ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA ŠPECIÁLNEHO INŽINIERSTVA

KRÍZOVÝ MANAŽMENT - 2/2010

POSSIBILITIES OF QUANTIFIED RISK ASSESSMENT

Jiří Stodola[1], Petr Stodola[2]

SUMMARY:

This article deals with possibilities of fully qualified decision-making in cases of uncertainty, absence of information, crises situation etc. The selected techniques being explained apply to both reliability and safety engineering as well as to optimizing system maintenance strategies. The techniques of risk assessment deal with reliability, availability, maintainability and safety.

1. INTRODUCTION

Risk, safety, and reliability technology has not developed as a unified discipline, but has grown out of their integration of number activities which were previously the province of the engineer. Since no human activity can enjoy zero risk, and no equipment a zero risk rate of failure, there has grown a safety technology for optimizing risk. This attempts to balance the risk against the benefits of the activities and the cost of further risk reduction. Similarly, safety, and reliability engineering, beginning in the design and production phases, seeks to select the design and production compromise which balances the cost of failure reduction against the value of the enhancement. The design of safety-related system (for example, military technique, road and railway vehicles, etc.) has evolved partly in response to the emergence of new technologies but largely as a result of lessons learnt from failures. The application of technology to hazardous areas requires the formal application of this feedback principle in order to maximize the rate of reliability improvement. Nevertheless, all engineered products will exhibit some degree of reliability growth even without formal improvement programmers. The advent of the informatics age, accelerated in the mid-1980s, led to the need for more complex mass-produced component parts with a higher degree of variability in the parameters and dimensions involved. The experience of poor field reliability of military equipment focused attention on the need for more formal methods of reliability engineering. This gave rise to the collection of failure information from both the field and from the interpretation of test data. The process industries become aware that, with larger plants involving higher inventories of hazardous material, the practice of learning by mistakes was no larger acceptable. Methods were developed for identifying hazards and for quantifying the consequences of failures. The techniques for quantifying the predicted frequency of failures were previously applied mostly in the domain of availability, where the cost of equipment failure was the prime concern. The tendency in the last few years has been for these techniques also to be used in the field of hazard assessment.

2. RELIABILITY, RISK PREDICTION AND SAFETY INTEGRITY

System modeling, by means of failure mode analysis and fault tree analysis methods, has been developed in recent years and now involves numerous software tools which enable predictions to be refined throughout the design cycle. The criticality of the failure rates of specific component parts can be assessed and, by successive computer runs, adjustments to the design configuration and to the maintenance philosophy can be made early in the design cycle in order to optimize reliability and availability. The subject of reliability prediction, based on the concept of

[1] Jiří Stodola, Prof. Ing. DrSc., Faculty of Special Technology, Department of Special Technology, Alexander Dubcek University of Trenčín, Študentská str. 2, 911 50 Trenčín, Slovak Republic, e-mail: jiri.stodola@unob.cz
[2] Petr Stodola, Ing. PhD., Faculty of Economic and Management, Department of Military Management and Tactic, University of Defence Brno, Kounicova str. 65, 662 10 Brno, Czech Republic, petr.stodola@unob.cz

validity repeatable component failure rates, has become controversial. First, the extremely wide variability of failure rates of allegedly identical components under supposedly identical environmental and operating conditions is now acknowledged. The apparent precision offered by reliability prediction models thus not compatible with the accuracy of the failure rate parameter. As a result, it can be concluded that simplified assessments of rates and the use of simple models suffice. In the case, more accurate predictions can be both misleading and a waste of money. The main benefit of reliability prediction of complex systems lies not in the absolute figure predicted but in the ability to repeat the assessment for different repair times, different redundancy arrangements in the design configuration and different values of component failure rate. This has been made feasible by the emergence of computer tools such as fault tree analysis packages, which permit rapid reruns of the prediction. Thus, judgments can be made on the basis of relative predictions with more confidence than can be placed on the absolute values. Second, the complexity of up-to-date engineering products and systems ensures that system failure does not analyse follow simply from component part failure. Factors such as:

- Failure resulting from software elements,
- Failure due to environmental factors,
- Failure due to operating documentation,
- Failure due to human factors,
- Common made failure whereby redundancy etc.

