

Safety Lifecycle Management In The Process Industries

The development of a qualitative safety-related information analysis technique

Copyright © 2002 by B. Knegtering

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Knegtering, Berend

Safety lifecycle management in the process industries : the development of a qualitative safety-related information analysis technique / by Berend Knegtering. – Eindhoven :

Technische Universiteit Eindhoven, 2002. – Proefschrift. -

ISBN 90-386-1747-X

NUGI 684

Keywords: Safety lifecycle management / Safety management systems / Lifecycle models / Safety instrumental systems / Process safety / Maturity index on reliability

Printed by: University Press Facilities, Eindhoven

Safety Lifecycle Management In The Process Industries

The development of a qualitative safety-related information analysis technique

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. R.A. van Santen, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op vrijdag 17 mei 2002 om 16.00 uur

door

Berend Knegtering

geboren te Eindhoven

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr.ir. A.C. Brombacher
en
prof.dr.ir. J.C. Wortmann

Copromotor:
dr.ir. J.L. Rouvroye

Summary

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 [Kne00b], [Kne01]. As this thesis will show, many of these specific problems are related to the control of safety-related *business processes*.

Review of recent studies on incidents and accidents showed 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 research 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 that arose during the research performed in this thesis is how to measure these quality aspects in order to be able to control them.

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 which 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.

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.'*

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 thesis 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) are adapted for the specific application of controlling safety-related information.

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.

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.

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.

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

Samenvatting

Ondanks het toepassen van een breed scala van veiligheidsmaatregelen, vinden vandaag de dag nog velerlei ongevallen plaats in the procesindustrie. Ervaringen opgedaan naar aanleiding van deze ongevallen hebben geleid tot een steeds verder groeiend aantal technische oplossingen. Een van de bekendste en meest toegepaste technische oplossingen betreft de instrumentele beveiligingen. Aangaande het beheersen van het ontwerp en uitvoering van deze technische oplossingen, zijn talrijke veiligheidsnormen opgesteld. Deze veiligheidsnormen bevatten technologiegeoriënteerde eisen betreffende ‘adequate’ implementatie van de ontworpen oplossingen. Daaruit volgend blijkt dat overeenstemming met deze normen vaak wordt beschouwd als ‘good engineering practice’. Echter, naleving van deze technische normen heeft verscheidene zware ongevallen niet weten te voorkomen. Als gevolg van een continue toenemende complexiteit van zowel industriële processen als betrokken instrumentele beveiligingsystemen, is gebleken dat een nieuwe type problemen zijn ontstaan [Kne00b], [Kne01]. Zoals dit proefschrift zal aantonen betreffen deze specifieke problemen het beheersen van de veiligheidsgerelateerde *bedrijfsprocessen*.

Bestudering van recent onderzoek van ongevallen laat problemen zien met betrekking tot de kwaliteit van informatievoorziening aangaande potentiële ongevallen en de gerelateerde technologische oplossingen. Daarom blijkt dat adequate beheersing van de kwaliteit van veiligheidsgerelateerde informatie van essentieel belang is indien een acceptabel veiligheidsniveau behaald dient te worden. Om een antwoord te vinden op deze bedrijfsprocesproblemen, hebben recente normen aangaande instrumentele beveiligingen zogenoemde veiligheidsgerelateerde levenscyclus modellen gedefinieerd. Veiligheidsgerelateerde levenscyclus modellen worden beschouwd een adequaat raamwerk te geven om veiligheidseisen te identificeren, lokaliseren, structuren en te beheersen. Normen op het gebied van instrumentele beveiligingen hebben de fasen van levenscyclus modellen gedefinieerd in termen als doelstellingen, vereiste input en vereiste output. Een beschrijving van de doelstellingen, input en output karakteriseert deze aspecten. Het blijkt echter dat karakterisering zelf, niet altijd voldoende is om op adequate wijze de gedefinieerde doelen te bereiken. Een eerste onderzoeksvraag betreft daarom de wijze waarop levenscyclus modellen kunnen worden gebruikt om veiligheidsgerelateerde bedrijfsprocessen te verbeteren. Het is vervolgens de vraag wat er precies door elke fase wordt omvat en welke factoren de kwaliteit bepalen van de te realiseren doelstellingen. De derde vraag betreft op welke wijze levenscyclus fasen onderling verbonden zijn, op welke wijze de kwaliteit van de uitvoering van een fase de kwaliteit van het doorlopen van een volgende fase beïnvloed, en hoe de kwaliteit van informatie-uitwisseling tussen levenscyclus fasen beheerst kan worden. Een vierde vraag die is opgekomen tijdens het onderzoek betreft de wijze waarop deze aspecten gemeten kunnen worden om beter te weten te kunnen komen wanneer deze aspecten aangepast dienen te worden.

