Risk assessment and safety engineering; applications for computer systems[1]

Björn Wahlström
VTT Industrial Systems
POB 1301, FIN-02044 VTT (Espoo)
Finland

1 INTRODUCTION

The modern society relies to an increasing extent on computers for various functions. This development has brought efficiency into the production of goods and services. Unfortunately however, this development has also brought an increasing societal dependence on the computer systems, which may be challenged by deficient designs, malicious actions or a combination of these. This fact has put a large emphasis on safety and security in the design of all kinds of computer systems.

Risk assessment and safety engineering are established methodologies that have been used in the design and analysis of many systems, including computers, to ensure their reliability and dependability. The applied methodologies have their origin in safety oriented industries such as the nuclear power, off-shore activities and transportation and they have recently found applications also in health care, banking and more generally in different kinds services that are important for a well functioning society. This broadening of the applications of risk assessment and safety engineering has actually suggested that systems safety and security could be treated as a discipline of its own.

The application of risk assessment and safety engineering in the computer field is important due to two reasons, firstly because computers are used to control and protect important systems and secondly because computers may represent a threat themselves if they have not been properly designed. One problem in the design and analysis of interconnected computer systems is their complexity, which makes it difficult to ensure their reliability and dependability in all possible situations. This complexity also puts a large demand on designing the human computer interfaces to be understandable and efficient.

The point of departure of the present paper is the safety and security needs as seen from the perspective of nuclear industry, but it takes a broader view towards the use of risk analysis and safety engineering more generally for ensuring computer dependability in important societal infra-structures. Taking this view it is important to consider systems safety and security on a more abstract level to ensure that there are enough interactions between designers and analysts in the development process and in different fields of application. There is also a need for a larger awareness and understanding of needs and solutions to make it possible to find balanced and cost effective designs. A conclusion of the paper is that a multidisciplinary approach and systems thinking are necessary prerequisites in ensuring reliability and dependability of future computer systems.

[1] Invited paper presented at SAFECOMP 2005, the 24th International Conference on Computer Safety, Reliability and Security 26-30 September 2005, Fredrikstad, Norway.

2 FOUNDATIONS OF RISK AND SAFETY

2.1 Basic concepts

Risk is usually interpreted somewhat differently in different fields. A dictionary definition typically includes words like hazard, a source of danger, a possibility of incurring loss, etc. Sometimes the term risk is also referred to various gambles, which are entered in the hope of something favourable to happen. More formally risks are often discussed as the triplet of possible threats together with their likelihood and consequences. This consideration has led to the introduction of the so called *probabilistic risk assessment* (PRA), which has found well established applications especially in the nuclear field [1].

Safety is usually seen as the reciprocal of risk, i.e. that adverse effects will not be caused by some event or agent in defined situations. Safety is however difficult to prove, because it would involve the proof of non-existence. Ensuring safety therefore always involves a kind of completeness argument that all possible threats have been considered and shown not to cause any danger in relevant situations.

Security carries a slightly different interpretation than safety, which is associated to a separation between threats introduced from events of natural origin as compared with threats introduced by malicious actors. With this interpretation security is often associated to gates, guards and guns. Computer security is somewhat blurring this distinction between normal events and malicious actions, because attacks against computer systems are often launched through existing weaknesses in the systems that are the result of normal design deficiencies.

Vulnerability is commonly used to indicate certain flaws and weaknesses in the design or implementation of systems that make them susceptible to attacks. Vulnerability is thus related to possible threats towards security, which may include harassment, theft or sabotage. The importance of assessing the vulnerability of computer systems has increased, because crucial societal infrastructures depend on their undisturbed functioning.

Dependability is often used as a collective concept to define system performance in terms of availability, reliability and maintainability. Dependability is a rather broad concept, because it builds on specific countermeasures, which are designed into the systems and in their environment to ensure that specific threats have been compensated for. This will in practice take place in the work processes of design and analysis in which risks are identified and safety built into the systems.

2.2 Decisions on risks

Decisions on risks are made continuously by people and organisations. Most of the decisions are simple choices, but some of them can have far reaching consequences. Decision analysis has been developed to approach the more difficult decisions and it is based on the expected utility theory (EUT) [2]. Some critique has been expressed towards EUT with the argument that people do not always act according to the axioms of the theory. This is true and the discussion still is ongoing, but for most practical applications EUT with its extensions provides a good normative model for decisions on risks. One extension expected utility theory is for example the multi-attribute utility theory (MAUT), which in some of the more controversial cases can been used to support decisions about risks [3]. Another extension is the theory of games in which the decision making of two or several independent players with at least partly diverging interests [4], [5].

