Safety of Machinery – the Need for Risk Assessment and the Reasons why

Siegfried Radandt *

Forschungsgesellschaft fü angewandte Systemsicherheit und Arbeitsmedizin, Mannheim/BRD

BIOGRAPHICAL NOTES

Prof. Dr. Siegfried Radandt, 1935-09-29. University of Stuttgart: degree of Diploma "Dipl.-Ing. (Machinery, Mechanics, Electrotechnics). University of Munich: degree of Diploma "Dr.-Ing. (Machinery, Vibration, Noise emission and prevention of bottling plants)"; 1975. Managing director of FSA (Research Centre for applied system safety and industrial medicine). Head of FSA Notified Body (Test and certification of non electrical Equipment for Use in explosive atmospheres. Gesellschaft für Sicherheitswissenschaft (GfS) (Society for Safety Science; Board of Directors), Vice President of GfS. ISSA (International Social Security Assosiation), Section "Machinery and System Safety": Technical Advisor; Convenor of WG "Risk-Management". Honorary Professor at Northeastern University Shenyang / P.R. China.

KEY WORDS

Risk management, , risk assessment methods, risk estimation, risk evaluation, risk treatment, safety of technical systems, functional safety ,protective measures, human factors.

1. Introduction

The DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery demands: The manufacturer of machinery or his authorized representative must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment.

By the iterative process of risk assessment and risk reduction, the manufacturer or his authorized representative shall:

- ***determine the limits of the machinery or technical system, which include the intended use and any reasonably foreseeable misuse thereof,***
- ***identify the hazards that can be generated by the machinery and the associated hazardous situations,***
- ***estimate the risks, taking into account the severity of the possible injury or damage to health and the probability of its occurrence,***
- ***evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of the Directive,***
- ***eliminate the hazards or reduce the risks associated with these hazards by application of protective measures.***

The Directive 89/391 - OSH "Framework Directive" of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work - "Framework Directive" contains principles concerning the prevention of risks, the protection of safety and health, the assessment of risks, the elimination of risks and

accident factors. These are obligations for employers.

The employer shall e.g.:

Evaluate all the risks to the safety and health of workers, inter alia in the choice of work equipment, the chemical substances or preparations used, and the fitting-out of work places.

Implement measures which assure an improvement in the level of protection afforded to workers and are integrated into all the activities of the undertaking and/or establishment at all hierarchical levels.

Take into consideration the worker's capabilities as regards health and safety when he entrusts tasks to workers.

To identify the risks which lead to unsafe situations he should use risk assessment methods.

2. Risk Management is Specific to the Organization and its External and Internal Context

The process is tailored to suit the organization and its internal and external context, taking into accounts the organization's external and internal culture, needs, resources, criteria and objective.

The organization's risk management process may also need to change, if the organization changes,

Risk management is dynamic, iterative and responsive to change.

Risks change, new risks emerge and others decline.

As events occur and essential risk control activity takes place, the knowledge in the organization changes. Risk management is not a "one pass" process and the "monitoring and review" step acts to ensure that the organization's risk controls reflect the current situation.

3. Risk Management for Technical Systems

Technical systems are planned as determinate systems. Only foreseeable and intended system behaviour is taken into account when the system is designed. Experience has shown, however, that technical systems also have a stochastic behaviour, i.e. external influences and/or internal modifications not taken into consideration in the design result in unintended changes of the system's behaviour and properties. The period of time until the unintended changes in behaviour and/or frequently also in properties occur cannot be accurately determined, it is a random variable.

Technical systems (e.g. machines) are intended to perform numerous functions and at the same time be safe.

It is assumed that, when present on a technical system, a hazard will sooner or later lead to harm if no protective measure(s) is (are) taken.

Protective measures are a combination of the measures taken by the designer and the user.

Measures which can be incorporated at the design stage are preferable to and generally more effective than those which are implemented by the user.

The human being and his influence on safety have to be taken into account in safety-relevant considerations as well ("human factor").

The safety of a system is given when there is no occurrence of function or action sequences with hazardous effects for people and/or property.

To identify the risks which lead to unsafe situations one uses risk assessment methods.

One shall take the following actions, in the following order : specify the limits and the intended use of the technical system; identify the hazards and associated hazardous situations; estimate the risk, for each identified hazard and hazardous situation; evaluate the risk and take decisions about the need for risk reduction; eliminate the hazard or reduce the risk associated with the hazard by protective measures.