In de procesindustrie belichaamt veiligheidsmanagement het geheel aan maatregelen en activiteiten welke dienen om een acceptabel veilig opererende procesinstallatie te bereiken. Dit behelst het beheersen van de veiligheidsgerelateerde processen. Overduidelijk geldt dat bekend zal moeten zijn hoe deze processen beheerst kunnen worden. Het is daarom noodzakelijk vast te stellen welke aspecten of parameters deze

processen beïnvloeden en vervolgens gebruikt kunnen worden om ze te beheersen. Dit impliceert dat het meten en analyseren van de parameters dient te resulteren in de benodigde informatie om de juiste beheersacties te kunnen nemen. Een essentiële vraag welke beantwoord dient te worden betrof welke parameters het meest relevant zijn om te beheersen. Om deze vraag te beantwoorden werden de veiligheidsmanagement-gerelateerde bedrijfsprocessen opgedeeld in elementaire veiligheidsgerelateerde activiteiten. Voor elk van deze activiteiten zijn, op basis van betrouwbaarheidsinformatie management concepten, de meest relevante parameters bepaald welke de prestatie beïnvloeden. Dit heeft geresulteerd in de ontwikkeling van het zogenoemde 'Safety-related Activity Management' of SAM model. Om de prestatie van de bijbehorende activiteiten te beheersen, moeten de waarden van deze parameters gemeten en beheerst worden.

Vanwege het feit dat de activiteiten welke onderdeel zijn van het veiligheidsmanagement, onderling afhankelijk van elkaar zijn, beïnvloedt de uitvoering van een activiteit direct de uitvoering van andere activiteiten. Het veiligheidsgerelateerde levenscyclus model is gebruikt om de relatie tussen de betrokken veiligheidsgerelateerde activiteiten vast te stellen. Dit heeft geresulteerd in de ontwikkeling van het 'Safety Lifecycle Activity Management' of SLAM model. Dit model beschrijft de informatiestromen tussen de veiligheidsgerelateerde activiteiten die dienen te worden gerealiseerd. De toepassing en beheersing van de veiligheidsmanagement gerelateerde bedrijfsprocessen, zoals gebaseerd op de concepten van de SAM en SLAM modellen, zijn samengevat in de term Safety Lifecycle Management (SLM). SLM is gedefinieerd als: *'het integraal beheersen van veiligheidsmanagement activiteiten met betrekking tot alle fasen van de veiligheidslevenscyclus. Het beheersen is gebaseerd op de toepassing van een gestructureerd levenscyclusmodel, welke het raamwerk betreft waarop het veiligheidsmanagement systeem is vastgesteld.'*

Om op adequate wijze de SLM-gerelateerde activiteiten te beheersen, dient de juiste informatie beschikbaar te zijn en dus is een aantal informatiestromen vereist. Het onderzoek, beschreven in deze dissertatie, toont aan dat de kwaliteit van informatiestromen direct het beheersen van veiligheidsgerelateerde bedrijfsprocessen beïnvloedt. Het is daarom aangetoond dat kwalificering van informatiestromen substantieel helpt om de veiligheidsgerelateerde bedrijfsprocessen te beheersen. Ten behoeve van de ontwikkeling van kwalificatiecriteria voor veiligheidsgerelateerde informatiestromen zijn concepten met betrekking tot betrouwbaarheidsgerelateerde informatiemanagement technieken (het MIR (Maturity Index on Reliability) concept) gebruikt en aangepast voor de specifieke toepassing betreffende het beheersen van veiligheidsgerelateerde informatie.

