm's risk controls on a regular basis'. His most juicy finding was Repo 105, which the report alleges was used to manipulate the balance sheet to give the short-term appearance of reducing assets and risk. Not since Chewco and Raptor – Enron's 'off balance sheet vehicles' – has an accounting ruse been so costly.

These events are all examples of operational risks.

In summary, operational risks include most of what can cause an organization harm, that is foreseeable and, to a very large extent, avoidable – if not the events themselves, then at least their impact on the organization. It is quite plain that once we recognize the operational risks that face our enterprise, we can mitigate them. It is important to understand that a risk, once identified, is no longer a risk – it is a management issue. OpR is the collection of tools, procedures, assets and managerial approach that are all aimed together at one goal: to understand the operational risks facing the enterprise, to decide how to deal with them and to manage this process effectively and efficiently. It should be noted that the idea of OpR is, in some sense, a circular problem. The processes and systems used for managing operational risks are all subject, themselves, to the same pitfalls that may cause systems and people to malfunction in other parts of the organization. It is hoped, however, that once OpR is adopted as a basic approach of management, the OpR system itself will be subjected to the same testing, screening and control that every other aspect of the operation is subjected to.

2.3 Operational risk management techniques

2.3.1 Risk identification

In order to manage and control risk effectively, management need a clear and detailed picture of the risk and control environment in which they operate. Without this knowledge, appropriate action cannot be taken to deal with rising problems. For this purpose, risks must be identified. This includes the sources, the events and the consequences of the risks. For this and other risk-related definitions, see also ISO 73 (2009).

Every organization has generic activities, processes and risks which apply to all business areas within the organization. Risk descriptions and definitions should be stored in one repository to allow organizations to manage and monitor them as efficiently as possible. This approach creates a consolidated, organization-wide view of risk, regardless of language, currency, aggregation hierarchy or local regulatory interpretations.

This consolidated view allows the organization to monitor risk at a business unit level. However, it is integral for each business unit to identify and monitor its local risks, as the risks may be unique to that business unit. In any case, a business unit is responsible for its results and thus must identify the risks it faces. In order to do this effectively, risks must be identified. Notwithstanding risks that are common knowledge, like fire, earthquakes and floods, they must also be included in the final list. All other risks, specific to the enterprise, must be identified by using a methodology designed to discover possible risks. This is a critical step, since management cannot be expected to control risks they are unaware of. There are a number of ways of identifying risks, including:

- Using event logs to sift the risks included in them.
- Culling expert opinions as to what may go wrong in the enterprise.
- Simulating business processes and creating a list of undesirable results.
- Systematically going through every business process used in the enterprise and finding out what may go wrong.

- Using databanks of risk events that materialized in similar businesses, in order to learn from their experience.

Some of these methods produce only a list of risks, while others may produce some ideas, more or less accurate, depending on the particular realization of the frequency of these risk events actually happening. This frequency is used to calculate the expected potential damage that may become associated with a particular event and, consequently, for setting the priorities of treating various contingencies.

Organizations ensure consistency in risk identification in two ways:

1. Risk identification is achieved via a centralized library of risks. This library covers generic risks that exist throughout the organization and associates the risks with the organization's business activities. When a business unit attempts to define its local risks and build its own risk list, it does so by considering a risk library. The library itself is typically created by using an industry list as an initial seed, and then augmented by collecting risk lists from every business unit, or it may be created by aggregating the risks identified by each business unit. In either case, this process must be repeated until it converges to a comprehensive list.
2. Identification consistency is further aided by employing a classification model covering both risks and controls. Using this model each risk in the library has an assigned risk classification that can be based on regulatory definitions, and each associated control also has a control classification. The key benefits of classification are that it allows organizations to identify common risks and control themes.

Once risks have been identified, control must be put in place to mitigate those risks. Controls can be defined as processes, equipment or other methods, including knowledge/skills and organization design, that have a specific purpose of mitigating risk. Controls should be identified and updated on a regular basis.

Controls should be:

- Directly related to a risk or a class of risks (not a sweeping statement of good practice).
- Tangible and normally capable of being evidenced.
- Precise and clear in terms of what specific action is required to implement the control.

The process of risk identification should be repeated at regular intervals. This is because risks change, the nature of the business evolves, the regulatory climate (sometimes defining which risks must be controlled) changes, the employees are rotated or replaced, new technologies appear and old technologies are retired. Thus, the risk landscape constantly evolves and, with it, the risks.

