

OPERATOR SUPPORT FOR ABNORMAL SITUATIONS USING SAFETY AND RELIABILITY KNOWLEDGE

P. Heino, P. Valkokari, K. Rönkkö, E. Kotikunnas and S. Lamberg

*VTT Industrial Systems, Risk Management
P.O. Box 1306, FIN-33101 Tampere, Finland
<http://www.vtt.fi/tuo/>*

Safety and reliability studies are standard practice in the process industry, and much of the information produced would be of benefit to plant operators and supervisors. In this study an information system to support risk management is being developed. Included is an abnormal situation management (ASM) documentation tool which stores the safety and reliability information in a structured database. Another part of the system, the disturbance analysis module, makes those safety and reliability analysis results which are relevant to the monitored situation available to the operations personnel and provides a tool for the recording of operating experiences. *Copyright © 2002 IFAC*

Keywords: Safety analysis, reliability analysis, risk, operators, chemical industry, processes, alarm, measurement

1. INTRODUCTION

Qualitative safety and reliability studies are standard practice in the process industry. As a result of those analyses, there is much information on the causes and consequences of hazards, failures and disturbances. These studies are not only useful for fulfilling the requirements set by authorities, but they also help to improve the performance of the plant. As most analyses are not computerised, the results are usually only available as paper-based documents. A majority of the information produced contains such information that could prove very useful also to the operations personnel at a plant – with the aid of appropriate information systems – if presented in a friendlier manner.

Already over ten years ago, research has been done on support systems for plant operation personnel (Venkatasubramanian and Rich, 1988). Heino *et al.* (1994) aimed to improve the utilisation of safety and reliability studies. Later on, abnormal situation management, aided by operator's tools, has been studied further (Nimmo, 1995). However, due to reasons recognised by Cochran and Rowan (1995),

the use of advanced decision support systems for abnormal situation management has not yet become common for chemical and petrochemical processes.

As part of the European part of the international CHEM¹ project, an information system to support risk management is to be developed over the next three years. VTT Industrial Systems' aim is to develop a tool to support the processing and storage of the safety and reliability analysis results in such a form that they can be more easily utilised. The tool will also make reliability and safety analysis results available to engineering and operations personnel and provide a facility for reporting actual disturbances. The tool will make reliability and safety analyses a part of daily operation routines by connecting the analyses to other plant information sources.

¹ CHEM Project is funded by the European Community under the Competitive and Sustainable Growth programme of the Fifth RTD Framework Programme (1998-2002) under contract G1RD-CT-2001-00466.

2. STATE-OF-THE-ART IN COMPUTER SUPPORTED PROCESS SAFETY

2.1 Review of earlier research

The rapid development of computer software and hardware systems has, during recent years, helped industrial companies dealing with complex process systems to provide useful support systems to their plant operations personnel. This was not evident ten years ago. Kim *et al.* (1990) pointed out that the nuclear industry in the USA was moving towards systems with symptom-oriented emergency operating procedures. This was partly due to the absence of a reliable and easily implementable methodology for building systems with capabilities for disturbance analysis.

Venkatasubramanian and Rich (1988) were pioneers in combining general and process specific knowledge in order to create a methodology which is suitable for practical use in industrial applications. Heino *et al.* (1994) aimed to achieve the same objective by improving the utilisation of existing safety knowledge resulting from process safety and reliability studies.

In spite of these and other developments, the use of advanced decision support systems for abnormal situation management is still not common in the chemical and petrochemical process industries. Cochran and Rowan (1995) analyse the obstacles which slow down the take-up of advanced decision support systems in complex process applications. Corporate downsizing and problems in showing the benefits to be gained by the use of such systems can make investments in advanced decision support systems look less attractive. Also, the poor capabilities of early systems in user-system collaboration may have had a negative impact on the public image of such systems.

The AEGIS system (Bullemer, *et al.*, 1999) developed in the USA by the Abnormal Situation Management (ASM) Joint Research and Development Consortium was a big step forward in the development and application of abnormal situation management methodologies. The AEGIS system has multiple roles as an element in the plant operation environment:

- State estimator,
- Goal setter,
- Planner,
- Executor,
- Communicator,
- Monitor.

These six functional roles of the AEGIS system give a good overview of the requirements to be set for an intelligent decision support system in a complex process operation environment.