Gebaseerd op de SLM concepten en het MIR concept, is een geformaliseerde MIR-gebaseerde SLM analysetechniek ontwikkeld. Deze analysetechniek bestaat uit 7 stappen welke leiden tot het herkennen en verklaren van veiligheidsgerelateerde problemen welke kunnen leiden tot een ongeval. Een van de hoofdkenmerken van de MIR-based SLM analysetechniek is de het opstellen van veiligheidsgerelateerde activiteiten- en informatie-stroomdiagrammen. De toepassing van veiligheidsgerelateerde levenscyclus modellen structureert op duidelijke wijze de opstelling van deze stroomdiagrammen.

Toepassing van de analysetechniek heeft bewezen dat inderdaad een aanvaardbare verklaring van veiligheidsgerelateerde informatie-overdrachtsproblemen kan worden gegeven, voor problemen welke anders moeilijk of niet te verklaren zouden zijn.

Gebaseerd op 11 industriële casussen, hebben de veiligheidsgerelateerde activiteiten- en informatie-stroomdiagrammen op basis van de levenscyclus modellen bewezen een waardevol middel te zijn op de waargenomen problemen te verklaren. Het is geconcludeerd dat toepassing van de SLM concepten samen met de geformaliseerde MIR-gebaseerde SLM analysetechniek een organisatie in staat stelt om zwakheden in het beheersen van de veiligheidsgerelateerde bedrijfsprocessen te lokaliseren. Het biedt de mogelijkheid om niet slechts te leren van opgetreden ongevallen, maar belangrijker om te dienen als middel ter voorkoming van deze ongevallen. Latente problemen omtrent het veiligheidsbeheersysteem worden eerder getraceerd en kunnen vervolgens worden opgelost alvorens zij resulteren in een ernstig ongeval.

In het algemeen is verwacht dat de theoretische principes van SLM en de conceptuele stappen van de geformaliseerde MIR-based SLM analysetechniek zeer goed ook in andere industriële sectoren toegepast zouden kunnen worden. De MIR theorie, welke is overgenomen (en aangepast) van haar ontwikkelingsgebied, namelijk de consumenten-productindustrie, laat direct de toepasbaarheid in een andere industriële sector zien. Het is de algemene indruk dat velerlei problemen die zijn gerelateerd aan kwaliteit, betrouwbaarheid of veiligheid van producten, processen of diensten, analyseerbaar zijn met gebruikmaking van de MIR concepten, onder de voorwaarde dat hun realisatie is gekenmerkt als zijnde reproduceerbaar dan wel herhaalbaar.

Acknowledgment

I remember well the moment during the ISA show in Houston Texas in October 1998, that Kees Kemps, Aarnout Brombacher and I had dinner in an Italian restaurant. It was at that occasion that we made the plan how to set-up the Ph.D. research and combine it with my work for Honeywell. Now, a little more than three and a half years later, that intent has resulted in this thesis.

Writing a thesis is not something you just do by yourself at an unimpeded moment. During the time period of three and a half years, many people have been of great support. Colleagues, both from Honeywell and from the Eindhoven University of Technology, relationships in the industries, friends, and family have helped me in accomplishing this assignment. Therefore, I would like to take this opportunity to thank a number of them in particular.

First, I would like to thank Honeywell Safety Management Systems b.v. Initially, an agreement was made to finalize the dissertation within four years. Since that moment, nobody ever spoke about this agreement and probably nobody knows what happened with it, but nevertheless I managed to finish it in time!