2.3.2 Control assurance

A control assurance process aims to provide assurance throughout the business that controls are being operated. It is generally implemented in highly 'control focused' areas of the business where management and compliance require affirmation that controls are being effectively operated.

Control assurance reporting is defined as the reporting of the actual status of a control's performance. This is fundamentally different from the risk and control assessment process discussed in Section 2.3.4, which is concerned with assessing and validating the risk and control environment. Control assurance is a core component of the risk management framework and is used to:

- Establish basic transparency and reporting obligations.
- Establish where 'control issues' occur and ensure that the relevant management actions are taken.
- Highlight insufficiently controlled areas.
- Highlight areas of 'control underperformance'.
- Provide detailed control reporting to various levels of management.

Control assurance is not necessarily undertaken by every area in the business; it is more noticeably present in the areas of the business that require assurance that controls are being effectively operated.

Control assurance is generally performed on a periodic basis, typically monthly or quarterly. Each business unit typically nominates someone to ensure that control assurance reporting is carried out. This does not mean that this is the only person who has controls to operate; rather this person ensures that all controls have been operated by the relevant person in the area for which he/she is responsible.

Business units, in conjunction with appropriate risk management personnel, should define all of the controls within their responsibility. From this, the shortlist of controls to be included in the control assurance process is developed. This shortlist should consider:

- The impact and likelihood of the risk mitigated by the control.
- The effectiveness and importance of the control.
- The frequency of the control operation.
- The regulatory relevance of the control.
- The cost/performance ratio of developing and implementing the control.

The OpR function monitors the control shortlists in conjunction with business units to ensure their appropriateness and adequacy.

2.3.3 Risk event capture

Risk event capture is the process of collecting and analysing risk event data.

An operational risk event, as previously defined, can result in:

- An actual financial loss of a defined amount being incurred – a loss.
- An actual financial profit of a defined amount being incurred – a profit.
- A situation where no money was actually lost but could have been were it not for the operation of a control – a near miss.
- A situation where damage is caused to equipment and to people.

When analysing risk events, it should be possible to identify:

- The controls which failed or the absence of controls that allowed the event to occur.
- The consequence of the event in terms of actual financial loss or profit.
- The correlations between risks – as a financial loss is often the result of more than one risk co-occurring.

Although collecting risk event data is in many cases an external regulatory requirement, it is also beneficial to an organization in that it:

- Provides an understanding of all risk events occurring across the organization.
- Provides quantifiable historical data which the organization can use as input into modelling tools.
- Promotes transparent and effective management of risk events and minimizes negative effects.
- Promotes root cause analysis which can be used to drive improvement actions.
- Reinforces accountability for managing risk within the business.
- Provides an independent source of information which can be used to challenge risk and control assessment data.

The degree of cooperation of front-line workers with the reporting requirements varies and is not uniform – not across industries and not even across a particular organization. As Adler-Milstein *et al*. (2009) show, workers are more likely to report operational failures that carry financial or legal risks.

2.3.4 Risk and control assessments

The management of risks and their associated controls is fundamental to successful risk management. Any risk and control assessment (RCA) process should be structured and consistent to allow for the qualitative assessment of the validity of key business risks and their controls. This is fundamentally different from control assurance which is concerned with providing assurance that controls are being effectively operated.

RCA is a core component of the risk management framework and is used to:

- Identify the key risks to the business.
- Assess the risks in terms of their overall significance for the business based on the judgement of business management.
- Establish areas where control coverage is inadequate.
- Drive improvement actions for those risks which are assessed as outside agreed threshold limits for risk.
- Provide consistent information on the risk and control environment which can be aggregated and reported to senior management to better help in making more informed decisions.

RCA is performed in different areas of the organization, referred to as assessment points. These are identified by the relevant business unit owners. RCA is generally performed on a periodic basis, typically monthly or quarterly. The duration of each assessment is variable and will depend on the number of risks and controls to be assessed. Both business unit owners and members of the risk management team will be involved in each RCA.

RCA is normally a three-step process which allows the business to identify, assess and manage risk:

1. The identification step (which takes place outside of any system) results in a list of the key risks to be included in the assessment.
2. The assessment step allows the business to rank the risks identified in terms of significance to the business and assess the validity of their scoring. This step will include an approval of the assessment.
3. The management step is primarily involved with ensuring improvement actions raised as a result of risks being outside agreed limits are followed up and compiling reporting information.