The need of assess the integrity of systems containing substantial elements of software increased significantly. The concept of validly repeatable elements, within the software, which can be mapped to some model of system reliability, is even more controversial than the hardware reliability prediction processes. The extrapolation of software test failure rates into the field has not established itself as a reliable modeling technique. The search for software metrics which enable failure rate to be predicted from measurable features of the code or design is equally elusive. Reliability prediction techniques, however, are mostly confident to the mapping of component failures to system failure and do not address these additional factors [1]. Methodologies are currently evolving to model common mode failures, human factors failures and software failures, but there is no evidence that the models which emerge will enjoy any greater precision than the existing reliability predictions based on hardware component failures. In any case the very thought process of setting up a reliability model is far more variable than the numerical outcome. The problem of matching a reliability or risk prediction to the eventual field performance consist of design (duplication, component selection, design qualification, equipment diversity), manufacture (control, quality assurance, production testing, method study, process instruction), and field (failure feedback, replacement strategy, preventive maintenance, user interaction). In practice prediction addresses the component-based design reliability, and it is necessary to take account of the additional factors when assessing the integrity of a system. The design reliability is likely to be the figure suggested by a prediction exercise. However, there will be many sources of failure in addition to the simple random hardware failures predicted in this way. Thus the achieved reliability of a new product or system is likely to be an order, or even more, less than the design reliability. Reliability growth is the improvement that takes place as modifications are made as a result of field failure information. A well-established item, perhaps with tens of thousands of field necessary to consider quantitative of field hours, might start to approach the design reliability. As a result of the problem, whereby systematic failures cannot necessarily be quantified, it has become generally accepted that it is necessary to consider qualitative defenses against systematic failures as an additional, and separate, activity to the task of predicting the probability of so-called random hardware failures. Thus, two approaches are taken and exist side by side:

1. Quantitative assessment;
2. Qualitative assessment;

Quantitative assessment predicts the frequency of hardware failures and compares them with some target. In the target is not satisfied then the design is adapted until the target is met. Qualitative assessment attempts to minimize the occurrence of systematic failures by applying a variety of defenses and design disciplines appropriate to the severity of the target. The question arises as to how targets can be expressed for the latter qualitative approach. The concept is to divide the spectrum of integrity into a number of discrete levels and then to lay down requirements. If we try to identify the characteristic of design or construction which have secured their longevity then three factors emerge:

Complexity: The fewer component parts and the few types of material involved then, in general, the grater is the likelihood of a reliable item. Up-to-date equipment, so often condemned for its unreliability, is frequently composed of thousands of component parts all of which interact within various tolerances. These could be called intrinsic failures, since they arise from a combination of draft conditions rather than the failure of a specific component. They are more difficult to predict and are therefore less likely to be foreseen by the designer.

Duplication: The use of additional, redundant, part whereby a single failure does not cause the overall system to fail is a frequent method of achieving reliability. It is probably the major design feature which determines the order of reliability that can be obtained. Nevertheless, it adds capital cost, weight, and maintenance and power consumption. Furthermore, reliability improvement from redundancy often affects one failure mode at the expense of another type of failure.

Excess strength: Deliberate design to withstand stress higher than are anticipated will reduce failure rates. Small increases in strength for a given anticipated stress result in substantial improvements. This applies equally to mechanical and electrical items. Modern commercial pressures lead to the optimization of tolerance and stress margins which just the functional requirements.
The last two of above methods are costly and, the cost of reliability improvements needs to be paid for by a reduction in failure and operating cost. This argument is not quite so simple for hazardous failures but, nevertheless, there is never an endless budget for improvement and some consideration of cost is inevitable. We can see therefore that reliability and safety are built-in features of a construction, be it mechanical, electrical or structural. Maintainability also contributes to the availability of a system, since it is the combination of failure rate and repair/down time which determines unavailability. Achieving reliability, safety and maintainability results from activities in three main areas:

Design: (reduction in complexity, duplication to provide fault tolerance, stress factors, qualification testing and design review, feedback of failure information to provide reliability growth).