The first four above indents are related to risk assessment.

The system analysis is the basis of all hazard analyses, which includes examination of the system functions, in particular of the performance goals and admissible deviations of the ambient conditions not influenced by the system, of the auxiliary sources of the system, of the system components and of the organization and behavior of the system.

Geographical arrangements block diagrams, material flow diagrams, information flow diagrams, energy flow diagrams etc. are used to depict technical systems. The objective is to ensure the required safe behavior of the technical systems by design methods, at least during the required service life and at intended use.

Having identified the various hazards that can be generated by the technical system, one shall estimate the risk for each hazard, as far as possible on

the basis of quantifiable factors, and finally decide if risk reduction is required as a result of the risk evaluation.

For this purpose, one shall take into account the different operating modes and intervention procedures.

Risk assessment is a series of logical steps to enable, in a systematic way, the examination of the hazards associated with technical systems.

Risk assessment includes: risk analysis (determination of the limits of the machinery; hazard identification; risk estimation) and risk evaluation.

Risk analysis provides the information required for the risk evaluation which in turn allows judgements to be made on the safety of a technical system.

Risk is a combination of a probability of occurrence and associated unwelcome outcome or impact of a risk element

Risks of unwelcome events are determined on the basis of the experience (e.g. catalogue of measures) with technical systems.

Unwelcome events are source conditions of processes and states, processes and states themselves, effects and influences of processes and states which can result in harm to persons or property.
Accordingly, the unwelcome event can be defined as a single event or an event within a sequence of events

Unwelcome events are looked for in process and functional sequences, work, action and organizational procedures, ambient conditions.

The expected frequency of occurrence of an event leading to harm is determined by e.g.: the probability of the occurrence itself, the duration and frequency of exposure of persons (if applicable, of objects) in the hazardous area, e.g. extremely seldom (e.g. repair), seldom (e.g. installation, maintenance and inspection procedures), frequently and very frequently (e.g. constant intervention during each working cycle), the influence of users or third parties on the risk of an event.

The extent of harm is determined by, e.g.: the type of harm (harm to people and/or property), the severity of harm (slight/severe/fatal injury of persons or corresponding damage to property), the number of people or objects affected.

Human factors can affect risk and shall be taken into account in the risk estimation. This includes, for example: interaction of person(s) with the system including correction of malfunction; interaction between persons; stress related aspects; ergonomic effects; capacity of persons to be aware of risks in a given situation depending on their training, experience and ability.

Risk estimation shall take account of the reliability of components and systems. It shall: identify the circumstances which can result in harm (e.g. component failure, power failure, electrical disturbances); when appropriate use quantitative methods to compare alternative protective measures; provide information to allow the selection of appropriate safety functions, components and devices.

Those components and systems identified as providing safety functions need special attention.

Risk evaluation is the next step. It is a process of comparing the estimated risk against given risk criteria to determine the significance of risk, where risk criteria are terms of reference by which the significance of risk is assessed. This can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects concerns of stakeholders, priorities and other inputs to the assessment.

The risk treatment is the consequence of the assessment. It is a process of selection and implementation of measures to modify risk. It has the possibilities of risk optimization (process to minimize the negative and to maximize the positive consequences and their respective probabilities), risk transfer (sharing with another party the benefit of gain, or burden of loss , for a particular risk), risk retention (acceptance of the burden of loss , or benefit of gain, from a particular risk).

Risk reduction methods: inherently safe design measures by limiting the actuating force to a sufficiently low value so that the actuated part does not generate a mechanical hazard; limiting the mass and/or velocity of the movable elements, and hence their kinetic energy; limiting the emissions by acting on the characteristics of the source; measures for reducing noise emission at source (see ISO/TR 11688-1); measures for reducing the emission of vibration at source include e.g.; redistribution or addition of mass and change of process parameters, e.g. frequency and/or amplitude of movements; measures for reducing the emission of hazardous substances include e.g. use of less hazardous substances or use of dust reducing processes; measures for reducing radiation emissions

include e.g. avoiding the use of hazardous radiation sources, limiting the power of radiation to the lowest level sufficient for the proper functioning of the machine, designing the source so that the beam is concentrated on the target, increasing the distance between the source and the operator or providing for remote operation of the machinery.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from:

- *Incorrect specifications of the system, hardware or software;*
- *Omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);*
- *Random hardware failure mechanisms;*
- *Systematic hardware failure mechanisms;*
- *Software errors;*
- *Common cause failures;*
- *Human error;*
- *Environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);*
- *Supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).*

In automated plant and processes, automation systems take on the tasks of monitoring safety as well as their process control functions.