One of the goals of this activity is to be able to predict the risks facing the organization, so that the priorities for handling them can be properly decided. That is, the goal is to be able to manage the operational risk and bring its size to that level which the organization can tolerate. It is not just about bookkeeping and clerical record keeping, done in order to demonstrate diligence. As Neil *et al*. (2005) note, ‘Risk prediction is inextricably entwined with good management practice and [that] measurement of risk can meaningfully be done only if the effectiveness of risk and controls processes is regularly assessed.’

2.3.5 Key risk indicators

Key risk indicators, or KRIs, are metrics taken from the operations of a business unit, which are monitored closely in order to enable an immediate response by the risk managers to evolving risks. This concept of 'Key X indicators' is not new, nor is it particular to risk management. Its more familiar form is KPI, where P stands for Performance. The basic idea behind these two acronyms is quite similar. Indicators – for risk or for performance – may be quite numerous within a given enterprise. For an industrial firm risk indicators may include:

- Number of defective items produced – in each production line.
- Percentage of defective items produced – in each production line.
- Change – daily, weekly, monthly, etc. – in the number of defective items produced in each production line.
- Number of items returned as defective for each product (again, this may be expressed in numbers, percentages or monetary value).
- Number of maintenance calls for each production line – absolute or per unit of time.
- Number of accidents on the production lines.
- Number of unplanned stoppages of each production line.

For achieving comprehensive OpR in an enterprise, we add to the KPIs listed above operational risk indicators associated with other divisions of the enterprise – finance, marketing, human resources and computer operations. So, it is evident that the number of risk indicators in a given enterprise may be very large, thus making it very difficult to track, monitor and control. Therefore, a select few risk indicators are chosen to serve as a warning mechanism for the enterprise. These may be simple risk indicators like 'number of computer crashes in a week', or 'number of communication breakdowns in a day', or 'costs of unscheduled repairs incurred in the computer centre during a prescribed period of time'. Alternatively, they may be compound indicators, artificial in a sense, made up of direct risk indicators for a given area of activity to create a representative indicator for that activity in such a way that changes in this compound indicator will warn the risk management officer of approaching difficulties.

The KRIs are lagging or leading indicators of the risks facing the enterprise. The way to create them changes from one organization to another, and their construction expresses such attributes as the level of importance that the organization attaches to each of its activities, the regulatory climate under which the organization operates and the organization's appetite for risk. Consequently, two similar organizations serving the same markets may have quite different KRIs. The list of possible KRIs is so long – when compiled from all possible sources – that libraries of KRIs have been set up and some can only be accessed under a subscription agreement – see, for example, KRIL (2010). The actual definition of a particular organization's KRIs requires usually a project targeted at this goal that is usually undertaken as part of an overall OpR approach. For more on KPIs and KRIs see Ograjenšek and Kenett (2008) and Kenett and Baker (2010). A study by Gartner positioning OpR software products is available in McKibben and Furlonger (2008).

2.3.6 Issues and action management

The management of issues and their associated actions is fundamental to successful OpR. The issues and actions management process should provide a standardized mechanism for identifying, prioritizing, classifying, escalating and reporting issues throughout the company.

The collection of issues and actions information allows the business to adopt a proactive approach to OpR and allows for swift reactions to changes in the business environment.

Issues and actions management is a core component of the risk management framework and is used to:

- Support the evaluation of risk likelihood and control effectiveness during the RCA process.
- Highlight control failures or uncontrolled risks during the control assurance process.
- Highlight events resulting in significant financial loss.

Guiding principles state that issues should generally originate from:

- Control improvements.
- Control weaknesses.
- Compliance gaps/concerns.
- Audit recommendations – both financial audit and risk audit.
- Risk event reports.
- Quality defects.

The issue management process should:

- Capture issues related to the RCA and control assurance processes, risk events, internal audits and compliance audits.
- Support the creation of issues on an ad hoc basis.
- Allow for the creation of actions and assign responsibilities and target completion dates for the same.

- Monitor the satisfactory completion of issues and actions.
- Provide reports to support the issue management and action planning process.