Considering this, I can merely conclude that Honeywell has never put the slightest obstacle in my way to work on the research, and gave me the freedom and support that was required to complete the work and combine it with my work for Honeywell. One of the most supportive persons regarding this was Kees Kemps. As my superior, he was a real prop and stay. Thank you for this, Kees!

Furthermore, I would like to thank my colleagues at the office in 's-Hertogenbosch. In particular the colleagues from the sales department, who many times had the patience to listen to me explaining the status of my research and who reacted always in a motivating way.

Aarnout Brombacher is a very special person, who has undoubtedly been my strongest motivator. His unlimited enthusiasm and unremitting support inspired me to keep the right mood and attitude to work on this thesis. Although the fact that he often had a very busy schedule, it appeared to never be a problem to arrange a meeting and talk things over. Quite a number of times this meant that I was welcome at his home and combined progress meetings with an excellent meal. Another moment I recall is Singapore in the summer of 1999. A place that is known for its constant and predictable weather but, while we had dinner outside together with Ineke, was seized by tremendous thunderstorm. Peculiar, if you consider the different places we met. I really owe him something and hope that I can show it by a continuation of our cooperation in future.

Another really great thanks goes to Jan Rouvroye. I don't think that there is any person who has commented and read this thesis more times than he did. Particularly the first rough versions must sometimes have been a real abhorrence to read. You were a true sounding board and have probably no idea how valuable this has been!

I sincerely want to thank the core promotion committee, consisting of Ad Hamers from Honeywell, Hans Wortmann from Baan and from the Eindhoven University of

Technology, Peter Sander from the Eindhoven University of Technology, Martin Newby from City University London, and Jan Rouvroye and Aarnout Brombacher as already mentioned. It was their not always to be envied task, to read the draft versions of my thesis. The many structural comments and recommendations that resulted from the committee meetings, have definitely contributed to this final thesis.

Obviously, the mentioned time period of three and a half years was not spent twenty-four hours a day, seven days a week on research and writing. Fortunately, I am in the wealthy position of being surrounded by a lot of friends with whom I spent many holidays, such as skiing vacations, sailing camps or other activities. Their presence gave me the very much-needed distraction to my research.

Last but not least, I want to thank my family. The warm relationship I have with my sisters and brothers-in-law is absolutely a pleasant environment in which to write a thesis. Playing with my nephews and nieces was always great fun!

I want to mention my father, who unfortunately died in the summer of 1982. If only he could have been here these moments. I guess he would have been a proud father.

Finally, I want to thank my mother. She probably had numerous moments wondering whether I would manage to combine my various pursuits with my schooling. While raising three children by herself, she must have had her hands full and presumably has gone through not always easy times. I hope this thesis shows that things turned out fine.

Once again, thank you all!!

Confidentiality of acquired field information

To a large extent, information coming from companies which are active in the process industries, is used within this thesis, e.g. as described by various examples and the included case studies. The author has gathered this information during many projects and site visits as a consultant with Honeywell Safety Management Systems b.v. Because company-related safety issues and safety policies are often considered to be confidential information, the names of the involved companies as described in the cases have been withheld.

Table of contents

<i>Summary</i>	I
<i>Samenvatting</i>	V
<i>Acknowledgment</i>	IX
<i>Confidentiality of acquired field information</i>	XI
<i>List of figures</i>	XVII
<i>List of tables</i>	XIX
<i>Abbreviations</i>	XXI
1 Safety and risks in the process industries.....	1
1.1 Introduction.....	1
1.2 Recent accidents.....	1
1.3 Growing complexity of industrial processes.....	2
1.4 Need for enhanced Process Safety Management	3
1.5 General problem description.....	5
2 Research objective, scope, and methodology	7
2.1 Research specification and scope.....	7
2.2 Research type and methodology	10
2.3 Research program.....	13
2.4 Research expectation.....	15
2.5 Outline of this thesis	15
3 Safety-instrumented Systems	17
3.1 Layers of Protection	17
3.2 Definition of a Safety-instrumented System	18
3.3 Safety Integrity Levels	19
3.4 Typical problems of safety-instrumented systems.....	20
4 SIS-related legislation, standards and lifecycle models.....	23
4.1 Legislation on process safety	23
4.2 Relationship between legislation and standards.....	24
4.3 New developments of safety standards.....	25
4.4 Recent standards on safety-instrumented systems	25
4.5 Safety lifecycle models	26
4.6 Parallels and similarities regarding safety lifecycles	29
4.7 Current problems with the implementation of safety lifecycles	30

