How to use lifecycle models for Process Safety Management?

Bert Knegtering
Honeywell Safety Management Systems
P.O. Box 116
5201 AC 's-Hertogenbosch
The Netherlands
bert.knegtering@netherlands.honeywell.com

Jan Rouvroye
Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven
The Netherlands
j.l.rouvroye@tm.tue.nl

This paper is a summary of "Safety lifecycle management in the process industries : the development of a qualitative safety-related information analysis technique" / by Bert Knegtering. – Eindhoven : Technische Universiteit Eindhoven, 2002. – Proefschrift. - ISBN 90-386-1747-X NUGI 684
To be defended on 17 May 2002.

1 Introduction

In spite of the application of a wide variety of safeguarding measures, many accidents in the process industries still happen today. Experiences gained from these past accidents have led to the development of an increasing number of technical solutions. One of the best known and widely accepted technical solutions concerns the use of Safety-instrumented Systems (SIS). In order to control the design and implementation of these technical solutions, numerous safety-related standards have been written. These safety standards are comprised of technology-oriented requirements concerning 'adequate' implementation of the designed solutions. Consequently, compliance with these standards is often considered to be 'good engineering practice'. Compliance with these technical standards, however, did not prevent several major accidents. As a result of the continuously growing complexity of both industrial processes and the related safety-instrumented systems, it appears that new kinds of problems have arisen [Kne01]. As this paper will show, many of these specific problems are related to the control of safety-related *business processes*. This is illustrated by a study performed by the British HSE. The HSE investigated the extent to which failures contributed to explosions in gas-fired plants in 1997. The failures were categorized into four groups (see Figure 1):

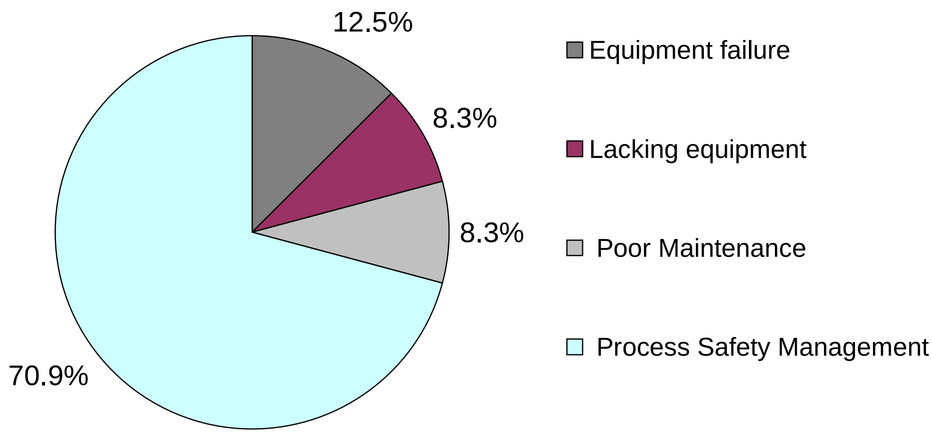

Figure 1 Contribution of failures to explosions in gas-fired plant [HSE97]

Review of recent studies on incidents and accidents shows problems regarding the quality of information on potential accidents and the related technological solutions. Therefore, adequate control of the quality of safety-related information seems to be of essential importance if realization of an acceptable safety level is to be achieved. As an answer to solve these problems related to business processes, recent standards on SIS have defined safety lifecycle models. Safety lifecycle models are considered to form an adequate framework to identify, allocate, structure, and control safety-related requirements. Standards on SIS often specify lifecycle phases of these models in terms of objectives, required inputs, and required outputs. A description of the objectives, inputs and outputs characterizes these aspects. It appears, however, that characterization itself is not always good enough to adequately achieve the defined objectives. This resulted in the definition of the following questions. The first question concerns the way in which lifecycle models can be used to improve safety-related business processes. It is subsequently questioned what exactly is included in each phase, and which other factors determine the quality of the objectives to be achieved in each phase. The third research question is how the lifecycle phases are mutually related, and how the quality of the completion of one phase influences the quality of the passing through of a subsequent phase, and how the quality of information exchanged between lifecycle phases could be controlled. A fourth question is how to measure these quality aspects in order to be able to control them.

