Alternative approaches to risk evaluation

Lars Harms-Ringdahl [a, b] and Ronald Wennersten [a]

[a] Chemical Engineering, Royal Institute of Technology, S-100 44 Stockholm, Sweden

[b] Institute for Risk Management and Safety Analysis, Bergsprängargr. 2, S-116 35 Stockholm, Sweden.

Preprint version from

Pasman, H.J., Fredholm, O., and Jacobsson, A. (eds.) *Proceedings of Loss Prevention and Safety Promotion in the Process Industries.* 10th International symposium, Stockholm. Elsevier Science, Amsterdam, (pp. 361 – 369) 2001.

ABSTRACT

Different approaches to risk analysis with a focus on risk estimation and risk evaluation have been compared. Critical aspects of quantitative and qualitative methods and criteria are summarised. An explosives accident has been analysed as an example. The explosion occurred in a system, which was frequently changed and exposed to disturbances. This entailed a number of difficulties in the validity of the results of the performed risk analysis. For example, the actual type of accident was not anticipated. Systems, where changes are frequently introduced as a result of disturbances in the process, offer a number of difficulties in making a risk analysis. Risk assessments, especially those based on probabilistic approaches, could easily be of reduced value, due to a number of reasons. For this type of situations, alternatives to traditional probabilistic assessments could offer advantages. There are a number of qualitative approaches that are interesting to explore further, and a test with Safety Function Analysis appeared to solve some of the problems related to system changes.

1 BACKGROUND

1.1 The perspective

Accidents occur as a result of loss of control of hazards. In order to avoid accidents companies apply risk management, which is a systematic application of management policies, procedures and practices to the tasks of analysing, assessing and controlling risks.

Risk analysis is a process where available information is utilized in order to identify hazards and hazardous events (events with loss of control of hazards) [1]. Risk analysis also includes an estimation of the risks, which traditionally is based on the frequency and the consequences of the identified hazardous events. It is important to note the difference between risk and hazard. Hazard is an inherent property in the system, usually in the form energy (chemical, mechanical, electrical etc.) or toxicity, when we are dealing with certain chemicals.

The identified and estimated hazardous events must then be evaluated in order to decide if the risks are acceptable. The evaluation is an essential part of the risk assessment. This is a challenging task, and there are a number of essential issues to consider in the choice of approach and strategy for the evaluation.

This paper discusses the process of risk assessment with focus on the process of risk estimation and risk evaluation and some problems related to that. The perspective is general, but in order to limit the context a simple case study is used as discussion basis.

1.2 Different approaches

There are several established approaches to risk assessment, and they could be dichotomised in different ways. One major distinction is between quantitative and qualitative approaches. The first one is well described and several methods are available to support the risk calculations [see e.g. 1-3]. The result could concern the individual risk, the group risk and/or the societal risk.

So far, qualitative approaches have received less attention, and sophisticated tools are seldom available. Some examples of qualitative criteria for risk acceptance are given below [4, 5]. These types of criteria imply a special analysis that should demonstrate that the safety criteria are met.

- Performance requirement, such as strength of components and safety components, e.g. safety valves.
- Fail safe requirements imply that certain component failures result in a safe state.
- Coverage requirements describe for which disturbances the safety system should be designed.
- Single and double failure criteria can describe how many different safety systems there should be, in order to prevent specific accidents.
- "Defence in depth" is an extension of the single failure criteria and was originally applied in the nuclear industry area.
- Demonstration that specific requirements are fulfilled, e.g. from authority regulations, international standards, or guidelines.

As a complement to risk based approaches, a category of assessments is concerned with the assurance of the safety integrity of the system. A number of methods are available, some are based on the energy concept [6]. Examples of more generic methods are barrier diagram analysis [4] and safety function analysis [7]. In this category, an international standard related to control systems and safety integrity could be included. It aims to describe a rational and consistent technical policy for all electrically-based safety-related systems [8].

One important aspect is the aim of the analysis and its intended use. It could for example concern one or more of the following:

- Identification of hazards.
- Assessment of the consequences of potential accidents.
- Assessment of the likelihood of potential accidents.
- Assessment of the prevention, control and mitigation measures.
- Identification of technical and organizational safety functions that should be carefully maintained and supervised.
- Give a basis for company safety management policy and practices.
- Satisfy demands from the authorities.