5	Controlling safety-related business processes.....	33
5.1	Process safety management.....	33
5.2	Safety-related business processes	37
5.3	System theory and control engineering.....	39
5.4	Lifecycle modeling.....	44
5.5	Related parallel research in the field of reliability management.....	46
5.6	Further specification of the research	53
6	Safety Lifecycle Management.....	57
6.1	Introduction to the management of safety-related activities	57
6.2	Elementary lifecycle management aspects.....	60
6.3	Scope of the involved lifecycle management activities	60
6.4	Development of the lifecycle management model.....	60
6.5	Safety-related Activity Management model	61
6.6	Development of the Safety Lifecycle Management concept	68
6.7	Safety Lifecycle Activities Management model	70
6.8	Organizational structures and the SLM concept	74
6.9	Evaluation of the SLM concept.....	78
7	Development of a MIR-based SLM analysis technique	79
7.1	The objective of a SLM analysis technique	79
7.2	Usability of the MIR concept for SLM analysis	80
7.3	Elaboration on safety-related information management	86
7.4	Earlier experiences with SLM and MIR techniques in other applications.....	90
7.5	Formalization of the MIR-based SLM analysis technique	96
7.6	Expected benefits of the MIR-based SLM analysis technique	102
7.7	Recapitulation	104
8	Case studies	105
8.1	Design of the case studies	105
8.2	Case 1 – IEC 61508 Overall safety lifecycle model analysis of a Belgian plant of a Swedish company.....	108
8.3	Review case 1, adapted strategy case 2.....	112
8.4	Case 2 – ANSI/ISA S84.01 safety lifecycle model analysis of a Dutch site of an American chemical company	112
8.5	Recapitulation of case studies 1 and 2	118
8.6	Evaluation of all case studies	119
8.7	Conclusions on all case studies	122
8.8	Discussion on industrial perspectives	124
9	Conclusions and recommendations.....	127
9.1	Conclusions	127
9.2	Discussion and recommendations on further research.....	131
10	Bibliography.....	133

Annex A Case studies	143
Annex B Standards and documents comprising lifecycle models	169
Annex C SLM interview procedure and questionnaire.....	173
Annex D Development aspects of activity flowcharts.....	181
Annex E SLM activity flow chart symbol conventions.....	183
Annex F Steps used in activity model development.....	187
Curriculum Vitae.....	189