2 Safety Lifecycle Management

In the process industries, Process Safety Management (PSM) embodies the whole of measures and activities to achieve an acceptable safe operating process installation. This includes the control of the safety-related business processes. Obviously, it needs to be known how these business processes can be controlled. Therefore, it needs to be established which aspects or parameters influence these processes and can subsequently be used to control them. This implies that measurement and analysis of the parameter values should result in the necessary information in order to take appropriate control actions. An essential question that needed to be answered was which parameters are most relevant to be controlled. To answer this question, the PSM involved business processes were divided into the elementary safety-related activities. For each of these activities, the most relevant parameters that influence the performance of the involved activity were established based on the key performance indicator as used in the field of reliability information management. This resulted in the development of the Safety-related Activity Management or SAM model. In order to control the performance of the involved activity the values of these parameters must be measured and controlled.

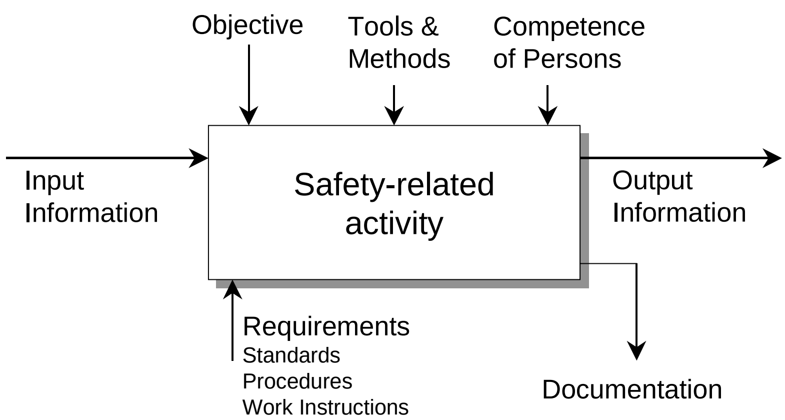

Figure 2 Safety–related Activity Management (SAM) model

Because of the fact that the activities as part of PSM are interrelated to each other, the performance of one activity directly influences the performance of other activities. The safety lifecycle model was used to establish the relationship between the involved safety-related activities. This resulted in the development of the Safety Lifecycle Activity Management or SLAM model. This model describes the information flows between the safety-related activities that need to be realized. The application and control of the PSM related business processes, as based on the concepts of the SAM and SLAM models, is captured by the term Safety Lifecycle Management (SLM). SLM is defined as: '*the integral control of the safety management activities with regard to all phases of the safety lifecycle. The control is based on the application of a structured safety lifecycle model, which is the framework on which the safety management system is established.*'