2.3.7 Risk mitigation

Risk mitigation is an action, consciously taken by management, to counteract, in advance, the effects on the business of risk events materializing. The risk mitigation strategies for operational risks fall into the same four general categories of risk mitigation used for managing risks of all types. These are:

- Avoid the risk.
- Accept the risk.
- Transfer the risk.
- Reduce the risk.

Avoiding the risk means not taking the action that may generate it. With operational risk, that means not performing the operation. Accepting the risk means that the organization, while well aware of the risk, decides to go ahead and perform the operation that may end in the risk event occurring, and to suffer the consequences of that occurrence. Transferring the risk may be accomplished by a number of methods. The most familiar one is to insure the business against the occurrence of that risk event. This way, the risk is transferred to the insurance company and a probabilistic loss event (the risk actually occurring and causing damage) is substituted by a deterministic, known loss – the insurance premium. Another way of transferring the risk is to subcontract the work that entails the risk, thereby causing some other business to assume the risk. Finally, reducing the risk means taking steps to lower either the probability of the risk event happening or the amount of damage that will be caused if it does occur. It is possible to act on these two distributions simultaneously, thereby achieving a lower overall risk.

Risk mitigation is an important part of risk management in general and operational risk is no exception. In some sense, the area of OpR that is restricted to the management of information and communications technology (ICT) operations has been concerned for quite some time with disaster recovery planning (DRP), which is a detailed plan for continued ICT operations in case a disastrous event happens. However, DRP deals with major disruptions of ICT operations in the enterprise, while risk management deals with all types of risks, large and small. Recently, this area of risk mitigation has been extended to the whole business and the area of business continuity management deals with the ways and means to keep a business going even after a major catastrophe strikes.

2.4 Operational risk statistical models

Operational risks are characterized by two statistical measures related to risk events: their severity and their frequency (Cruz, 2002). A common approach to model the frequency and the severity is to apply parametric probability distribution functions. For severity, the normal and lognormal distributions are often applied. Other distributions used to model the severity are: inverse normal, exponential, Weibull, gamma and beta. For details on these distributions see Kenett and Zacks (1998).

On the other hand, in order to model the frequency of specific operational risk events, two main classes are used: ordinary (Poisson, geometric, binomial) and zero-truncated distributions.

The most common goodness-of-fit test for determining if a certain distribution is appropriate for modelling the frequency of events in a specific data set is the chi-square test. The formal test for testing the choice made for a severity distribution is instead the Kolmogorov–Smirnov test and related measures of interest (see Kenett and Zacks, 1998).

Having estimated, separately, both the severity and the frequency distributions, in operational risk measurement we need to combine them into one aggregated loss distribution that allows us to predict operational losses with an appropriate degree of confidence. It is usually assumed that the random variables that describe severity and frequency are stochastically independent. Formally, the explicit formula of the distribution function of the aggregated losses, in most cases, is often not analytically explicit. One popular practical solution is to apply a Monte Carlo simulation (see Figure 2.1).

On the basis of the convolution obtained following a Monte Carlo simulation, operational risk measurement can be obtained as a summary measures, such as the 99.9th percentile of the annual loss distribution, also called value at risk (VaR). In operational risk the distribution of a financial loss is obtained by multiplying the frequency distribution by the severity distribution. These considerations motivate the use of the geometric mean of risk measures, when aggregating risks over different units. The use of the geometric mean is a necessary condition for preserving stochastic dominance when aggregating distribution functions.

Cause and effect models have also been used extensively in operational risk modelling. Specifically Bayesian methods, including Bayesian networks, have been proposed for modelling the linkage between events and their probabilities. For more on these methods see Alexander (2000, 2003), Giudici and Billota (2004), Cornalba and Giudici (2004), Bonafede and Giudici (2007), Fenton and Neil (2007), Ben Gal (2007), Dalla Valle *et al*. (2008), Figini *et al*. (2010), Kenett (2007) and Chapters 7 and 8 in this book. These and the next chapters include examples from the MUSING project (MUSING, 2006). The next section presents a short overview of classical operational risk measurement techniques.