List of figures

Figure 1	Contribution of failures to explosions in gas-fired plant [HSE97].....	4
Figure 2	IEC 61508 Part 1, Overall safety lifecycle (see also Figure 7)	6
Figure 3	Concept of layers of protection [IEC61511-1]	18
Figure 4	Safety-instrumented System	19
Figure 5	Safety-instrumented Function.....	19
Figure 6	Primary causes of control system failures [HSE95]	21
Figure 7	IEC 61508 Part 1, Overall safety lifecycle	27
Figure 8	Concept of risk reduction.....	35
Figure 9	Main activities of risk management.....	35
Figure 10	An open system with its boundary and environment [Rob90]	40
Figure 11	HAZOP study activity, required inputs and outputs.....	41
Figure 12	Long-linked technology [Tho67].....	41
Figure 13	Intensive technology [Tho67].....	42
Figure 14	Activity model with required inputs and outputs [Mol01]	43
Figure 15	Example of related lifecycle phases	45
Figure 16	Cost impact of design stages as a function of the development phase	51
Figure 17	The V-model.....	52
Figure 18	Shared responsibility for the specification, realization and utilization of the SIS.	52
Figure 19	HAZOP, a safety-related activity	59
Figure 20	PSM, a collection of safety-related activities	59
Figure 21	Ishikawa diagram showing input categories resulting in the output.....	63
Figure 22	Safety-related Activity Management (SAM) model.....	64
Figure 23	Information flow from activity M to activity N.....	71
Figure 24	Identification of information sources.....	72
Figure 25	Allocation of involved people	72
Figure 26	Relationship between people and safety-related objectives	73
Figure 27	Allocation of lifecycle phase boundaries.....	74
Figure 28	Line management, the vertical approach.....	75
Figure 29	Process management, the horizontal approach.....	76
Figure 30	Lifecycle-based management approach.....	77
Figure 31	Steps from every reality to SLM modeling and visa versa.....	79
Figure 32	Storage of test results.....	82
Figure 33	Testing and repair actions.....	83
Figure 34	Analysis of failure rate data.....	84
Figure 35	Development of a knowledge database	85
Figure 36	Aspects of information flows.....	87
Figure 37	Categories of information	93
Figure 38	Communications between a superior and other superiors and executors	95
Figure 39	Reference safety lifecycle model.....	98
Figure 40	Differences between ‘formal’, ‘actual’ and ‘ideal’ situations	99
Figure 41	Simplified flowchart of the combined lifecycle phases.....	110
Figure 42	Missing or incomplete phases.....	110
Figure 43	SIS lifecycle model as resulting from the case study	114
Figure 44	The observed SIS-related safety lifecycle model	117
Figure 45	Risk matrix of the fertilizer plant.....	144
Figure 46	Activity flowchart of the HAZOP and SIS realization phases	145

Figure 47	Safety-related activity flowchart of the American oil company.....	147
Figure 48	The first three phases of the Overall safety lifecycle model of IEC 61508.....	148
Figure 49	Risk graph.....	150
Figure 50	Phases 3, 4 and 5 of the IEC 61508 Overall safety lifecycle model.....	151
Figure 51	Safety-related activity flowchart of the Hungarian oil refinery.....	154
Figure 52	Safety-related activity flowchart of the Belgian oil refinery.....	156
Figure 53	Safety-related activity flowchart of this Belgian chemical site.....	158
Figure 54	IEC 61508 Overall safety lifecycle model (phase 3,4,5 and 9), and lifecycle phase 9.1 of the E/E/PES lifecycle model.....	160
Figure 55	Primary causes of control system failures [HSE95] (see also Figure 6)	162
Figure 56	Three-tiered approach of covering aspects of the IEC 61508 safety standard	163
Figure 57	The Quality Evolution model [AT&T90].....	164
Figure 58	The organization with its product creation process (PCP), product realization process (PRP) and parallel processes.....	165
Figure 59	The Product Creation Process (PCP).....	166
Figure 60	Model of development engineering activities.....	167
Figure 61	Flowchart of the main phases of the Logic Solver lifecycle	168
Figure 62	ANSI/ISA S84.01 : Safety lifecycle	169
Figure 63	IEC 61511 Part 1, Safety lifecycle	171
Figure 64	EN 50126-0 : System lifecycle.....	172
Figure 65	Safety-related activity model.....	174
Figure 66	Different situations that can be distinguished.....	174
Figure 67	Example of process-oriented information and task oriented information flows .	176
Figure 68	Various types of information flows	177