1.3 The problematic side

Problems with quantitative assessments have been debated from the 1970's with arguments for and against; for an overview see e.g. [2] and [9]. There are many known problems, e.g. considering human errors. The emphasis is often numerical error probabilities for use in fault trees. It is widely recognized that there are considerable uncertainties in the data available for inclusion in these analyses [10]. Benchmark studies have shown essential uncertainties in quantitative estimates, especially concerning probabilities [e.g. 11].

Qualitative judgements have other drawbacks. They are less systematically investigated, although they are frequently used. E.g. are probabilities often classified in coarse categories, as well as in categories of consequences. Criticism could be raised that such assessments are subjective. They also could be subject to wishful thinking if the consequence is high, it might be easy to predict that the likelihood is low.

There are also a number of problems, which can be observed less or more frequently in the practical applications of risk analysis and in formal risk management systems. However, this is only rarely reported in the literature. Some examples are:

- The risk analysis is seen as a separate activity, results are not used afterwards.

- There are often problems with the interplay between risk analysis, handling of production deviations, and system changes. There is a need for information between these activities, also in a long time perspective.
- Changes of organisation, downsizing, and responsibilities have an essential impact on the quality of the risk management system.
- Difficulties in obtaining data for estimation of probabilities.
- Problems with transparency. E.g. suspicions could be raised that assumptions and analysis are adjusted in order to get estimates of probabilities low enough to get an acceptable level.

2 ANALYSIS OF A CASE STUDY

2.1 The production system

In order to illustrate the problems that have to be tackled in an industrial environment, one accident has been chosen as an example. This accident occurred in a production system where old military ammunition is disassembled. In this specific production line small bombs containing a copper cone and explosive material covered with steel were separated into its constituents. The bombs are crushed mechanically after being cooled with liquid nitrogen, in order to get the steel cover fragile. The crushed material is than separated as shown in the simplified drawing in Fig. 1.

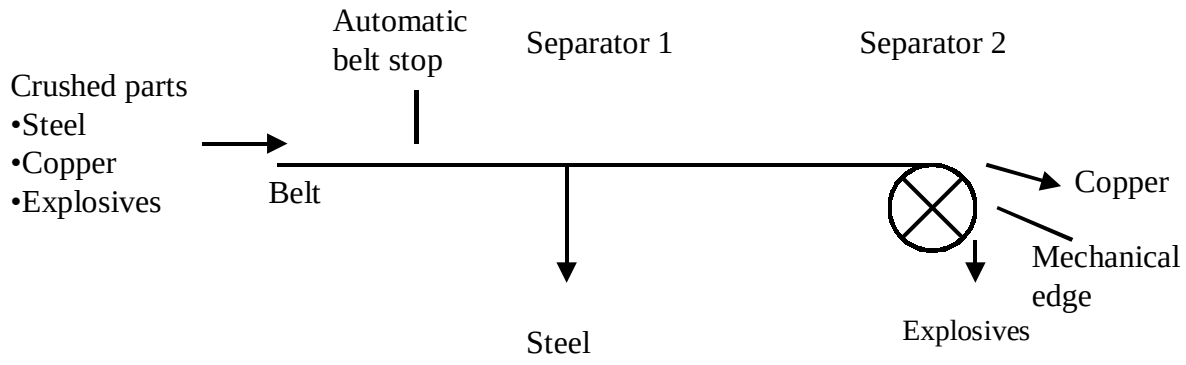

Fig. 1. Simplified drawing of the production line

Crushed parts are transported on a belt and passing an automatic belt stop, which allows small pieces to pass, whereas larger parts, e.g. whole bombs, will stop the band. Steel (magnetic material) is separated in Separator 1 and the rest (copper and explosives) continues. Separator 2 consists of a rotating permanent magnet, which separates copper from explosives.

As an extra safety barrier, the production line is placed inside a bunker and is managed by the operators from the outside.