Decisions on risks within the society have led to disagreements between experts and laymen on the risk assessment methodology and the interpretations of the results. These disagreements are partly due to differences in how experts and laymen understand risks and frame decision making situations and partly to difficulties in communication. Controversies are also connected to the models, which are used to predict consequences of a decision and to the conversion of these consequences into value judgements [6]. This debate is still going on, but better communication between stakeholders in the risk communication process together with a consideration of the full spectrum of possible consequences and the uncertainties involved, should be able to resolve at least some of the controversies [7].

2.3 Safety management

Safety management is the activity by which risks are identified, assessed and acted upon. Safety management therefore encompasses many different activities of people and organisations that have a stake in the risks involved. For nuclear power plants for example, these stakeholders include designers, vendors, owners, operators and maintainers of the plant as well as authorities, politicians, media and people in general. The plants are designed, built, commissioned, operated and decommissioned over a period, which may be as long as hundred years. After that the spent fuel is to be stored safely for far longer periods of time. A structured way of working and record keeping is a prerequisite for this to succeed in a way that could be considered to make the risks as low as reasonable practicable (ALARP).

The basis of safety management at a smaller scale is a reliance on structured and well documented work processes to ensure transparency in decisions and repeatability in critical work activities. This applies to all people involved in design, operation and maintenance. A common requirement today is that organisations involved in safety critical work should have a strong safety culture, which is present in their attitudes and behaviour [8]. This requirement has several implications on how the organisations involved should structure their work processes and how the interfaces between them should be arranged.

2.4 International co-operation

International co-operation has an important position in placing a foundation for the handling of risk and safety. This work is taking place on several levels of which academic research has laid the groundwork for understanding risks and building safety. Secondly hazardous areas have their own specialised fora for the exchange of experience and guidance. Some of these organisations are closely connected to the safety authorities, other to operators and some are non-profit organisations with a more research oriented agenda. In the nuclear field for example IAEA, OECD/NEA and WANO have important functions facilitating the emergence of safety standards and guidelines.

Important work is also done by the international standardisation organisations such as IEC and ISO. These organisations in turn are networking with national standards organisations and authorities. This international co-operation can actually be seen as a complex network, which ensures that important experience is taken care of and can be utilised for a continuously improving safety.

3 RISK ASSESSMENT

3.1 Phases in risk assessment

Risk assessments are often divided into three distinct phases. In the first phase the scope of the study is set and potential threats are identified. In this phase it is important to separate between different categories of risk and to approach them with an open mind to ensure that all important threats are covered. Threats may be natural or artificial, they may influence different groups of people differently and they may vary with place and time.

In the second phase event models are built based on possible errors and failures as initiators of some unwanted chain of events. In the models responses of safety provisions and actions are taken into account to arrive at event chains in which a specific threat is realised. The probability of this to happen is calculated from the probabilities of single events within the chain. The resulting risk can then be obtained by summing over the event chains and their probabilities. This phase relies on the collection event and failure frequencies together with the construction of models for how single events influence the system in consideration. Event and failure frequencies can be obtained from statistics and the cause consequence models from knowledge in physics, chemistry, biology, etc. on how various injuries and damages occur. The scope of this phase has for practical reasons to be restricted to the most important event chains.

The third phase of the risk assessment is typically devoted to the assessment, i.e. making value judgements on the results of the two preceding fact finding phases. The third phase also includes the decisions on actions to be implemented based on the results from the assessment. Such actions can for example be the decision to abandon a certain technology, to implement various protective facilities or to redesign some part of the system. In the decision the benefits of acting on the risk have to be compared with the costs of the actions.

3.2 Challenges in risk assessments

There are many challenges in risk assessments of which the perhaps largest is connected to the value judgement in the third phase of the risk assessment. In this phase the scope of the study and its results have to be communicated to decision makers and stakeholders in the process. Experience from risk assessments in societal decision making demonstrates that models, data and reasoning have to be made transparent and believable not to introduce almost unsolvable controversies. This has been seen for example in the search for repositories for high level nuclear waste. Applications of risk assessments in engineering design, where the focus is on the phases one and two, have been mostly uncontroversial.