List of tables

Table 1	Main steps of the research project.....	13
Table 2	PFD requirements per SIL	20
Table 3	Description of MIR levels based on modeling cases 1 - 4.....	86
Table 4	Description of quality levels of safety or reliability problem-related information ..	88
Table 5	Description of barrier types.....	90
Table 6	MIR-based SLM analysis steps	96
Table 7	Applicable tools, techniques, methods per MIR level	101
Table 8	Comparison and evaluation of all cases.....	120
Table 9	MIR-based SLM analysis steps (copy of Table 6 Chapter 7, Section 5.2).....	130
Table 10	Consequence categories	144
Table 11	Probability categories.....	144
Table 12	Risk graph parameters.....	149
Table 13	Accident scenario A	150
Table 14	Accident scenario B	150
Table 15	Activity flow chart symbol conventions	183
Table 16	Steps used in activity model development.....	187

Abbreviations

AIB	Automated Independent Backup
ANSI	American National Standards Institute
ARL	Acceptable Risk Level
BPCS	Basic Process Control System (IEC 61511)
CC	Common Cause
CCPS	Center of Chemical Process Safety (USA)
CFR	Code of Federal Regulation (USA)
C&E	Cause and Effect
DC	Diagnostic Coverage
E/E/PE	Electric/Electronic/Programmable Electronic
EPA	Environmental Protection Agency (USA)
ERRF	External Risk Reduction Facility
ESD	Emergency Shut Down
ETA	Event Tree Analysis
EUC	Equipment Under Control
FAR	Fatal Accident Rate
FEL	Front End Loading
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
HSE	Health Safety and Environment
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
IPF	Instrumented Protective Function
ISA	Instrument Society of America and Control
ISO	International Organization for Standardization
LTI	Lost Time Injuries
MIR	Maturity Index on Reliability
MIS	Management Information System
MOC	Management Of Change
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
OSHA	Occupational Safety and Health Administration (USA)
OTB SRS	Other Technology-Based Safety-Related System
PDP	Product Development Process
PLC	Programmable Logic Controller
PRP	Product Realization Process
PFD	Probability of Failure on Demand
PFDavg	Average Probability of Failure on Demand

PFSavg	Average Probability of a Safely tripped process
PHA	Process Hazard Analysis
P&ID	Piping and Instrumentation Diagram
PSM	Process Safety Management
QMS	Quality Management System
RMP	Risk Management Plan
RR	Risk Reduction
RRF	Risk Reduction Factor
SAM	Safety-Related Activity Management
SF	Safety Function
SFF	Safe Failure Fraction
SHE	Safety, Health and Environment
SIF	Safety-Instrumented Function
SIL	Safety Integrity Level
SIS	Safety-Instrumented System
SLAM	Safety Lifecycle Activity Management
SLC	Safety Life Cycle
SLM	Safety Lifecycle Management
SMS	Safety Management System
SR	Safety-Related
SRS	Safety-Related System
STR	Spurious Trip Rate
SWIFT	Structured What If Technique
TI	Off-line Proof Test Interval
TR	Trip Rate

1 Safety and risks in the process industries

1.1 Introduction

Major industrial accidents, such as those that occurred in Bhopal, India, Seveso, Italy, Three Mile Island, Piper Alfa, are vivid reminders of the destruction that can occur due to inadequate safety measures. Huge losses of human life, immense environmental pollution, and large capital costs were involved.

Unfortunately, extremely serious accidents still happen today. For example, in December 1999 a refinery fire due to an overflowed tank occurred at the national oil company of Thailand. Seven people died and thousands of people were forced to flee their homes [Tha99]. Another characteristic example involves a gas explosion at the Kuwait national oil refinery in June 2000. Five people were killed, and 49 people were seriously injured. Presumably the most impressive recent accident concerns the explosion at the AZF chemical fertilizer factory in Toulouse, France in 2001.

1.2 Recent accidents

The fact that safety in the process industry is still a topical subject, is probably best illustrated by the following summary of accidents that occurred during the period of five weeks from December 14 of the year 2001 until January 18 of the year 2002 [Acu2002]. The summary only concerns accidents that were reported to the local authorities. The actual number of accidents (including smaller ones) is assumed to be much higher.