It is a challenge for the on-going CHEM project and other researchers working on this topic to provide the best models and techniques to enable systems like

AEGIS to perform well in all the roles. There are numerous research groups all over the world doing high quality research on diagnostic systems and other relevant topics. A network of excellence resulting from the international part of the CHEM project could connect these research groups to the developers of industrial applications.

2.2 Issues to be resolved

Abnormal situations are a major concern to the process industry. They cost huge amounts of money to chemical industry in the form of damage, loss of market share, interruption costs, legal costs, etc. often in addition to severely injuring people. Abnormal situation management (ASM) has been studied actively during recent years, for example, in the ASM R&D programme of US chemical companies, automation system manufacturers and other industries (Nimmo, 1995).

One of the top causes for industrial accidents is human factors. In a study of 190 accidents in chemical facilities, the most frequent causes were insufficient knowledge (34%), procedural errors (24%), and operator errors (16%) (Nimmo, 1995).

To prevent accidents, operators need tools to perform more efficiently in abnormal situations. We must understand the root causes of these incidents and the steps that need to be taken to eliminate or prevent escalation from an abnormal condition to a major catastrophe (Nimmo, 1995). The ASM programme is aimed at the creation of methods and tools for this purpose.

One key issue in process operator decision support is alarm system configuration. In a complicated process, there can simultaneously be many alarms. What is required is some form of intelligence to put the alarms in context with the plant situation, eliminate unnecessary information and forward meaningful information to the operator and avoid information overload (Nimmo, 1995).

Early and accurate fault diagnosis forms the basis for effective abnormal situation management. It is very important to understand the state of the process at all times as well as the root causes of deviations. Control system design has traditionally been based on the current state of the system, but should be moved from a reactive mode to a predictive mode (Vedam, *et al.*, 1999; Nimmo, 1995). Plant personnel should have a clear and up-to-date understanding of the types of recently occurred abnormal situations, including the identified root causes and the steps to be taken to resolve problems of that kind.

Errors in situation assessment can also be a source of abnormal situations, assumptions can direct plant personnel down the wrong diagnostic path, and due to the response times required to correctly deal with a situation, the problem may escalate (Nimmo, 1995).

Nowadays, there is plenty of information at a plant in internal as well as external databases. However, operators are not always motivated to spend time in searching and browsing through accident databases (Chung and Jefferson, 1998). The use of this information should be made simple and a part of normal process control and monitoring routines. The user interface should focus on providing tools for the efficient generation, storage and retrieval of information in a problem-oriented manner (Heino *et al.*, 1994). User interface design, as well as system structure, can have a significant impact on the acceptability and utilisation of the system.

3. PROPOSED METHODOLOGY FOR ABNORMAL SITUATION MANAGEMENT

3.1 Objective of the methodology

VTT Industrial Systems intends to develop an information system to support risk management. The system will consist of two modules. The abnormal situation management (ASM) documentation module will be a tool for safety and reliability analysis result as well as other plant documentation management, which stores the information in a structured database. Both engineering personnel and operations personnel are given the possibility to utilise this information. The plant operations personnel will be provided with useful decision support information with minimal extra effort. The disturbance analysis module chooses and shows relevant safety and reliability analysis results related to the current process state and measurements. In addition, the module provides a feedback link to record operating experiences.

3.2 Introduction to the safety and reliability studies

A safety analysis is a systematic examination of the structure and functions of a system. The aims of a safety analysis are to identify factors that have the potential to contribute to accidents, to evaluate the risk induced by them and to find ways to minimise these risks. Safety analysis is a general term, which also includes the term risk analysis and thus the safety analysis process covers the risk analysis process. However, a safety analysis can also cover only a part of the risk analysis (Rouhiainen, 1990).

The aims of reliability analysis are to identify factors that have the potential to contribute to the reliability of a component or equipment, to evaluate for example, the production losses and maintenance costs induced by failures, and to find ways to minimise reliability risks. Reliability analyses are widely used in areas where they can be based on statistical component data. Qualitative reliability analysis methods can be used in plants where reliability data is not available.

A hazard and operability study (HAZOP) is a standard hazard analysis technique used in the assessment of new systems or modifications to existing ones. A hazard is a condition with the

potential of causing an adverse effect, for example, injury to people, damage to property or to environment, or weakening of the ability of the system to perform a prescribed function (Rouhiainen, 1990). A HAZOP study is a detailed examination, by a group of specialists, of components within a system to determine what would happen if any component were to operate outside its normal design mode.