Risk assessments also include technical challenges of which the completeness of the analysis is the most important. A comprehensive study becomes complex and difficult to take in, but a more superficial study may not be accurate enough. A study has for practical reasons always to be restricted in scope, but it should still include all important failure modes. Very unlikely sequences can be disregarded, but this introduces a certain rest risk, which has to be considered to be acceptable. Finally there will always be uncertainties involved both in the modelling of the event chains and in the probabilities assigned. The largest uncertainties are typically connected to event chains that have very small probabilities and very high costs, which make it difficult to arrive at objective estimates of the importance of these risks.

3.3 Models and modelling

Models and modelling plays an important role in the risk assessments [9]. Firstly there have to be an understanding of when threats will be realised and how they will influence the affected systems, i.e. a theory of accidents and their consequences [10]. Secondly the effects of primary consequences to the initiating event should be modelled also to include secondary consequences and so on. This information should be used to build the event models in which also the responses of safety systems and other actions are included.

As long as the event sequences are restricted to technical systems the modelling is relatively straightforward, but at some level there is a need also to include models of human actions and organisational influences [11], [12]. For example some human maintainer may have forgotten to reset an important safety system after some maintenance activities and this may have been due to deficient instructions. Some advances have been made in the modelling of people and organisations for their inclusion in risk assessments, but available methods and tools rely on a large extent on engineering judgement.

3.4 Threats connected to computer systems

Computers present, due to their versatility and ubiquity, a large challenge for their proper inclusion in risk assessments, especially if some level of detail is pursued in the modelling effort. More limited models can off course be used, but they seldom give enough guidance for the planning of safety precautions. From another point of view, computers seldom, due to the reliability of used hardware, are the initiators of unwanted chains of events. It is more likely that that some hardware failure or software error renders the computer unavailable for some restricted time, before this is detected and corrected. Another important failure mechanism is connected to human actions, which either inadvertently or deliberately may cause computer failures.

On a more technical level one could separate between different threats toward a proper functioning of computer by considering losses of integrity, availability and confidentiality. Loss of integrity is the most serious, because it would mean that the proper functioning and the output from the computer cannot be trusted before it has been reinitialised with its original software. Loss of computer availability can also be quite serious during transients in which the computer is assumed to provide essential services in coping with some disturbance. Loss of confidentiality is the least serious threat, but data that has been stolen may be used later in deliberate attacks with more serious consequences.

4 SAFETY ENGINEERING

4.1 Basic safety principles

Safety engineering can be said to include all the methods of design and analysis that are used to ensure that systems fulfil their safety and security requirements. Present views on safety engineering have emerged through development in many different fields. The early development of nuclear power for example generated several important insights, which today are seen as corner stones of safety engineering. The perhaps most important concept in this connection is *defence-in-depth*, which is based on the principles removing, preventing and controlling certain threats and mitigating their consequences if they in spite of these precautions should be realised. The principles of *redundancy*, *diversity* and *separation* can be derived from the defence-in-depth concept as well as the so called *single-failure* criterion.

Another important concept from the nuclear field is the concept of a *design-basis-accident*, which means that one or a set of accident scenarios are defined to serve as probing stones for the analysis. The design of the safety systems is thus given a clear objective to ensure that the systems should be able to cope with possible variations of these base scenarios without any harm. A concept *design-basis-threat* has been introduced in the security field to serve in a similar way to govern the design and analysis of security precautions [13].

4.2 Technical safety systems

The technical safety systems typically consist of a supervision and control system, which is given the task of detecting, counteracting, controlling, mitigating and finally restoring safe operation. The design and analysis of the supervision and control system involves a careful definition of safe operation together with alarms for situations when some important parameter has exceeded its allowed range. The supervision and control system can be automated or it can rely on manual operation. For large and complex systems, which need a continuous monitoring, the supervision and control is typically realised through a combination of automatic and manual control.

The tasks of the supervision and control system are generally detection of adverse situations and activation of protective systems and devices. Parts of the control systems may also be designed to prevent dangerous situation by inhibiting for example operator actions that may lead to the realisation of some threat. As an example the technical safety systems for a nuclear reactor include automatic systems for the following functions

- shut down of the reactor,
- isolation of important systems,
- pressure relief to protect the integrity of the reactor,
- reactor cooling,
- emergency power supplies.