2.2 Production start-up

During testing of the line and at production start-up a lot of deviations occurred. These deviations caused a series of “minor” changes in order to get the line to work properly, which is not an unusual situation in general. Important deviations (important as seen in the rear view) are given in Table 1.

2.3 Risk assessment

The company has several routines for risk assessment:

- Before a production line can be started a risk analysis has to be accomplished.
- Major changes have to be analysed from a safety perspective.

Prior to start-up of this line a risk analysis was carried out utilizing a type of PHA, which is commonly used in Swedish industry. After this analysis had been accomplished an operator instruction was written. The analysis also led to several changes in equipment.

Table 1 Production deviations and changes of equipment

Production deviations	**Changes of equipment as a result of the deviations**
Before start-up, the line was tested using bomb dummies. When whole dummies passed through all the way to separator 2, the dummies got stuck at the mechanical edge. Here, the dummies where heated at the separator and burnt stuck to the belt.	The distance of the mechanical edge was increased so that the dummies could pass out from the separator downwards.
Piles of crushed material kept triggering the automatic belt stop thus stopping the belt.	The automatic belt stop was disconnected
Larger pieces of copper passed the mechanical edge and were found in the explosives.	The distance of the mechanical edge was decreased in order to stop copper from passing out with explosives.
Bombs which had not been crushed passed through to separator 2, where they were separated together with steel.	No changes in equipment. The bombs were manually passed back to the crusher.

2.4 The Accident

The accident occurred when a whole bomb was not separated in Separator 1 and passed further to Separator 2. Here the bomb got stuck and the operators noticed the problem through an alarm. The production line was stopped, and the operators got clear sign from the control system to enter into the bunker. However Separator 2 was still rotating at a high speed although the power was cut off. This was enough to heat the bomb which exploded. The explosion initiated a secondary explosion of explosive dust in the vent system. Fragments from the ventilation system killed one of the operators.

2.5 What went wrong?

The technical reason for the accident is obvious. Changes of equipment as a result of the deviations during testing and start-up of production had seriously effected important safety functions in the process. No one was aware of this situation.

Some important observations are summarized regarding the situation prior to the accident.

- This particular hazardous event was not identified in the risk analysis.
- There was a time stress, as the production was behind schedule.
- Hundreds of production disturbances and deviations occurred and problems were continuously solved.
- Focus was on production.
- The company has a system for incident reporting but none of these deviations were reported. The deviations were identified as production deviations, not deviations affecting safety. A contributing factor was the stress and no time for reporting.

Although the company had high ambitions to have a good safety record, a number of good intentions failed. Could a different strategy have been more successful?

3 DISCUSSION

3.1 About management factors

After an accident has occurred, it is easy to say that the risks were evident, and that a risk analysis should have anticipated what happened. In this case, the system was changed several times, and it was not the "same system" as when the risk analysis was made. It should be noted that the deviations and actions described here were identified as important after the accident investigation. In reality there were hundreds of deviations of which the majority did not affect safety. A problem is how the dangerous ones should be selected in a reliable way.

Even if the specific risk had been identified, the probability for accident would have been given a very low value. That could be a reasonable estimate, since several safety barriers existed contributing to a reduction of the probability. In order to anticipate all the system changes occurring later, a far more sophisticated risk analysis would have been required. It might not be reasonable or effective to maintain a strict probabilistic risk analysis in this kind of production systems.

The accident could be interpreted as a failure of the “management of change” routine. The standard rule was that every change of significance for safety should be the object of a risk assessment. In order to keep production running, several adjustments were made on the equipment. They were seen both as minor and that they were not vital to safety. The management was focused on production.

It appears that management regarded the system as safe enough. They might have confidence in the conclusions of the risk analysis saying that the "risk was low". We only guess this; it is difficult to investigate peoples believes afterwards.

An interesting aspect how the risk analysis was performed, and why that approach was chosen. The reasons for making analyses were a combination of authority requirements and aspirations of the company. There were no guidelines how to perform an analysis and how the quality should be assured. However, this is a common lack at companies.

3.2 Conflicts and gaps

These interpretations point at potential conflicts and gaps between risk management intentions and the practical production demands. This could be summarized in three points.