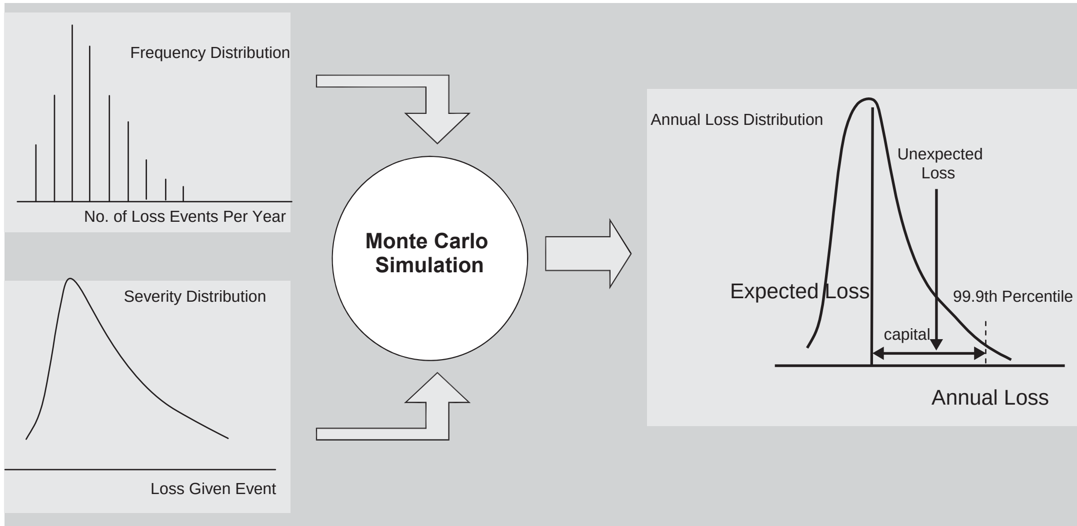


Figure 2.1 Monte Carlo convolution of frequency and severity.

2.5 Operational risk measurement techniques

In order to be able to assess and manage risk, it must be measured. It is impossible to manage anything that is not measured, risk being a prime example of this approach. In this section we introduce three operational risk measurement techniques: the loss distribution approach, scenario analysis and balanced scorecards.

2.5.1 The loss distribution approach

The loss distribution approach (LDA) is a measurement technique that is particularly suitable for banks and other financial institutions. It aims at calculating the VaR, which is a monetary value that these institutions need in order to assign adequate capital, as far as their regulators are concerned, against operational risk (see Figure 2.1). This expected value may be of lesser interest for businesses that have a different approach to risk, for example if they view small losses, bounded above by a periodically changeable limit, as either negligible or part of the cost of doing business. On the other hand, these businesses insure themselves against losses that surpass another dynamically changed amount and consequently implement mitigation strategies to handle only losses that fall between these two bounds. This optional mitigation strategy is not available to banks and many other financial institutions for they function, in effect, as their own insurers and therefore must have a more precise knowledge of the risks, not just some bounds and frequencies. As an example of this type of risk management behaviour one may look at supermarkets and large food sellers in general that have become accustomed, albeit unwillingly, to losses stemming from employee theft – a definite operational risk. Many consider this theft-produced loss a part of doing business as long as it does not rise above a certain level, determined individually by each chain or food store, and take out a specific policy with an insurance company against larger thefts.

The LDA, which is used extensively in calculating the capital requirements a financial institution has to meet to cover credit risks, is a statistically based method that estimates two functions involved with risk – the occurrence frequency and the loss amount frequency. From these two distributions, the distribution of the VaR may be computed. For financial institutions, the VaR has to be calculated for each business line (Basel II, 2006), and then a total VaR is calculated by summing the individual business line VaRs multiplied by their weight in the bank's outstanding credits. While this measuring method is complex to implement and requires extensive databases, some of them external to the bank, and is computationally intensive, there are a number of approaches for financial institutions to calculate it (see e.g. Frachot *et al*., 2001; Tapiero, 2004; Shevchenko, 2009). The effort and investments involved may be worthwhile only for large banks, since it can lead to a significantly smaller capital allocation for operational risk, thus freeing a highly valuable resource for the bank.

For operational risk in other types of business, such a very fine breakdown of events and their consequences may not be required, for a number of reasons.

First, the operational risk is seldom, if ever, related to a business line. Second, operational risk events are frequently the result of more than one causing factor in the wrong range and thus attributing the risk to one of them or distributing it among them will be highly imprecise, to say the least. Third, the costs of implementing such a measurement system may prove prohibitive for a business that is capable of getting insurance against these losses for a small fraction of that cost. A method similar to the LDA is demonstrated for a process that is part of OpR in banks in Chapter 10 describing the near miss/opportunity loss in banks.