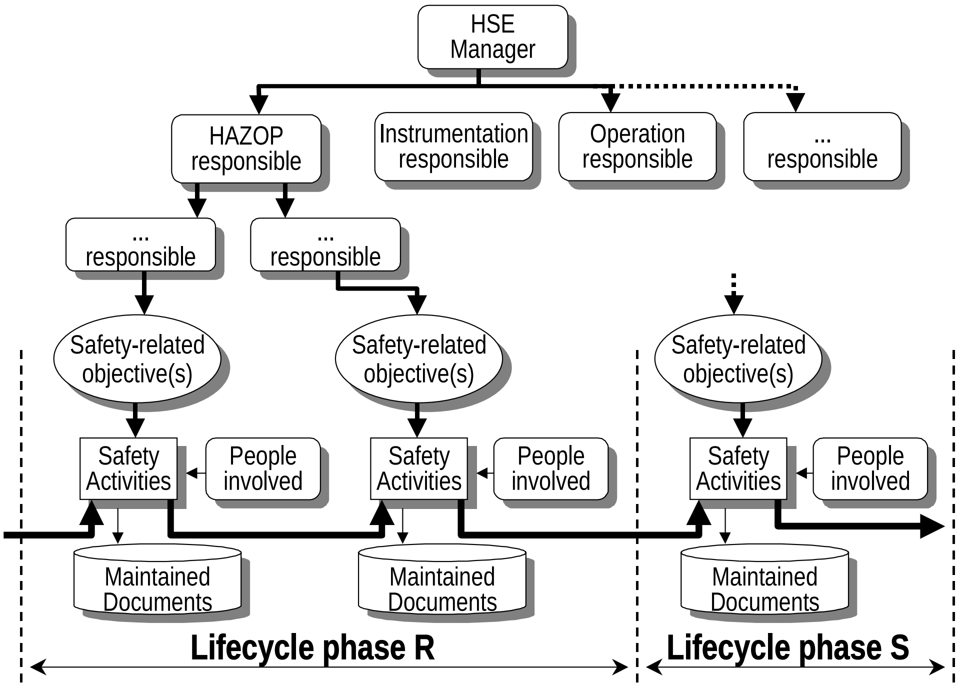

Figure 3 Lifecycle-based management approach

To adequately control the SLM activities, proper information must be available and thus a number of information flows is required. The research described in this paper demonstrates that the quality of information flows directly influences the control of safety-related business processes. It is therefore demonstrated that qualification of information flows substantially helps to control safety-related business processes. In order to develop qualification criteria of safety-related information flows, concepts of reliability-related information management techniques (the MIR (Maturity Index on Reliability) concept [Bro00]) are adapted for the specific application of controlling safety-related information.

Table 1 Description of MIR levels

SIS-related SMS	Description of reliability problem handling	MIR
Uncontrolled	No reliability tests or measurements are performed	**0**
	Reliability tests are performed, where failures are detected and their rates are stored (action not vital)	**1**
	Partial analysis is conducted in order to take appropriate repair actions	**2**
Controlled	Complete fault analysis whereby SIS performance is guaranteed and controlled	**3**
	Complete fault analysis, information is stored and evaluated for future improvement actions	**4**

Based on the SLM concepts and on the MIR concept, the formalized MIR-based SLM analysis technique has been developed. This analysis technique consists of 7 steps that led to the detection and explanation of safety-related problems that might result in an accident. One of the main steps in the MIR-based SLM analysis technique is the development of safety-related activity and information flowcharts. The application of safety lifecycle models clearly structures the development of these flowcharts.

3 MIR-based SLM analysis case studies

3.1 Eleven case studies

A total of eleven MIR-based SLM analysis case studies have been performed. The cases concern observed safety-related problems, which were later on explored and explained using the MIR-based SLM analysis technique. In order to draw general conclusions on the added value of the developed analysis technique, this section will give an overview and evaluation of all case study results.
In order to compare the study results of the eleven cases, comparison criteria need to be defined. Because it appeared that some companies were much further developed in the process of implementing the latest SIS standards than others, it is chosen to define the comparison criteria such that the these differences are included in this overall evaluation. The cases are therefore evaluated and compared based on the following aspects:

— Separation between BPCS and SIS
— SIS standard applied
— Safety lifecycle model defined
— SIL defined
— Problem observed in IEC 61508 Overall lifecycle model
— MIR level observed problem

Table 2 gives an overview of the comparison results. Subsequently, the description of these aspects and the results of the evaluation are discussed.

Table 2 Comparison and evaluation of all cases

	Separation between BPCS and SIS	SIS standard applied	Safety lifecycle model defined	SIL defined	Problem observed in IEC 61508 Overall lifecycle model *	MIR level observed problem
Case 1	yes	yes	yes	other	6,7,8,15	1,2
Case 2	no	yes	no	other	9,14	2
Case 3	yes	yes	no	no	3,4	1
Case 4	yes	no	no	yes	3,4	1
Case 5	no	no	no	yes	1,2	-
Case 6	yes	no	no	yes	4	2
Case 7	yes	no	no	yes	3,4	1
Case 8	yes	no	no	other	4,13	1,2
Case 9	no	yes	yes	other	5	1
Case 10	-	yes	yes	other	4,5	2
Case 11	-	yes	yes	yes	13	2,3

* *These number refer to the phases of the Overall Safety Lifecycle of IEC 61508 part 1. (See also reference on IEC 61508)*