Manufacture: (control of materials, methods, changes; control of work methods and standards).

Field use: (adequate operating and maintenance instruction, feedback of field failure information, replacement and spark strategies).

It is much more difficult, and expensive, to add reliability/safety after design stage. The quantified parameters must be part of the design specification and can no more be added in retrospect than power consumption, weight, signal-to-noise ratio, etc.

3. RISK ASSESSMENT (QRA)

3. 1 Frequency and consequence

The term Quantified Risk Assessment (QRA) refers to the process of assessing the frequency of an event and its measurable consequences (e.g. fatalities, damage).

Having identified a hazard, the term risk analysis is often used to embrace two types of assessment:
- Frequency or probability of the event (the probability of an accidental release of a given quantity of toxic material might be 1 to 10 000 years);
- The consequences of the event (the consequence, following a study of the toxic effects and having regard to the population density, might to 40 fatalities);

The analysis of consequence is a specialist area within each industry and may be based on nuclear, electrical, chemical, gas or military technology. In many cases the method is identical, particularly where the event is dependent only on:
- Human error,
- Systematic failures,
- Random hardware failures,
- Random software failures.

3. 2 Risk and ALARP

The principle of ALARP (As Low As Reasonably Practicable) describes the way in which risk is treated legally and by the HS (Health and Safety). The concept is that all reasonable measures will be taken in respect of risk which lies in the tolerable zone to reduce them further until the cost of further risk reduction is grossly disproportionate to the benefit. In any case it is always necessary, whatever the cost benefit arguments, to

demonstrate the application of good practice. Figure 1 shows the so-called ALARP triangle which illustrates these regions.

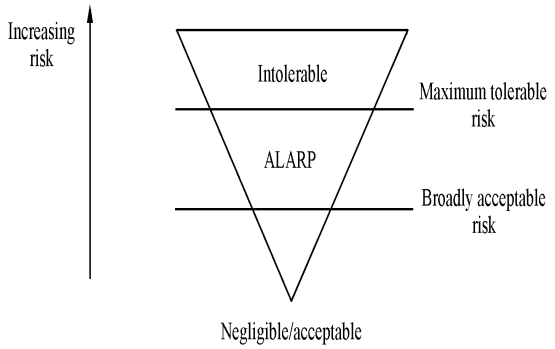

Figure 1 ALARP triangle [1]

It is at this point that the concept of cost per life saved arises, would regard as becoming grossly disproportionate to a reduction in risk. Perception of risk is certainly influenced by the circumstances. A far higher risk is tolerated from voluntary activities than involuntary risks. Compare, also, the fatality rates of cigarette smoking and those associated with train travel etc. They are three orders magnitude apart. Furthermore the risk associated with multiple, as opposed of the single, fatalities is expected to be much lower in the former case. It is sometimes perceived that the level of risk which is acceptable to the public should be lower than to an employee who is deemed to have chosen to work in a particular occupation. Members of the public, however, endure risks without consent or even knowledge. Yet another factor is the difference between individual and societal risk. An accident with multiple fatalities is perceived as less acceptable than the some number occurring individually. Thus, whereas the 10^{-4} level might be tolerated for road vehicles (single death – voluntary), event 10^{-6} might not satisfy everyone in the case of nuclear power station (multiple deaths – involuntary) incident. Figure 2 [2] shows how, for a particular industry or application, the Intolerable. Tolerable and Negligible or Acceptable regions might be defined and how they can be seen to reduce as the number of fatalities increases. Thus for a single fatality risks of 10^{-5} to 10^{-3} are regarded as ALARP. Above 10^{-3} is unacceptable and below 10^{-5} is acceptable. For 10 fatalities, however, the levels are 1é times more stringent.