- The "management of change" routines appeared to be seen as unpractical, since changes occur so frequently.
- Line management was mentally focused on production disturbances, and adjustment to changing demands. Safety implications were reflected on only to a small extent.
- In a way, the risk evaluation could be said to be partly counterproductive, since it led to an unjustified trust in safety. The management was not aware, that the assumptions made in the analysis were no longer valid.

These types of conflict are especially essential in production systems, which are frequently changed and exposed to disturbances.

3.3 Need for other types of risk assessment?

In situations, when these kinds of conflicts are likely to occur, it could be advantageous to investigate more qualitative approaches. It would mean a shift of focus from estimates of risk in terms of frequency and consequences, to the identification of hazards and to risk control. It is desirable to find sustainable safety solutions, which better could be integrated with production requirements. The safety solutions also have to be transparent to everyone working with the system.

A comparison of alternative qualitative approaches has been made (see section 1.2). On this case, a simple safety function analysis [7] was made as test to describe the safety features. A number of technical and organisational safety functions very quickly identified, and several of these had failed before the accident. In the discussion with the company, it showed that the concept of safety function was easily conceived and could be used in practical discussions.

This test indicated that Safety Function Analysis could be a suitable tool to give an overview of the technical and organisational safety functions of the system. One essential feature would be to clarify safety features, which simultaneously affects production and safety. It appeared plausible that a risk assessment of this kind would support preserving safety, also during a period of change.

The practical experience of the traditional methods based on identifying hazardous events and estimating risks based on frequency and consequence is not always encouraging, especially in this case. The ideas of a more qualitative focus on hazards and safety functions have been discussed with people involved in the production. At least in the light of the occurred accident, it appeared as such a concept would raise the quality and transparency of risk analysis.

4 CONCLUSIONS

Systems, which are frequently changed and exposed to disturbances, offer a number of difficulties in making a risk analysis. Risk assessments, especially based on probabilistic approaches, could easily be of reduced value, due to two major reasons:

1. Changes of the system makes the assumptions and data less valid.
2. It might be difficult for production people to interpret the relation between risks and system changes.

For this type of situations, alternatives to traditional probabilistic assessments could offer advantages. There are a number of qualitative approaches that are interesting to explore further. The application of Safety Function Analysis appeared to be prosperous according to the preliminary test made in this case study.

REFERENCES

[1] IEC. Dependability management -Risk analysis of technological systems. (IEC 300-3-9) International Electrotechnical Commission, Geneva, 1995.

[2] Lees, F. Loss prevention in the process industries (Sec.edition). Butterworth-Heinemann, Oxford. 1996.

[3] Papadakis, G. A. and Amendola, A. Guidance on the preparation of a safety report to meet the requirements of Council Directive 96/82/ec (SEVESO II). Office for the Official Publications of the European Communities, Luxembourg. 1997.

[4] Taylor, J.R., Becher, P., Pedersen, K.E., Kampmann, J., Schepper, L., Kragh, E., and Selig, R. Quantitative and qualitative Criteria for the Risk Analysis. Danish Environmental Agency, Copenhagen, Denmark, 1989.

[5] Harms-Ringdahl, L. Safety Analysis - Principle and Practice in Occupational Safety. (Second edition.) Taylor & Francis, London, 2001.

[6] Johnson, W.G. MORT Safety Assurance Systems. National Safety Council, Chicago, 1980.

[7] Harms-Ringdahl, L. Assessment of safety functions at an industrial workplace - a case study. In *ESREL2000 Foresight and Precaution*, A.A.Balkema, 1373-1378, 2000.

[8] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements. (IEC 61508-1) International Electrotechnical Commission, Geneva, 1998.

[9] Taylor, J. R. Risk analysis for process plan, pipelines and transport. E & FN Spon, London. 1994.

[10] Embrey, D. Guidelines for Preventing Human Error in Process safety. American Institute of Chemical Engineers, New York. 1994.

[11] Amendola, A., Contini, S., & Ziomas, J. Uncertainties in chemical risk assessment; Results of a European benchmark exercise. Journal of Hazardous Materials, **29**, 347-363, 1992.