— *Separation between BPCS and SIS*

A first aspect that is compared concerns the observation whether the subject organization has installed separate systems for process control (BPCS) and process safety (SIS). Because it appeared that a number of organizations that are investigated did not have adopted this separation, these organizations were expected to have significantly more difficulties with the implementation of e.g. IEC 61508. In total, three companies did not define clear separation between the BPCS and SIS. The first company (case 3) had problems between the operation and maintenance department, and the departments responsible for previous activities of the safety lifecycle model. The probable reason that no problems appeared in phases 3,4 or 5 is that equal equipment was applied for control as well as for safety but nevertheless the same equipment was used for both applications. From that point of view, a kind of separation in functionality was realized. The observation that no dedicated equipment was used for safety purposes was one of the root causes of the observed problems. Case 5 appeared to have problems, allocated in phase 1 and 2, for the reason that one and the same safeguarding instrumentation was used for control and safety function. Case 9 appeared to have problems in phase 5 (which at that moment did not yet have any relation to the observation that no separation was realized), because this company had decided to apply dedicated safeguarding instrumentation in future. Therefore, the problem was related to the allocation of (part of) the safety requirements to the SIS.

— *SIS standard applied*

It appeared that particularly the larger companies have defined their own corporate standard, which are based on the official SIS standards. The smaller companies tried to directly follow the official standards or adopted one of the corporate standards.
It was observed that the application of a corporate standard has certain advantages as well as certain disadvantages. The advantage is that general requirements can be translated into more practical requirements which are easier to understand and easier to implement. On the other hand it was observed that in a number of cases the official standards were not correctly translated into the corporate standard. (For instance, the fact that for case 1, 2, 8, 9 and 10 the company had defined their own safety levels, which did not match with the defined SIL's of the official standard.) The corporate standard of the company that was analyzed in case 2 did not appear to have defined a safety lifecycle, although this corporate standard was based on the ANSI/ISA S84.01 standard.
Case 4 through case 8 concerned companies who did not yet adopt a SIS standard, but were confronted with certain requirements of SIL-based standards (e.g. the fact that certain equipment needed to comply with a certain SIL). The observed problems were primarily the consequence of the fact that without adoption of such a standard the process of implementing certain requirements is more complicated.

— *Safety lifecycle model defined*

A total of 7 out of the 11 companies that were investigated during the case studies did not have defined a safety lifecycle model. Those companies that had a corporate SIS standard showed a better result. The corporate SIS standard of only 2 out of 6 companies did not include a safety lifecycle model. The observed problems of the 7 companies with no defined safety lifecycle model, appeared to be directly the result of the fact that no safety lifecycle model existed, and thus no clear overview of interrelated activities and lifecycle phases, and responsible persons was present. The observed problems at the remaining 4 companies were the result of incorrect or incomplete implementation of the lifecycle model.

— *SIL defined*

Not every company turned out to have adopted the SIL terminology as defined by the latest SIS standards. Some companies already had defined and implemented another kind of categorization of safety levels. It appeared that one company did not define different safety levels at all. Obviously, many problems that were observed, were related to the fact that deviations from the official SIS-related standards existed. In a number of cases this deviation appeared to lead to inconsistency, which formed the basis for the observed problems. The fact that each SIL represents a specific quantified availability performance of the SIS, appeared to contribute to a common understanding of its added value. At the same time however, it was observed that consistent application of safety integrity levels by different departments was experienced to be very difficult. The fact that e.g. a Safety Instrumented System (SIF) and its SIL is designed by the instrumentation department, but can only be controlled during operation if the maintenance department operated correctly, was often considered as difficult to comprehend. In many cases the definition of safety lifecycle models helped to explain this relationship.

— *Problem observed in the IEC 61508 Overall lifecycle model*

Each problem that is observed during the case studies has been allocated to the particular lifecycle phase of the Overall safety lifecycle model of IEC 61508. The reason that this lifecycle model is used, is because it is the most extensive model and most referred to. The allocated lifecycle phases indicate the phase(s) where the root causes of the problem are observed. Especially in case 1 many phases with problems were allocated. This case study was not restricted to exploring and explaining a particular problem, but all phases were analyzed in order to determine if they complied with IEC 61508. The observation that phase 6,7,8 (planning phases) and 15 (modification or retrofit phase) did hardly or not exist, resulted in the consequences that also following phases were not correctly implemented. Concerning the other cases, it was observed that most problems are observed in the first 5 phases. (A total of 6 out of the 11 cases appeared to have problems with phase 4, i.e. specification of the safety requirements.) These phases concern the hazard & risk assessment, and the specification and allocation of the safety requirements. The fact that for each SIF a SIL needs to be determined, is in many cases observed as being difficult and therefore causing a number of problems. Limited guidelines and general requirements are often experienced as difficult to implement.