3. 3 Hazard identification

Hazard Identification (HAZID) is used to identify the possible hazards, Hazard and Operability Studies (HAZOP) is used to establish how the hazards might arise in a process whereas Hazard Analysis (HAZAN) refers to the process of analyzing the outcome of a hazard. This is known as Consequence Analysis. This is carried out at various levels of detail from the earliest stages of design throughout the project design cycle. Preliminary Hazard Analysis, at the early system design phase, identifies safety critical areas, identifies and begins to quantify hazards and begins to set safety targets. It may include: previous experience, review of hazardous materials, legislation, standards, regulations, impact on the environment, interfaces with operators, etc. the purpose of a HEZOP is to identify hazards in the process. HEZOP is a study carried out by a multidisciplinary team, who apply guidewords to identify deviations from the design intent of a system and its procedures. The team attempt to identify the causes and consequences of these deviations and the protective systems installed to minimize them and thus to make recommendations which lead risk reduction. This requires a full description of the design and a full working knowledge of the operating arrangements. A HEZOP is thus usually conducted by a team which includes and operators as well as the safety engineer. A key feature is the HEZOP team leader who must have experience of HEZOP and be full time in the sense that he attends the whole study whereas some members may be part time. An essential requirement for the leader is experience of HEZOP in other industries so as to bring as wide a possible view to the probing process [3]. Detailed recording of problems and actions is essential – during the meeting. Follow-up and review of actions must also be formal. The procedure will involve: define the scope and objectives, define the documentation required, select the team, pre-reading, carry out and record, implement the follow-up action etc. In order to formalize the analysis a guideword methodology has evolved in order to point the analysts at the types of deviation. The guidewords are applied to each of the process parameters such is flow, temperature, pressure, velocity, acceleration, amplitude, voltage, current etc. under normal operational as well as start-up and shut-down modes [5]. Account should be taken of safety systems which are allowed, under specified circumstances, to be temporarily defeated.

Table 1 describes example of possible the HAZOP approach [5]. Each deviation of a parameter must have a credible cause, typically a component or human error related failure or a deviation. Causes lead to

consequences which need to be assessed. When a parameter has varied beyond the design intent then it might lead to vessel rupture, fire, explosion, toxic release, etc. The likelihood may also be assessed. The reliability prediction techniques can be used to predict the frequency of specific events [4]. However, these techniques may be reserved for the more qualitative approach at the HEZOP stage might be to assign, using team judgment only, and say 5 grades of likelihood. A similar approach can be adopted for severity pending more formal quantification of the more severe consequences.

Possible grades of likelihood and classifying of severity is in Table 2 [3]. HAZOP is very suitable for applying to finalized plant design drawings etc. Typical phases of the life cycle and types of equipment at which HAZOP might be applied are: conceptual and detailed design, proposed modification, regulatory requirements, transport systems, buildings and structures, mechanical and military equipment, electricity distribution etc.

Whereas HAZOP is an open-ended approach, HAZID is a checklist technique. At an early stage, such as the feasibility study for a hazardous plant, HAZID enables the major hazards to be identified. At the conceptual stage a more detailed HAZIP would involve designing out some of the major problems. Often, the HAZID uses a questionnaire approach and each organization tends to develop and evolve its own list, based on experience. HAZAN (consequence analysis) is technique applied to select hazards following the HEZOP and HAZID activities. It is usually the high-consequence activities such as major spillage of flammable or toxic materials or explosion which are chosen. High-consequence scenarios usually tend to be the low-probably hazards. Consequence analysis requires a detailed knowledge of the materials or hazards involved in order to predict the outcome of the varies failures. The physic and chemistry of the outcomes in necessary in order to construct mathematical models necessary to calculate the effects on objects and human beings. Some example are: ground, see, air, and space vehicle impact (on structures and human), explosion (pressure vessels and chemicals) or nuclear contamination, large scale water release (vessels, pipes, dams, etc.), flammable and toxic releases (heat radiation, food and water pollution and poisoning), structural collapse etc.