4.3 Administrative safety systems

In addition to the technical safety systems there are many administrative systems, which are important for safety and security. The most important is the quality systems, which can be considered as an important part of safety engineering in spite of the fact that they mostly are implemented as a set of administrative rules for work processes within an organisation. A quality system can in principle be seen as a description of required quality, a description of how this quality can be reached and the processes of auditing and updating by which the quality system is maintained [14]. Quality systems typically stress a structured way of working, inspection and review, documentation and record keeping, etc. The procedures and instructions used in operation and maintenance are often considered to be a part of the quality system.

Another part of the administrative safety systems is the feedback of experience, which sometimes is interpreted narrowly to consist only of accident and incident reporting. The feedback of experience is an important source of information both for modelling the cause consequence chains and for the calculation of failure frequencies. Today causation mechanisms for incidents and accidents are well known and several data banks are available for equipment failure frequencies. Unfortunately however, incidents and accidents show that human errors and organisational deficiencies often are important contributors and for them it is far more difficult to find adequate models and data.

4.4 The systems design process

Systems design is not only concerned with the design of the technical system, but also with the design of administrative systems and training programmes. Safety engineering relies on a graded approach to design and analysis, which means that the parts of the systems that are important for safety are given more attention than less important ones. This principle aims at a balanced design in which a high safety level is reached without spending fortunes on protection against very unlikely sequences of events. The graded approach is in practice implemented as a safety classification of systems and equipment [15].

The systems design process is usually divided into the phases of requirements specification, conceptual design and detailed design. Design projects usually build on earlier design projects, which are modified for the changes as compared with earlier designs. It is common to see iterations in design projects, where concepts are brought to a rather detailed level and tested against requirements before they are implemented in the actual design. A common observation is that the freedom of design decreases and that the costs of changes increase as the design project evolves in time.

4.5 Operational precautions

Safety relies not only on a well designed system, but also on how this system is operated and maintained. Safety precautions for operations and maintenance include well designed human system interfaces for operators, maintainers and other groups of people that are involved in various hands on activities. They also include the instructions these people are using and the administrative provisions, which ensure that only qualified persons are allowed to perform safety critical tasks.

Nuclear power plants for example rely on a comprehensive system of instructions, which have been created to cover normal operation, disturbances and emergencies. For the training of operators training simulators are used both in the initial training and the annual retraining sessions. For the training of emergencies it is usual to arrange emergency drills in which relevant outside organisations are engaged to serve the dual purpose to improve available instructions and to give training to the people involved.

4.6 Regulatory oversight

Regulatory oversight can be seen as the final step of safety engineering. Most high risk areas have some sort of regulatory oversight, which includes regulatory requirements, operating licenses and various types of inspections and reviews. In principle one may say that it is not enough that the facilities operate safely, but their operators have to be able to prove for an outside party that they actually do so. If there is a doubt that necessary safety provisions are not in place, the operations license may be revoked with immediate effect for a certain time or until defined actions have been taken. The regulation in the nuclear field has over time moved from prescriptive systems more towards risk informed approaches [16].

Regulatory oversight in the nuclear field is exercised through a safety case, which has to be prepared, submitted and assessed before an operating license can be granted. The safety case provides in principle the full description of the plant, its safety provision, modes of operation, administrative systems and responsible persons. When an operational license has been granted all modifications that will change something in the safety case, have to be submitted to the regulator for approval.

5 APPLYING SAFETY ENGINEERING TO COMPUTERS

5.1 Designing for computer dependability

Research and development in computer reliability over the last quarter of a century has generated methods and tools with which a high dependability can be reached. In the design of computer software it very early became evident that a large emphasis had to be put on ensuring the correctness of the code. Early research suggested that the use of structured programming and high level languages could improve both correctness in the code and productivity in the coding process. The requirements specifications were also identified as an important source of persistent errors in the final code. Further development led to the emergence of practices and standards, which gave recommendations for the software design process [17], [18]. More detailed guidance for the software verification and validation activities can be found in [19].

Especially in the computer field, but also in other applications, there is an increased use of formal methods in requirements specification and analysis. This development is connected to the increasing complexity of all systems, which makes it difficult to ensure consistency and completeness without specialised tools. Formal methods also have the benefit of enabling computerisation of design and analysis, which make these processes more reliable as compared to manual alternatives. In these cases it is usual to give reference to so called CASE-tools (computer aided software engineering).