Several other safety and reliability analysis methods are used in industry, e.g. FMEA (Failure Mode and Effects Analysis), ETA (Event-Tree Analysis), FTA (Fault-Tree Analysis). However, the main emphasis in this study will be on the HAZOP analysis method.

3.3 Basic functions of the modules

The tool being developed consists of two different modules – an ASM documentation and a disturbance analysis module – which are linked together by a database. A general description of the methodology is presented in Figure 1.

The ASM documentation module is a safety and reliability analysis – mainly HAZOP – documentation tool, which stores the analysis information in a structured database. Users experience data, which is a feedback link from the engineering and operations personnel, is also stored to the database. Other plant documents created during the plant's life (automation design process descriptions, automation design results, cycle operational instructions, checklists etc.) may also be imported into database. Alternatively, a link to the document or to other additional information of frequent need (chemistry, interlock information) can be used to access its contents. In cases where portions of a process have not yet been analysed, users' experiences or other plant documents can be used as a data source.

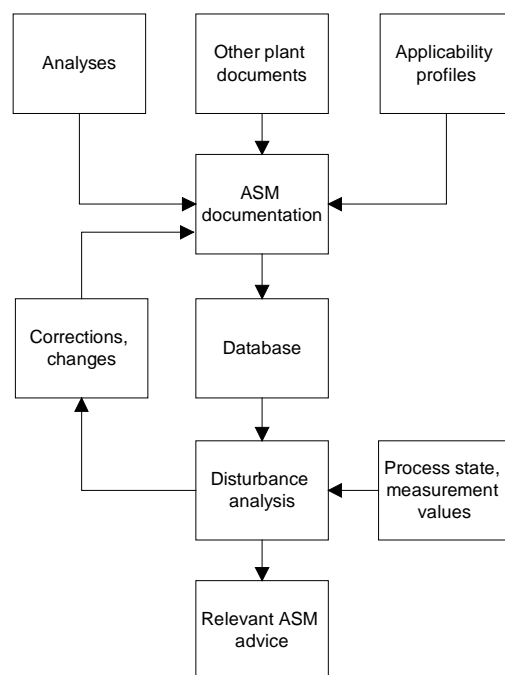


Fig. 1. The function of the tool to be developed.

Both engineering and operations personnel are given the possibility to use the analysis information. The plant operations personnel will be provided with useful decision support material with minimal extra effort. The disturbance analysis module is intended to make safety and reliability analysis results which are relevant to the monitored situation available to the operations personnel and to provide a tool for the recording of operating experiences.

3.4 Description of the ASM documentation methodology

The ASM documentation module is basically a database where safety and reliability related information is collected as abnormal situation management advice (ASM). ASM means either, for example, a HAZOP deviation with its causes and consequences, or a link to a document describing the process state and how to manage the abnormal situation. The main inputs, safety and reliability analysis objects, are to be defined properly. Special attention will be paid to the proper and useful content of the analysis data. An applicability profile will be attached to every ASM advice. The applicability profile is defined as a combination of the measurement and the process state. By fulfilling the conditions specified in the applicability profile, the piece of advice is assumed to be relevant. Careful definition of the applicability profiles is required in order to achieve a powerful disturbance analysis capability (Heino *et al.* 1994). The ASM advice is also linked to a process unit with a position within the process diagram.

In addition to analysis results and other documents, also users' experience notifications are used as a feedback link from operators to complement and correct the ASM database. The module includes a tool for the person maintaining the database to include operating experience notifications. The administrator will include new ASM advice into the database, filter user experience notifications and add appropriate portions of notifications to the database. Also "positive" information, e.g. how the process should be run under special conditions, is valuable to avoid production losses or accidents. The contents of the database will be used by the disturbance analysis module to show ASM advice in the form of events graphs or documents.

3.5 Description of the disturbance analysis methodology

The most important feature of the disturbance analysis module will be the mechanism for selecting data from a repository containing large amounts of various kinds of data. The selection mechanism is based on matching the current state of the process against predefined applicability profiles of the data contained in the data repository. Process state information obtained from other modules developed in the CHEM project, together with online measurement values obtained from the automation

system, are used to identify the relevant ASM advice. The module supports operator decision-making by indicating and allowing easy access to the relevant ASM advice – in the form of links to existing documents or as event graphs created from the safety or reliability analysis. The system will give a suggestion for relevant advice, but the operator is still responsible for browsing through the suggestions and evaluating their usefulness.