— *The observed MIR level*

The observed problems during the case studies are analyzed in order to determine the actual achieved MIR level. The determination of the MIR level is based on the criteria as defined in the previous section and focuses on the quality of the information that is created. The observed problems are considered to be the result of inadequate information, or otherwise expressed, the result of a too low quality level. Not surprisingly, the observed problems that are evaluated are classified lower than MIR level 3. The specific problems concern the implementation of new safety standards that the investigated companies struggle with. Their first challenge is to implement and control the standard requirements. The second challenge is to improve their safety management by learning from experiences. Obviously, the first challenge goes together with control problems. A total of 6 problems were allocated to MIR level 1 and also a total of 6 problems were allocated to MIR level 2. Apparently, to a certain degree the investigated companies do measure problems and determine specific modifications. The fact that the business processes were nevertheless not under control is assumed to be the result of insufficient information of the root causes of the problems.

3.2 Conclusions on the 11 case studies

— *MIR-based SLM analysis technique*

Based on the case study results, it is concluded that the MIR-based SLM analysis technique has the ability to prevent safety-related problems before they result in serious accidents. This prevention concerns two aspects. Firstly, the analysis technique has proven to be able to detect otherwise probably undetectable problems in actual situations. Furthermore, the MIR-based SLM analysis technique offers the ability to further explore and explain these safety-related problems.

Detection and explanation are essential steps towards taking adequate actions and thereby solving these problems. The power to detect and explain these problems is the result of focusing on the functionality of the SIS. The SIS often appeared to be considered as physical equipment that is able to measure process parameters and activate certain field devices if certain process parameters exceed specific limits. The new approach, where the SIS is considered as equipment that is used to fulfill certain safety functions and reduces the process risks to acceptable level, results in a completely different interpretation of these systems. The detected problems would probably not have been detected without this new approach.

— *Safety lifecycle models*

The utilization of safety lifecycle models offers the ability to analyze potential problems and their impact on later lifecycle phases. Allocation of a potential problem in one phase offers the ability to determine in which specific phase such a problem is best prevented by taking appropriate measures. In 4 cases safety problems were found in companies that had defined a safety lifecycle model. It is therefore concluded that the definition of such a lifecycle model is an important step towards controlled safety-related business processes, but nevertheless the implementation and control of the involved safety-related activities requires additional effort.

— *SLM modelling concept*

The MIR-based SLM analysis technique focuses on the analysis of safety management systems that are based on a defined lifecycle model. An aspect of the SLM modeling concept is that safety-related activities are allocated to phases of the lifecycle model and relationships between them are indicated. The MIR-based SLM analysis technique focuses particularly on the quality of the safety-related information flows. Obviously, the SLM model is used to establish where, when, and what kind of information needs to be created, and where this information must be available to be processed. Safety management systems that are not based on the SLM modeling concept have proven to show a worse MIR-based SLM analysis performance.

— *Allocation of MIR levels to information flows*

The assignment of MIR levels to information flows indicates the actually achieved quality level and needs to compare this level with the required quality level. Qualification of information flows to specific MIR levels helps to explain the actual type and attributes of information and eventual shortcomings of this information. SIS standards such as IEC 61508 only define in rather general terms the required information that is needed for a particular lifecycle phase. It is experienced that detailed qualification of information is needed to improve the control of safety-related activities.

— *Relationship of MIR levels and industrial safety*

The relationship of achieving e.g. a MIR 4 and achieving a safe operating process installation is not guaranteed. MIR 4 implicates that the safety-related information flows are controlled and the infrastructure for improvements is implemented. The actual safety level depends on the level of the process installation risks and on the defined acceptable residual risk level, after the implementation of the risk reduction measures. It is nevertheless concluded that an unsafe operating plant can only become a real safe plant, if an adequate measurement, control and improvement process has taken place. Such a process is only then successful, if the required information flows are realized correctly. Therefore, it is stated that a unsafe plant can only achieve a safe state, if control (MIR level 3) and improvement mechanisms (MIR level 4) are in place.

— *Quality of safety-related activities*

Currently, no criteria or models exist to assist the process of determining the effort and time that should be spent on a certain safety-related activity in relationship with other safety-related activities. For example, a minimum effort could be spent on the determination of the required safety integrity level of a particular SIS. However, within the same Safety Management System (SMS) a huge effort may be spent on the validation process to exactly determine the realized probability of the SIS to fail to perform its design function in case of a demand due to an out of control process.