In the design of high integrity software it is a common practice assign *safety integrity levels* (SIL) in which the likelihood and consequences of software errors are combined to separate for instance between small, tolerable, medium, high and intolerable risks. This classification is then used to select methods and tools for the software development process.

5.2 Computers in safety systems

The problems of using computers in systems important to safety of nuclear power plants was identified more than ten years ago [20]. The basic dilemma in using computers is connected to providing proofs that required functionality can be obtained in all possible situations and that no unwanted functionality will occur in any situation. This problem has for a few commercial systems been solved to the satisfaction of national licensing authorities, but the process to generate these proofs has shown to be tedious and expensive. Available systems often use computer based tools for the design and analysis, but then the burden of proof is moved from the system itself to the tools.

The methods of safety engineering are based on independence between the safety precautions in a probabilistic sense. Unfortunately the bulk of the computer failures are due to deficiencies in the software, which implies that the failure mechanism basically is deterministic, although the software usage profile, i.e. how the environment is exercising the software, in some sense is probabilistic. It is therefore impossible to exclude the possibility of a common cause failure, even when redundant or diverse software is used, because such a failure may be due to common hardware, common specifications, common methods or tools, etc. In addition with digital systems there is always the possibility that a software error will cause very large changes in outputs values as the consequence of a very small change in inputs, which means that it is practically impossible to predict the consequences of a software error without actually running the code and hitting the error.

5.3 Computers in societal infra-structures

The development of modern computers has been a large achievement, which contains many promises for the future. The benefits as we see them today are undisputable, but the increasing reliance on computers and computer networks are introducing new threats that have to be understood and acted upon. The first indications of emerging difficulties were mainly connected to programming errors, which in the beginning mostly caused ridiculous situations, but also some more serious incidents.

The second indication of emerging threats came when additional functionality in the computer systems was obtained through networking. Firstly the growing complexity of the systems paired with relatively lax security provisions of that time, made it possible for frustrated computer specialists to do harm to their employers or to exploit their knowledge for criminal gains. Secondly a generation of hackers grew up, who found contentment in breaking into computer systems of large companies and organisations. Thirdly writers of malignant computer code found amusement in writing viruses that rapidly infected thousands of computers around the world. Today there is a growing concern that criminals and terrorists may use existing vulnerabilities in the computer systems for their own ends.

5.4 The ubiquitous computer

The societal reliance on computers has increased tremendously over the last decade. Where for example shops and banks ten years ago usually had an emergency fallback to manual routines in the case of computer failures, this is not possible anymore. Today a car can contain tens of embedded computers and even simple everyday products such as stoves, freezers and washers contain computers. Many of the computers are connected through local area networks to the global cyber sphere. Updates of the software are sent automatically to many of these computers and these channels may as well be used for malevolent purposes.

One difficulty in the new situation is that computer users have a good understanding for only a small set of the functions available. This means that s/he has difficulties to identify failures and even lesser possibilities to do anything about them. At the same time computers experts continuously become narrower in their expertise due to the growing complexity in the systems. The rapid technological development also implies that expertise will deteriorate rapidly if it not continuously maintained. In addition there is a growing black market of sophisticated computer based tools that can be used to introduce different kinds of damage for systems that are important for a well functioning society.

6 CHALLENGES FOR THE FUTURE

6.1 Escalating costs

With the experience from computer systems today it seems very clear that more efforts in the future have to be placed on issues that are connected to safety and security. The question is how such efforts should be allocated to get the best impact, because there is a growing concern that costs will escalate without a real contribution to system safety and security. In the nuclear field some of these concerns have been addressed in a recent report [21].

One approach to abate escalating costs has been to bring in so called *commercial-off-the-shelf* (COTS) products both on the hardware and on the software side. This practice has many benefits by making it possible to divide development costs among a larger number of users, but it has also certain drawbacks. COTS products are for example often black boxes with little or no information on their development process, which makes it difficult to assess their suitability for some specific application.

Software reuse has also been proposed as a method to cut system development costs. Again there are pros and cons with this approach, because there may be subtle differences between the original application for which the software was developed and the new intended application. One possibility for software reuse is reverse engineering, which is used either to develop new hardware for the old software or to port the old software onto a new hardware platform.