The second function of the toolbox is to collect operating experience data that is to be included in the database. The aim of the function is to easily modify and update the contents of the database, in a partly automated manner, using the tools from the ASM documentation module. Sometimes, the operating experience data may include useful information on non-measurable observations, such as smell, noise or visual observations.

The main output of the disturbance analysis module is ASM advice applicable for the current process state. The format will be based on the safety or reliability analysis results, and presented in an easily understandable form. Other advice in the form of hypertext will be shown using an appropriate viewer application.

3.6 IDEF0 descriptions of the modules

The functions of modules are described with the help of integrated computer-aided manufacturing definition, IDEF0 graphs. Both modules are presented in Figure 2 as an IDEF0 graph. An IDEF0 graph is used to document the functions of an enterprise in terms of inputs, outputs, controls and mechanisms. Functions are described inside, controls above (applicability profiles, process state and measurement), and mechanisms below (plant personnel) the boxes. The function of the ASM documentation module is to collect and update safety and reliability analysis data in the database. ASM data with its applicability profile obtained from the ASM documentation module acts as input for the disturbance analysis module – the function of which is to support operations personnel during abnormal situations by finding relevant ASM advice for each deviation.

4. TESTING OF THE METHODOLOGY

The system will be developed such as to be able to interface with commercial plant database and process control software. The developed methodology and tool will be tested and validated, both offline with real process data and online in a paper manufacturing process. The system will be directly applicable to process facilities to ensure rapid technology transfer. A methodology will be proposed so that, in the future, new supervision applications can be easily developed on different processes.

Reliability analysis has a crucial role in the definition of test cases for online tests. During an analysis,

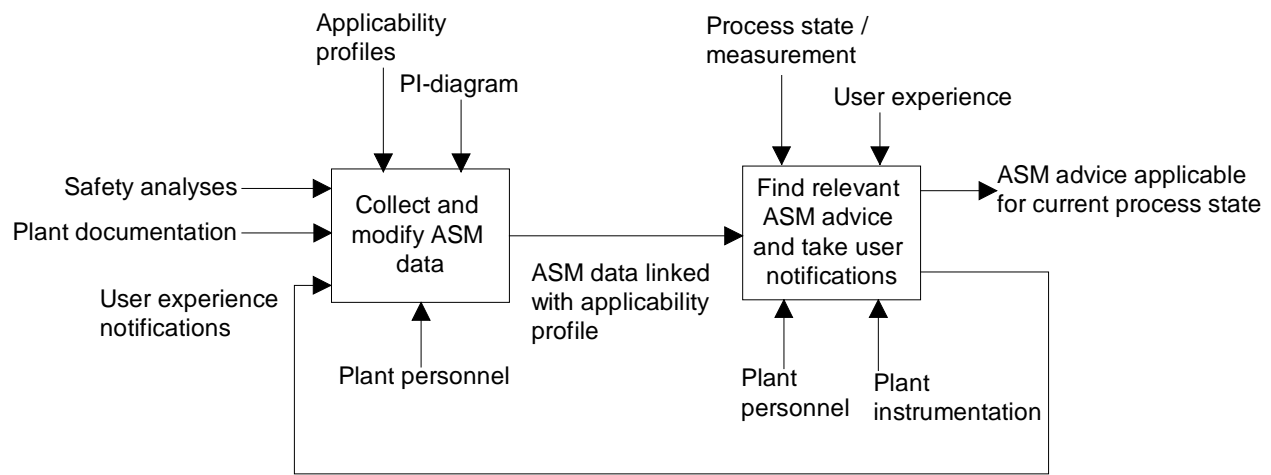


Fig. 2. Methodology for abnormal situation management.

several causes and consequences of fault situations will be identified. The consequences of some faults can be minimised by improvements, which eliminate the causes of the fault.

On the other hand, some faults will reoccur despite the improvements implemented, and these fault cases will form a key group for online tests. In these cases it is important to ensure that operators have the right instructions if the fault scenario occurs. In online testing, the developed application will be connected to the process automation system and it will be used to identify the relevant ASM advice from the set of analysis results according to the process measurements.