4. CONSLUSIONS

Minimization of failures and errors is an important goal. Much clearer and more consistent basis for error analysis, tracking learning, defining minimum error rates, and inter-comparing different technological and military systems has recently been established. The approach applied to the assessment consisted in as follows: to analyze the data, determine trends, and compare them to the minimum error rate theory [6]. The quality management, the goal of zero failures is stated as the output for any process and its improvement. At present we are sure that errors occur all the time and cannot be reduced to zero. We live in a technological environment, and are exposed to risk and errors and the fear of death. But there are many possibilities available how to assess and evaluate risk, hazard, threat, reliability, technology etc. which can lead and result in problems optimization. Some methods are comprised in this article. The principal aim of the article consists in presenting the fact how we can learn from the many errors and accidents which have spread in developing technique and technology.

5. ACKNOWLEDGEMENT

This paper has been supported by the research project of the Faculty of Military Technology, University of Defense Brno, Project No. MO0FVT0000401 founded by Ministry of Defense of the Czech Republic.

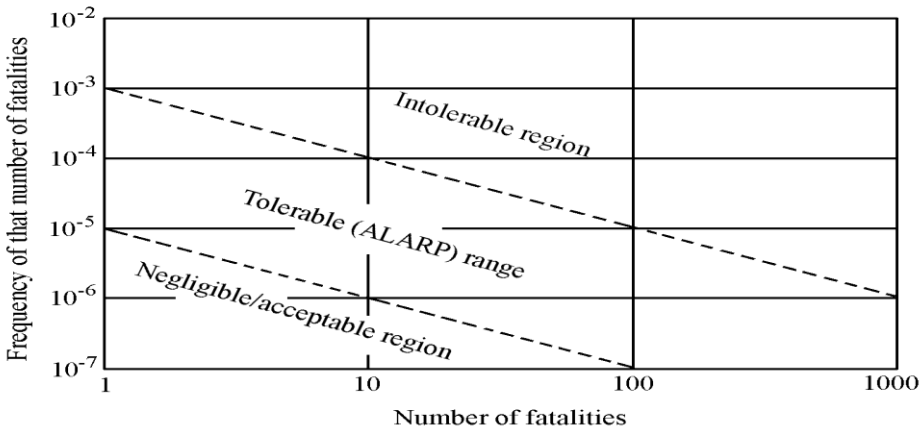

Figure 2 Example of acceptable, tolerable and intolerable region [2]

Table 1 Example of possible HEZOP approach [5]

Guideword	Meaning	Explanation
NO or NOT	The parameter is zero	Something does happen but no order effect
MORE THAN or LESS THAN	There are increases or decreases in the process parameter	Flows and temperatures etc. are not normal
AS WELL AS	Qualitative increase	Some additional effect
PART OF	Qualitative increase	Partial effect
THE REVERSE	Opposite	Reverse flow or material etc.
OTHER THAN	Substitution	Totally different effect

Table 2 Example of possible grades of probability and classifications of severity [3]

Grades of likelihood	Classification of severity
Not more than in the plant life	No impact on plant or personnel
Up to once in 10 years	Damage to equipment only or minor releases
Up to once in 5 years	Injures to unit personnel
Up to once a year	Major damage, limited off-site consequences
More frequent than annually	Major damage and extensive off-site consequences

REFERENCES

[1] SMITH,J,D.: Reliability, Maintainability and Risk. 1st edition. Elsevier Ltd. Oxford, 2005,, ISBN 978-0-7506-6694-7

[2] SMITH,J,D.- SIMPSON,L,K.: Functional Safety: A Straightforward Guide to IEC 61508. 2nd edition. Butterworth-Heinemann, 2004. ISBN 0 7506 6269

[3] DUFFEY,B, R.-SAULL,W, J: Know the Risk. Elsevier Science Ltd. Belington, 2003. ISBN 0-7506-7596-9, (p 227)

[4] BENEŠ,L.-ROSICKA,Z.-FLEISSIG,P.: Vita in SocieteSecura. 1st edition. Univerzita Pardubice. 2008. ISBN 978-80-7395-117-7

[5] O´CONNOR,D,P.: Practical Reliability Engineering. John Willey & SONS, LTD, 2006. ISBN 0-47084462-90 (p 513)

[6] STODOLA, J. – STODOLA,P.: Safety Assessment of Special Systems. Crisis management. Volume 8, No. 1, 2009. ISSN 1336-0019 (str. 71 – 80)