— *Consistency of terms and definitions*

The processing and control of safety-related information is considered to be of essential importance to successfully carry out the activities. With respect to this, it is observed that an unambiguous understanding of terms and definitions is a prerequisite. Problems might arise at the moment that e.g. people from the HAZOP team have a different understanding of the definition of a SIF than people from the instrumentation department. For instance, if people from instrumentation, operation or maintenance do not understand that a SIL is related to time, safety-related problems might arise.

— *Problem areas of safety lifecycle models*

It appeared that many problems were found in the first phases of the IEC 61508 Overall safety lifecycle model. The most probable reason is that, at the time the case studies were carried out, the lifecycle-based SIS standards were only recently published. It appeared that in the first place companies struggle with the determination of the SIL requirements. The second difficulty concerns the design, implementation and validation of the SIS. Furthermore, these standards have defined a lot of requirements on how to comply with a specific SIL. The first phases of the investigated safety lifecycle models consists of the risk assessment and the determination of the SIL requirements. Because the SIS standards have not defined requirements on acceptable risk levels and the allocation of safety requirements to different risk reduction measures, these phases require a considerable input of the companies themselves. Furthermore, it appeared that especially those phases of the lifecycle model that do not contain detailed requirements but only general requirements, are experienced to be difficult to implement. A generic standard such as IEC 61508 with general requirements is often experienced as being difficult to translate into concrete requirements or procedures.

4 Industrial perspectives

Based on the experiences gained during the various case studies, the following points for improvement to use safety lifecycle models, safety integrity levels, the SLM concept and the MIR-based SLM analysis technique in an industrial environment are established. In particular, extensive application will result in improved industrial use of the SLM concept and the MIR-based SLM analysis technique, and as a consequence in improved PSM.

– *SLM models*

At almost every company, investigated during the case studies, it has been experienced that it is very difficult to explain that the success of the implementation of the safety lifecycle model depends on the preparedness of different departments to cooperate. It appears e.g. to be difficult to explain that a shared responsibility exists with regard to the entire lifetime of safe operations. More case studies should demonstrate which type(s) of organization structure are best suitable for safety lifecycle management.

– *Need for SLM implementation guidelines*

During the case studies, it was often observed that the different departments, which were involved in the safety-related activities of the safety lifecycle model, many times operated as independent self-regulating entity. Account is in those cases only given to the head of the department, who, once again, needs to give account to his superiors. During the case studies, this observation was often revealed and it was explained that the latest safety standards require a more ‘horizontal approach’ of controlling the safety-related business processes. Although a certain level of awareness and commitment towards these new insights was created, the organizations still struggle with the implementation. More industrial experience with the implementation of the SLM concept should lead to the development of implementation guidelines for these organizations.

– *Quality levels of safety-related activities*

The safety lifecycle model comprises a collection of safety-related activities, structures these activities in time, and structures them in relationship with each other. The MIR-based SLM analysis technique primarily focuses on the quality of information flows between safety-related activities. The quality of these safety-related activities itself however, directly influences the performance of the SMS and the quality of the information flows. The quality of the performance of each activity depends, amongst other things, on the quality of the input information. The term ‘amongst others’ could for instance be the quality of the methods and tools used to carry out the activity. The SAM model describes these other aspects. This is supported by the conclusion in the previous section that a MIR level 4 does not mean that a highly safe operating plant is achieved, but only that the ability and infrastructure is in place to control and improve the safety-related business processes. More industrial experience with the qualification of the SAM model parameters will help to determine the criticality of the performance parameters of safety-related activities.

– *Need for SIL requirement determination guidelines*

The definition and implementation of safety lifecycle models, as required by the latest SIS-related standards, is an essential step towards the control of the safety-related business processes. The lifecycle model framework clearly offers a structure for this control. Nevertheless, it appears that problems are still observed at companies who have implemented such a lifecycle. Therefore, it is concluded that the requirements surrounding the implementation of the lifecycle model, still appear to be difficult and additional guidelines are needed. The fact that the latest SIS-related standards primarily focus on requirements on how to realize and maintain a required SIL, demonstrates the restricted scope of these standards. Concerning other risk reduction measures as implemented in safety-related systems, it is not improbable that also for these systems specific SIL-based standards will be developed. These standards will, in that case, most probably also be based on the concept of safety lifecycle models, comparable with the ones of e.g. IEC 61508. What is not covered are guidelines on the process of determining the required safety integrity levels for all these risk reduction measures in order to achieve an acceptable residual risk level. Further development is required to develop these guidelines.