The reliability and safety analysis tool will be tested both on- and offline at the paper production line of UPM-Kymmene's Jamsa River mills, in Finland. At UPM-Kymmene, the most significant fault situations of the process will be analysed qualitatively and used in several test cases with the measurement data obtained from the process.

For paper machines, profit margin losses can extend into tens of thousands Euros per hour. Thus, it is important to ensure that breakdowns and the amount of poor quality paper are minimised. If relevant ASM data can be provided to the operators when faults occur, the proposed method could be found to be a significant tool in minimising the economic losses caused by faults.

In addition, the fluidised bed coal gasifier pilot plant of UPC (Universitat Politècnica de Catalunya) will be used in offline testing. The process data will be delivered as Matlab files. Some of the faults, and the HAZOP analysis results of those faults, will be considered.

5. CONCLUSIONS

It has been discovered that a majority of the safety and reliability information produced could prove to be very useful to plant operations personnel if presented in a friendlier manner. Thus, the aim of

this study is to develop an information system to support risk management.

The developed system will offer its users a methodology which stores safety and reliability related information in a structured database and makes the relevant results available to the operations personnel. The system also provides a tool for the recording of operating experiences.

Modern process plants are normally fitted with a number of sensors throughout the plant which warn operators if critical parameters are exceeded. The tool to be developed takes things a bit further by providing the operator with information about possible causes and consequences of the fault. This allows them to make a quicker and better judgement about what further action should be taken.

Embedding safety and reliability data from process plants into their control and monitoring systems will help operators understand deviations and control both safety and reliability risks. Apart from giving the operator more detailed information another benefit of the data approach is that the information already exists. Furthermore, the generated safety and reliability database becomes a living model of plant safety and reliability when it is kept up to date based on reports on actual process disturbances.

The systematic identification of hazards and the analysis of production dependability is becoming a part of daily life in any industrial activity. The improved data processing and management capabilities of modern networked computer systems provide the basis for the extended use of the resulting safety and reliability knowledge.

In this study, the developed methodology will be tested on- and offline in two continuous industrial processes. In the future, new supervision applications can be easily developed and installed also on different kinds of processes. The development and testing of the safety and reliability tool will occur as part of the CHEM project. In CHEM, 23 toolboxes for abnormal situation management will be developed, and because of the common framework,

the integration of the safety and reliability tool with other applications developed in the CHEM project will offer complete software solutions dedicated to specific processes (Cauvin, 2001).

REFERENCES

- Bullemer, P. T., Cochran, T., Harp, S. and Miller, C. (1999). Collaborative decision support for operations personnel. *INTERKAMMA 99 ISA Technical Conference*. 24 p.
- Cauvin, S. (2001). Integrated plant control promises safer working. URL: <http://europa.eu.int/comm/research/growth/gcc/projects/plant-control.html>. 23.11.2001.
- Chung, P.W.H, Jefferson M. (1998). The Integration of Accident Databases with Computer Tools in the Chemical Industry. *Computers and Chemical Engineering, Supplement*. Vol 22, pp. S729-732.
- Cochran, T. and Rowan, D. (1995). (Human) supervisory control and decision support: state of the art. *ISPE 1995, An International Conference on Intelligent Systems in Process Engineering*. 5 p.
- Heino, P., Karvonen, I., Pettersen, T., Wennersten, R. and Andersen, T. (1994). Monitoring and analysis of hazards using HAZOP-based plant safety model. *Reliability Engineering and System Safety*, 44, pp. 335-343.
- Kim, I. S., Modarres, M. and Hunt, R. N. M. 1990. A model-based approach to on-line process disturbance management: the models. *Reliability Engineering and System Safety*, 28, pp. 265-305.
- Nimmo I. Abnormal Situation Management. URL: <http://www.ics.org/memOnly/conference/papers/95N152.html>
- Rouhiainen, V. (1990). The Quality Assessment of Safety Analysis. *VTT Publications*, 61. Technical Research Centre of Finland. Espoo. 133 p.
- Vedam H., Dash S. and Venkatasubramanian V. (1999). An Intelligent Operator Support System for Abnormal Situation Management. *Computer and Chemical Engineering, Supplement*, pp. S577-580.
- Venkatasubramanian, V. and Rich, S. H. (1988). An object-oriented two-tier architecture for integrating compiled and deep-level knowledge for process diagnosis. *Computers and Chemical Engineering*, 12(9/10), pp. 903-921.