6.2 Technical improvements

Most trends in the computer field indicate a continuation of the present rapid development of hardware and software for many years to come. This will most likely bring a higher sophistication in the computer systems we are using, but also a growing complexity and a decreasing transparency of the systems. It is likely that many technical fixes will be implemented to get rid of present difficulties for example in ensuring that certain messages are coming from trusted origins and do not contain any hidden malignant pieces of code. However, it is also likely that these fixes will open up new loopholes, which then consequently will need their own subsequent fixes.

A difficult technical question for the future is the extent it would be better to rely on open or proprietary code for high integrity applications. If the code is open it may be easier to design an attack on it, but the code may on the other hand be more robust and stable. Similarly a proprietary code may contain several bugs when it is released and it may enforce more accurate version management to prevent that detected bugs are not exploited before they are corrected. A supplier of proprietary code may also be reluctant to release information on bugs that are detected.

6.3 Administrative improvements

It is important that administrative safety and security systems are created in parallel with the technical improvements, because lax administrative systems can easily offset the most rigid technical safety precautions. The first step is to create an understanding by the computer users that safety and security are important issues and that it is necessary to stick to agreed administrative rules. This will only succeed if the administrative system is properly balanced between too lax and too rigid systems.

The administrative system should be based on a safety and security plan, which has identified threats that the system should be able to withstand. To be realistic this should most likely include attacks, which are mounted through a co-operation between a single insider and several outsiders. For present systems it may be difficult to provide convincing proofs that the success of such an attack is very unlikely. More generally it would be important to identify potential attackers together with their motives and resources. This would make it possible, at least in principle, to design the safety and security precautions to make the likelihood of a successful attack small enough as compared with the costs of mounting an attack.

6.4 Solutions for high integrity systems

For computer system where a very high integrity is required and a large certainty should be reached that it actually has been achieved, new methods and tools for design and analysis will be needed. The design methods and tools should force designers to restrict themselves to simple constructs within a given domain of functions and to leave a documented trace of the advancement of the design process. The methods and tools for analysis should aim at quantitative risk assessments for computer system, because only then given acceptance criteria can be verified. Quantitative acceptance criteria can also guide the verification and validation efforts to be in balance with the increased assurance that the system will provide all specified functions and no unwanted functions.

These requirements can at least in principle be fulfilled by combining deterministic and probabilistic reasoning. On one hand it may be argued that certain deterministic requirements can be relaxed, because the specific event chains they involve can be considered to be very unlikely. On the other hand it may similarly be argued that some event chains can be excluded from the probabilistic analysis, because deterministic provisions during the design process make them very unlikely. In addition it is clear the design, testing and installation of critical modules always should progress as a joint effort of at least two persons to prevent the possibility that a single insider can tamper with the process.

6.5 A societal response

A societal response towards the new threats has to be built on several levels. Starting from above it is evident that new legislation will be needed, which criminalises intentional actions, which are aimed at disturbing important societal infra-structures. This legislation should be harmonised between countries, because effective prevention of harmful activities will need international co-operation. Secondly there is an evident need for more research and development in the area of safety and security and it is important that this work is given a broad and multi-disciplinary character. New standards will be needed for various technical solutions especially in the interfaces between systems. For some of the most critical infra-structures in the society it may be necessary to introduce new regulation.

In designing societal responses to the new threats, one interesting question is whether or not it is possible to use market mechanisms for the actions necessary or if centrally planned activities may be more efficient. The answer seems to be that market mechanisms are probably not enough, because societal funding to an agency seems to outperform other organisational solutions [22]. This recognition is important also in ensuring that efficient error reporting and analysis is used to close the experience loop to achieve organisational learning [23]. A final question for the future could be, if it is possible to reach significantly better safety and security in the future. The answer is probably no, because according to the theory of risk homeostasis the gain of better methods and tools are usually spent on an increased overall performance and not on safety [24].

7 CONCLUSIONS

Risk assessment and safety engineering have been used to create solutions for analysing and protecting systems against a large spectrum of threats. The developed methods and tools can with success be used also for computer systems, but this may become prohibitive costly if a very large certainty is sought that the computer software will function as intended. Therefore it is practical to restrict this requirement only to the most central mechanisms and build the less sensitive parts with more conventional methods. This can only be achieved with a good understanding of the risks involved and how these risks can be acted upon.

In the quest for safety and security a separation has to be made between the game against nature and the game against an intelligent opponent. One has also to understand the general development mechanisms of the computer field, because no single person can grasp the full complexity of the interconnected computers all with their own software, which can be modified almost from anywhere around the globe. This actually implies that our societal infrastructures rely on a system with emergent properties and not understanding this development may have serious repercussions.