The failure of individual components may lead to undetected malfunctions of the automatic system - even to complete failure.

Such individual components are e.g.: sensors, signal and data transmission paths, interface cards, central processor unit, positioners and their power supplies.

The Safety Instrumented System (SIS) must be designed in such a way to assure significantly higher reliability and availability.

In practice, implementing one or more, or a combination, of the following techniques, can achieve this: redundancy (multiplication of elements/systems); diversity (of redundant components whose operation is based on different principles in order to avoid common-mode failures); voting modules; reliability; identification of passive failures.

The automation system tasks that ensure plant safety are:

- *Data acquisition of plant conditions (sensors)*
- *Identification of critical states (by checking measured variables against limits, comparing desired and actual conditions, monitoring their behavior over a period of time, etc.)*
- *Annunciation of critical conditions (alarm, recording)*
- *Ensure automatic intervention*
- *Prevention of erroneous operator intervention*

Plant safety may be enhanced, by implementing additional monitoring functions.

They include interlocks and alarms, which are activated when limit values are exceeded:

- *Limit values fixed by equipment specification (critical limits)*
- *Limit values determined by product to be processed in the equipment*
- *Tighter limits during critical process steps if necessary*
- *Automation system malfunctions.*

Power down conditions: failure of any utilities supply or form of auxiliary power such as the normal electrical supply, the emergency electrical power supply, compressed air, instrument air, cooling media, etc. must not cause the plant to be driven to a potentially dangerous state.

Failure of any power supply does not necessarily drive the plant to a safe state but is to be analyzed as a potential hazard in the risk analysis.

In automated plant it is not only the normal operating states that must be described, but also the abnormal states, particularly the power down conditions and the safety states, must be defined.

Information about the criticality and reliability considerations has to be collected within the risk analysis (search for hazards, risk evaluation, design of measures). The description of measures must always include the failsafe position of elements in order to define SSS* (Software Safety State) and HSS* (Hardware Safety State) once the Risk analysis is complete.

The safety states can be divided into hardware and software safety states.

The difference is that within software safety states all actions and controls are driven by application software, while within hardware safety states all actions are achieved with bypassing of the control system.

The impact of the control system on the process is interrupted by disconnecting the power supply

to the output interface cards

The disconnection of the interface power supply is often sufficient for chemical processes, but in machine-controls (e.g. packaging lines) it is requested to disconnect the power supply with the main-switch, driving the "zero energy state" (e.g. thyristor controllers with high-voltage power supply with a malfunction in the control are active).

The Hardware safety state is considered to be the highest safety level of a plant and protects primarily persons and equipment.

In the HSS all digital and analog outputs which operate actuators (valves, actuators, motors), must be reliably uncoupled from the „Basic Process Control System"

The actuators may not be automatically re-coupled by the „Basic Process Control System" after the problem causing the HSS has been resolved. For this an operator initiated coupling operation is necessary.

Several software safety states with different purposes may be defined and called upon during a process sequence.

When SSS is activated it usually aims at keeping the process interruption as short as possible.

For this reason, columns, scrubbers and essential services should be separated from the rest of the process and kept operational in closed circuit rather than being shutdown.

The structure of „machine-systems" show the importance of the safe function of the control systems

A control system is a device, or set of devices to manage, command, direct or regulate the behavior of other devices or system.

There are two common classes of control systems, with many variations and combinations: logic or sequential controls, and feedback or linear controls.

An automatic sequential control system may trigger a series of mechanical actuators in the correct sequence to perform a task.

In the case of linear feedback systems, a control loop, including sensors, control algorithms and actuators, is arranged in such a fashion as to try to regulate a variable at a set point or reference value. Open-loop control systems do not make use of feedback, and run only in pre-arranged ways.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from: incorrect specifications of the system, hardware or software; omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation); random hardware failure mechanisms; systematic hardware failure mechanisms; software errors; common cause failures; human error; environmental influences (e.g. electromagnetic, temperature, mechanical phenomena); supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).