2.5.2 Scenarios

Scenarios are used in many areas where the prospects of having accurate predictions are slim or where there are no analytical tools available to produce such predictions at all. They are frequently used for strategic planning in order to discover, as realistically as feasible, what would be a suitable reaction by the business to a wide range of possible developments of many variables that affect the business, in various combinations. Scenarios range from an extension of current reality into the foreseeable future to extreme changes in the business's environment, status, capabilities and associations. Scenarios are used in operational risk measurement in a number of cases. The first case involves an organization that wishes to engage in OpR, but lacks the requisite risk event repository from which to calculate – or even simply summarize – the results of the various risks. That is the most usual case, and it is frequently used because it takes a long time from the initiation of a risk management activity to the time when the organization has a workable repository with enough risk events that materialized. Thus, organizations use the scenario technique in order to shorten the time to the implementation of a risk management approach with the proper mitigation strategies. The second case involves a significant change in the environment that the business operates in. Usually it is a change in the external environment: new regulatory demands, radically changed economic environment, new technologies being brought rapidly to bear on the economic segment the business operates in, and so on. Occasionally, it may be a drastic reorganization of the business, such as a merger of different units into a single one, or a merger with another business or an acquisition of a business and the attempt to assimilate it successfully into the business.

The scenarios technique involves a team, familiar with the business processes being studied, devising possible business scenarios – and trying to see what the reaction of the business might be, and what might go wrong. Doing this systematically, step by step, and covering all possible areas (technology, people, processes, etc.) that might be affected by the scenario, results in a list of potential risk events that are latent within the business process under study. This method is then applied to every business process used in the business until a complete list of latent risk events is compiled. This list is then analysed, categorized and stored as a virtual risk event repository. Then, a measure may be computed for variables that are of interest, including the VaR involved with each risk event. If some data is available that describes the frequency of executing a particular business process, estimates of expected losses can be computed. Mitigation strategies are then devised for each risk event, and the implementation of OpR continues from this point onward.

The benefits of this technique are:

1. It is not dependent on an existing repository of risk events.
2. Even if a risk event repository exists in the business, this technique may prepare the business for risk events that have not yet been registered in the repository – for the simple reason that they had not occurred or that they had occurred prior to the repository being established – but these risks are nevertheless worth considering and preparing mitigation strategies for them.
3. It may be done in a relatively short period of time, eliminating the need for waiting for a significant accumulation of risk events in the risk repository.
4. It may be used in addition to using the risk repository.

The drawbacks of this technique are:

1. It is based on a complete mapping of all business processes in the business. Leaving out a few business processes may make the whole effort not useful since significant portions of the business activity may be left uncovered.
2. It usually requires a large team. The team usually includes people from the risk management office, from the industrial engineering unit and from the operation of the business itself. The core people, like the risk managers and the industrial engineers, may form the central, fixed part of the team, but the people familiar with the various business processes will have to change with each area of activity covered.
3. Lacking any significant history of risk events, it requires a very determined management to undertake such an extensive and expensive activity.

All things considered, it is a good technique, though usually the lack of complete mapping of all business processes prevents it from being very effective. On the other hand, this mapping – a requisite for this technique – may be a very substantial side benefit of this operation and, indeed, it may be a sufficient benefit in and of itself so as to justify the whole process.

2.5.3 Balanced scorecards

Scorecards were made famous in the business world by Norton and Kaplan in the early 1990s (Kaplan and Norton, 1992, 1993, 1996; see also Organjenšek and Kenett, 2008). Since that time, the notion has caught on and today the balanced scorecard (BSC) is widely used in businesses in all disciplines. For an application to organizations developing systems and software see Kenett and Baker (2010). In short, the basic concept of the scorecards is, as the name implies, to compute a score for the measured phenomena and to act upon its changing values. The concept of an operational risk scorecard is the same as that of the general scorecard, except that in this case it is much more specialized and concerns only operational risks in the business. Whereas in the classic BSC the scores represent the performance in the financial, customer, internal processes and learning and growth facets of the business (although many variations exist), in the operational risk scorecard the measured aspects may be technology, human factors and external factors affecting the business operations. This division is by no means unique, and many other divisions may be used. For example, a bank trying to comply fully with the Basel II recommendations may concentrate more heavily on the ICT part of the operations when handling operational risk, and subdivide this score into finer categories – hardware, software, communications, security and interface. Similar subdivisions may be tried out in other areas representing operational risk.