It is evident that ensuring safety and security of the computer systems of tomorrow will require far more efforts as compared with what is spent today. This quest can metaphorically be seen as a race between the safety and security as built into the systems and an unknown population of hostile attackers. When a new safety or security provision has been invented and built in, it can be attacked by new means and vice versa.

Safety and security of computer systems is a field, which is growing in importance. This is due to the increasing reliance on computers within important societal infrastructures. If this threat is not properly counteracted, it can have dire consequences on the world economy. A balanced approach will require a realistic assessment of the risks involved and paired with a combination of technical, administrative and societal means. Present safety engineering principles are well adaptable to the needs in different sectors of the society. The ultimate question, what is safe enough, has however always to be based on a broad consideration of costs and benefits for the society.

In the future development of the risk and safety field, it would be beneficial if there is an interaction between different areas of application, because this has the potential to stimulate innovations and development of new methods and tools. Practitioners in the risk and safety field require a multi-disciplinary education together with a good knowledge of their own area of applications. A systems oriented thinking can finally help in finding a practical perspective to support cost effective solutions.

References

[1] I. Wall, J. Haugh, D. Worlege (2001): Recent applications of PSA for managing nuclear power plant safety, Progr.Nucl.Energy, 39, pp. 367-425.

[2] David E. Bell, Howard Raiffa, Amos Tversky (eds.) (1988). Decision making; descriptive, normative and prescriptive interactions, Cambridge University Press, Cambridge.

[3] Simon French, Tim Bedford, Elizabeth Atherton (2005). Supporting ALARP decision making by cost benefit analysis and multiattribute utility theory, Journal of Risk Research 8(3), 207–223.

[4] von Neuman, Morgenstern (1947). Theory of games and economic behavior, Princeton University Press.

[5] R. Axelrod (1984). The evolution of co-operation, Basic Books.

[6] Mary Douglas (1985). Risk acceptability according to social sciences, Russell Sage Foundation, New York.

[7] T. Aven, V. Kristensen (2005). Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach, Reliability Engineering and System Safety, pp. 1–14.

[8] IAEA (1991). Safety Culture, INSAG-4, International Atomic Energy Agency, Vienna.

[9] Björn Wahlström (1994). Models, modelling and modellers; an application to risk analysis, European Journal of Operations Research (EJOR), Vol.75, Issue 2.

[10] James Reason (1997). Managing the Risks of Organizational Accidents, Ashgate, Burlington, VT, USA.

[11] Erik Hollnagel (1998). Cognitive Reliability and Error Analysis Method. Oxford: Elsevier Science Ltd.

[12] K. Davoudian, J.-S. Wu, G. Apostolakis (1994). Incorporating organizational factors into risk assessments through the analysis of work processes, Rel. Eng. & Syst. Safety, 45, pp.85-105.

[13] IAEA (1999). The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), International Atomic Energy Agency, Vienna

[14] Björn Wahlström (2004): Quality systems: Support or hindrance for learning, in J.H. Erik Andriessen, Babette Fahlbruch. How to Manage Experience Sharing: From Organizational Surprises to Organizational Knowledge, Elsevier.

[15] IEC (1993). Nuclear power plants – Instrumentation and control systems important to safety – Classification, International Standard 1226, Geneva.

[16] Björn Wahlström (2003). Risk Informed Approaches for Plant Life Management: Regulatory and Industry Perspectives, FISA-2003, 10-12.11.2003, Luxembourg.

[17] IEC (1986). Software for Computers in Safety Systems of Nuclear Power Plants, Standard No. 880, Geneva.

[18] IEC (2000). Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software, Standard No. 60880-2, Geneva.

[19] IAEA (1999), Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, TRS-384.

[20] IAEA (1994). Software Important to Safety in Nuclear Power Plants, TRS-367.

[21] IAEA (2002). Solutions for cost effective assessment of software based instrumentation and control systems in nuclear power plants, TECDOC-1328.

[22] Karthik Kannan, Rahul Telang (2005). Market for software vulnerabilities? Think again, Management Science, Vol.51, No.5, May, pp.726-740.

[23] IAEA (2000). Effective handling of software anomalies in computer based systems at nuclear power plants, TECDOC-1140.

[24] Gerald J.S. Wilde (1994). Target Risk, PDE Publications.