The performance levels can be applied to: safety-related parts of control systems as protective devices (e.g. two-hand control devices, interlocking devices), electro sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices; control units (e.g. a logic unit for control functions, data processing, monitoring etc.); power control elements (e.g. relays, valves etc); control systems carrying out safety functions at all kinds of machinery, from simple (e.g. small kitchen machines or automatic doors and gates) to manufacturing installations (e.g. packaging machines, printing machines, presses).

4. Conclusion

Finally risk analysis is the systematic use of information to identify sources and to estimate the risk

It includes source identification (process to find, list and characterize sources) and risk estimation (process used to assign values to the probability and consequences of a risk).

Risk management is methodical and uses recognized methods that ensure that the results are repeatable and reliable.

Risk management is part of decision making.

Risk Management can help prioritize actions. It provides an objective and effective way to distinguish between alternative courses of action and thus helps decision makers to make choices.

Ultimately it can help with decisions on whether risk is tolerable and whether risk controls will be adequate and effective.

Risk management leads to the optimisation of risk control and maximization of net benefit.

Risk management is transparent and understood by all interested parties through their inclusion and involvement in the process.

Risk analysis provides the information required

for risk evaluation which in turn allows judgments to be made on the safety of the machinery or plant under review. Risk assessment relies on judgmental decisions.

Risk assessment shall take into account:
the phases of system or plant life; the limits of system or plant including the intended use (both the correct use and the operation of the technical system or plant, as well as the consequences of reasonably foreseeable misuse or malfunction); the full range of foreseeable uses of the technical system (e.g. industrial, non-industrial and domestic) by persons identified by sex, age, dominant hand usage, or limiting physical abilities (e.g. visual or hearing impairment, size, strength); the anticipated level of training, experience or ability of the foreseeable users such as: operators including maintenance personnel or technicians, trainees and juniors, general public, exposure of other persons to the hazards with the machinery where it can be reasonably foreseen.

The following principles apply to design:
Service life, safe life, fail safe and tamper proof design. Design ensuring service life safety has to be chosen when neither the technical system nor any of its safety-relevant partial functions are allowed to fail during the service life envisaged. This also includes that components for partial functions need to be exchanged at previously defined time intervals (preventive maintenance).

5. References

[1] The DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery
[2] Siegfried RADANDT1, 2, Jianye SHI21Inherent Safety - A Concept for a Safe Process with a low Level of Danger even if Things Go wrong; Publication at Northeastern University Shenyang, China
[3] ISO/EN 12100 Safety of machinery — Basic concepts, general principles for design
[4] ISO/EN 14121 Safety of machinery — risk assessment
[5] S. Radandt; System Safety: A Science and Technology Primer; Presentation at NEU Shenyang, China
[6] Siegfried Radandt; Risiken in der Industrie, Sicherheit, Vorsorge, Meidung in der Technik, , Publication in FSA Proceedings
[7] Bischoff;Risks in Modern Society, ISSA-Section Machine and System Safety, Mannheim, Germany, published by Springer Science + Business Media B.V. 2008
[8] Safety of Machinery; a Guide to European Legislation and Standards for Manufacturers, Dealers, Users and Others; by Beuth Verlag GmbH, 10772 Berlin, Germany
[9] Siegfried Radandt; System Safety; Principles for MACHINERY- and SYSTEM SAFETY , Presentation at NEU Shenyang, China
[10] ISO 11161 Safety of machinery — Integrated manufacturing systems
[11] Bardach E (1996) ;Thinking for Deliberative Risk Communication. Risk Analysis 21(6), 1065–1076.
[12] Behn RD, Vaupel JV (1982) Quick Analysis for Busy Decision Makers. Basic,New York.
[13] De-Marchi B, Ravetz JR (1999) Risk Management and Governance: A Post-Normal Science Approach. Futures 31, 743–757.
[14] Cross FB (1996) Paradoxical Perils of the Precautionary Principle. Washington and Lee Law Review 53, 851–925.
[15] Assessment and Management of Chemical Risks. American Chemical Society, Washington, DC, pp. 97–112.
[16] Morgan G, Henrion M (1992) Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge University Press, Cambridge.