When the complete classification and categorization of all operational risks are completed, weights are assigned to the elements within each category and then a risk score may be computed for each category by providing the values of the individual risks of the elements. The resulting score must be updated frequently to be of value to the organization.

As a final note, it is worthwhile to consider a combined risk indicator, composed of the individual risk categories managed by the organization, which is added to its overall scorecard, thus providing management not only with performance indicators in the classic BSC, but also with an indication of the risk level at which the organization is operating while achieving the business-related indicators.

2.6 Summary

This chapter introduces the basic building blocks of operational risk management, starting from the basic definition of operational risk, through the steps of identifying, classifying, controlling and managing risks. The following chapters, organized in three parts, provide an in-depth analysis of the various ways and means by which operational risk are handled. We briefly describe these three parts.

Part II: Data for Operational Risk Management and its Handling

Operational risk management relies on diverse data sources, and the handling and management of this data requires novel approaches, methods and implementations. This part is devoted to these concepts and their practical applications. The applications are based on case studies that provide practical, real examples for the practitioners of operational risk management. The chapters included in Part II are:

Chapter 3: Ontology-based modelling and reasoning in operational risks
Chapter 4: Semantic analysis of textual input
Chapter 5: A case study of ETL for operational risks
Chapter 6: Risk-based testing of web services

Part III: Operational Risks Analytics

The data described in Part II requires specialized analytics in order to become information and in order for that information to be turned, in a subsequent phase of its analysis, into knowledge. These analytical methods are described in the following chapters:

Chapter 7: Scoring models for operational risks
Chapter 8: Bayesian merging and calibration for operational risks
Chapter 9: Measures of association applied to operational risks

Part IV: Operational Risk Management Applications and Integration with other Disciplines

Operational risk management is not a stand-alone management discipline. This part of the book demonstrates how operational risk management relates to other management issues and intelligent regulatory compliance. The chapters in this part consist of:

Chapter 10: Operational risk management beyond AMA: new ways to quantify non-recorded losses
Chapter 11: Combining operational risks in financial risk assessment scores
Chapter 12: Intelligent regulatory compliance
Chapter 13: Democratization of enterprise risk management
Chapter 14: Operational risks, quality, accidents and incidents

The book presents state-of-the-art methods and technology and concrete implementation examples. Our main objective is to push forward the operational risk management envelope in order to improve the handling and prevention of risks. We hope that this work will contribute, in some way, to organizations which are motivated to improve their operational risk management practices and methods with modern technology. The potential benefits of such improvements are immense.

References

Adler-Milstein, J., Singer, S.J. and Toffel, M.W. (2009) Operational Failures and Problem Solving: An Empirical Study of Incident Reporting, Harvard Business School Technology and Operations Management Unit, Working Paper No. 10-017. http://ssrn.com/abstract=1462730 (accessed 21 May 2010).

Adusei-Poku, K. (2005) Operational Risk Management – Implementing a Bayesian Network for Foreign Exchange and Money Market Settlement, PhD dissertation, Faculty of Economics and Business Administration of the University of Gottingen.

Alexander, C. (2000) Bayesian Methods for Measuring Operational Risk, http://ssrn.com/abstract=248148 (accessed 21 May 2010).

Alexander, C. (2003) *Operational Risk: Regulation, Analysis and Management*, Financial Times/Prentice Hall, London.

Basel Committee on Banking Supervision (2006) Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version. http://www.bis.org/publ/bcbs128.htm (accessed 21 May 2010).

Ben Gal, I. (2007) Bayesian Networks, in *Encyclopaedia of Statistics in Quality and Reliability*, ed. F. Ruggeri, R.S. Kenett and F. Faltin, John Wiley & Sons, Ltd, Chichester.

Bonafede, E.C. and Giudici, P. (2007) Bayesian Networks for Enterprise Risk Assessment, *Physica A*, 382, 1, pp. 22–28.

Cornalba, C. and Giudici, P. (2004) Statistical Models for Operational Risk Management, *Physica A*, 338, pp. 166–172.

Cruz, M. (2002) *Modeling, Measuring and Hedging Operational Risk*, John Wiley & Sons, Ltd, Chichester.