– *MIR-based SLM analysis technique*

Much of the successful execution of the MIR-based SLM analysis technique still depends on the expertise and perception of the researcher. The development of models and theories offers enough structure for a scientist to analyze safety-related business process problems. However, the described analysis technique is still characterized as being generic and not made specific for the analysis of particular safety-related activities. Especially, techniques concerning the qualification of the sources that generate information, the qualification of the information transfer medium and the qualification of the manner the information is offered for further processing, need to be developed. In this respect, the quality of the mechanisms available for communication between sender and receiver of information should also be considered.
With regard to MIR analyses that are carried out in other industrial sectors, the experiences show that a high level of expertise is still required and criteria on the achieved MIR level are not defined clearly and unambiguously.

The application of the analysis technique proves that indeed a reasonable explanation of safety-related information transfer problems could be given for problems which otherwise were difficult to explain or unexplainable. Based on eleven industrial case studies, these safety lifecycle model based activity flowcharts have proven to be a valuable means to explain the observed problems. It is concluded that the application of the SLM concepts together with formalized MIR-based SLM analysis technique enables an organization to allocate weaknesses in the control of safety-related business processes. It offers the ability not just to learn from accidents that have actually occurred, but more important to serve as a means to prevent these accidents from occurring. Latent problems within the safety management system are traced much earlier, and can subsequently be resolved before they result in serious accidents.

5 General conclusion

In general, it was expected that the theoretical principles of SLM and the conceptual steps of the formalized MIR-based SLM analysis technique could be very well applied to other industrial sectors. The MIR theory that has been adopted (and adapted) from its development area, namely the consumer products industry, immediately demonstrated its applicability in a different industrial sector. It is the general impression that many problems related to quality, reliability or safety of products, processes or services are analyzable using the MIR concepts, on the condition that their realization is characterized as being reproducible or repetitive.

6 Bibliography

[Acu02] Acu Tech Consulting Inc. – AcuSafe Newsletter January 2002. http://www.acusafe.com/Newsletter/Stories/0102News-MonthlyIncidents.htm

[Bro00] Brombacher, A.C. – Designing reliable products in a cost and time driven market: a conflict or a challenge Inauguration speech, Eindhoven University of Technology. February 18. 2000

[CCPS89] Center for Chemical Process Safety (CCPS) – Guidelines for Technical Management of Chemical Process Safety New York: American Institute of Chemical Engineers. 1989

[Hee99] Heel, K.A.L. van , Knegtering, B , Brombacher, A.C. – Safety Lifecycle Management – A flowchart presentation of the IEC 65108 Overall Safety Lifecycle Model
Quality and Reliability Engineering International 15: 1999

[HSE97] Health and Safety Executive, clause 6.2 of Contract Research Report 139/1997, ‘Explosions in gas-fired plant’ United Kingdom 1997

[IEC61508] IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems 1998/2000

[IEC61511] IEC 61511 – Functional safety: Safety-instrumented Systems for the process industry sector (Draft version 1999)

[ISA96] ANSI/ISA S84.01 – 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709 1996

[Kne01] Knegtering, B. – Safety Lifecycle Management
Automation in Petro Chemicals Industry Conference
Congress center Delft University of Technology, 21-22 November 2001

[Kne99a] Knegtering, B , Bakel van, F, – Experiences with organizational aspects of implementing the IEC 61508 safety standard into an existing quality management system Philadelphia – ISA-Tech 1999

[Kne99e] Knegtering, B., Brombacher, A.C., Heel, K.A.L. – Safety Lifecycle Management In Process Industries International conference safety of industrial automated systems
IRSST – Montreal, Canada 1999

[Tha99] Thai Oil Refinery – Laem Chabang Thailand, Gasoline storage tank explosion.
US Chemical Incident Reports Centre Databases. December 17, 1999