Dalla Valle, L., Fantazzini, D. and Giudici, P. (2008) Copulae and Operational Risk, *International Journal of Risk Assessment and Management*, 9, 3, pp. 238–257.

Doebli, B., Leippold, M. and Vanini, P. (2003) From Operational Risk to Operational Excellence, http://ssrn.com/abstract=413720 (accessed 11 January 2010).

Fenton, N. and Neil, M. (2007) *Managing Risk in the Modern World: Applications of Bayesian Networks*, London Mathematical Society, London.

Figini, S., Kenett, R.S. and Salini, S. (2010) Integrating Operational and Financial Risk Assessments, *Quality and Reliability Engineering International*, http://services.bepress.com/unimi/statistics/art48 (accessed 6 March 2010).

Frachot, A., Georges, P. and Roncalli, T. (2001) Loss Distribution Approach for Operational Risk and Unexpected Operational Losses, http://ssrn.com/abstract=1032523 (accessed 21 May 2010).

Giudici, P. and Bilotta, A. (2004) Modelling Operational Losses: a Bayesian Approach, *Quality and Reliability Engineering International*, 20, pp. 407–417.

ICH (2006) The International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use, *Guidance for Industry: Q9 Quality Risk Management*, http://www.fda.gov/RegulatoryInformation/Guidances/ucm128050.htm (accessed 6 March 2009).

International Association of Financial Engineers (2010) http://www.iafe.org/html/cms_orc.php (accessed 8 March 2010).

ISO GUIDE 73 (2009) Risk management – Vocabulary.

Kaplan, R.S. and Norton, D.P. (1992) The Balanced Scorecard – Measures that Drive Performance, *Harvard Business Review*, 70, 1, pp. 71–79.

Kaplan, R.S. and Norton, D.P. (1993) Putting the Balanced Scorecard to Work, *Harvard Business Review*, 71, 5, pp. 134–142.

Kaplan, R.S. and Norton, D.P. (1996) *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School Press, Boston, MA.

Kenett, R.S. (2007) Cause and Effect Diagrams, in *Encyclopaedia of Statistics in Quality and Reliability*, ed. F. Ruggeri, R.S. Kenett and F. Faltin, John Wiley & Sons, Ltd, 2007.

Kenett, R.S. and Baker, E. (2010) *Process Improvement and CMMI for Systems and Soft- ware: Planning, Implementation, and Management*, Taylor & Francis Group, Auerbach Publications, Boca Raton, FL.

Kenett, R.S. and Zacks, S. (1998) *Modern Industrial Statistics: Design and Control of Quality and Reliability*, Duxbury Press, San Francisco.

KRIL (2010) The KRI Library, http://www.kriex.org/ (accessed 7 February 2010). McKibben, D. and Furlonger, D. (2008) Magic Quadrant for Operational Risk Management Software for Financial Services, Gartner Industry, Research Note G00157289.

MUSING (2006) IST- FP6 27097, http://www.musing.eu (accessed 21 May 2010).

Neil, M., Fenton, N. and Tailor, M. (2005) Using Bayesian Networks to Model Expected and Unexpected Operational Losses, *Risk Analysis Journal*, 25, pp. 963–972.

Ograjenšek, I. and Kenett, R.S. (2008) Management Statistics, in *Statistical Practice in Business and Industry*, ed. S. Coleman *et al*., John Wiley & Sons, Ltd, Chichester. Shevchenko, P.V. (2009) Implementing Loss Distribution Approach for Operational Risk, *Applied Stochastic Models in Business and Industry*, DOI: 10.1002/asmb.811.

Solvency II (2009) http://www.solvency-2.com/ (accessed 21 May 2010).

Sunday Times (2010) Lehman's $50 Billion Conjuring Trick: A report into the Ameri- can bank's collapse reveals financial chicanery and negligent management, March 14. Quoted from http://www.blacklistednews.com/news-7798-0-24-24–.html (accessed 21 May 2010).

Tapiero, C. (2004) *Risk and Financial Management: Mathematical and Computational Methods*, John Wiley & Sons, Inc., Hoboken, NJ.

The Foreign Exchange Committee (2004) Management of Risk Operational in For- eign Exchange, *Risk Analysis*, 25, 4, http://www.ny.frb.org/fxc/2004/fxc041105b.pdf (accessed 7 March 2010).

ISSN 1932-2321