- ...
- *December 14* Iowa Ammonia Pipeline Leak Leads to Massive Fish Kill
- *December 16* Illinois Hydrochloric Acid Leak Leads to Evacuations
- *December 17* Static Electricity Blamed in Georgia Paint Plant Blast
- *December 19* Wyoming Refinery Blast Injures 2
- *December 23* Custodial Worker Killed by Ammonia Leak
- *December 29* Peruvian Fireworks Blast Kills 122
- *January 2* Many Killed In Chinese Fireworks Explosion
- *January 7* Chemical Leak Settles over New York Town
- *January 7* Iowa Fertilizer Leak leads to Fish Kill
- *January 8* Explosion at Louisiana Chemical Plant Felt Miles Away
- *January 13* Nine Injured in Explosion at Texas Refinery
- *January 13* Five Injured in Louisiana Refinery Fire
- *January 15* UK Platform Evacuated after Gas Leak
- *January 18* N. Dakota Derailment, Ammonia Leak led to 1 Death
- ...

Many good reasons can be enumerated that justify the application of the various safeguarding measures in the process industry. These reasons can be divided as follows:

- Protect people from harm and protect the environment.
- Satisfy laws and regulations.
- Reduce cost of production loss and cost due to damage to equipment.
- Lower losses due to negative impact on ‘company image’ and lower plant risk profile (Insurance premium cost).

Whether these aspects are relevant or not, depends on the typical application, environmental circumstances, and requirements from local legislation. It is the responsibility of a company to establish the need of dealing with these aspects.

1.3 Growing complexity of industrial processes

The last decades, industrial processes are becoming more and more complex [Lee96]. Expanding product and production requirements led to further optimization of the concerned processes. Due to continuously increasing competition, the necessity for increased productivity force process installations to operate to their limits. At the same time, a growing number of different semi-manufactured products put a high demand on the flexibility of the process installations, resulting in several different applications. Dedicated instrumentation, which also makes process control more and more complex, is expected to control and safeguard these processes. As a consequence of the growing complexity of the process installations, the control instrumentation, and safeguarding instrumentation, safety-related business processes have become even more difficult to manage [Kne98c], [Kne00a]. Furthermore, many individuals and organizations are involved in the design, implementation, and operation of process installations, including the end-user, the engineering contractor, the system integrator, and the equipment suppliers. For instance, consider an oil company that decides to build a new refinery at a certain location. Normally, an engineering contractor, who becomes responsible for the design and realization of the new installations, is hired. Dedicated system integration engineering companies are assigned to provide automated process control equipment. Manufacturers, vendors, and suppliers of instruments all are responsible for the design and development of those instruments.

Fortunately, during the last decades, much has been improved in the process industry. Thorough investigations of accidents have resulted in specific hazardous event prevention with regard to process installations. Consequently, many new safeguarding measures have been developed and are implemented. However, at the same time it has become increasingly difficult to acquire a comprehensive view of the entire processes, installations, and instrumentation. Due to this growing complexity and an ever-expanding process capacity, the potential for serious accidents have heavily increased. For instance, increased automation (hardware) might simplify the operator’s role but may increase the complexity and frequency of maintenance. *‘Operators may rely on alarms to warn of upset potentials and relax their tracking of operations if a system is overly automated. Reliance on the operator to take certain actions in emergency situations may not take completely into account fatigue, time to respond, background noise levels obscuring alarms, inadequate numbers of types of communications channels, and the like’* [CCPS89].

A striking example concerns the accident at the nuclear power plant at ‘Three Miles Island’ in the U.S. In 1979, on March 28, unit 2 of the plant was operating at full power. A pump in the secondary circuit failed, resulting in an automated stop of the turbine. The temperature in the primary cooling circuit increased. A valve opened to lower the pressure. If the pressure decreased sufficiently, this valve, the Pilot Operated Relief Valve (PORV), would close. After some time the control lamp indicated that the PORV was normally closed. Nevertheless, the pressure in the primary system decreased. Afterwards, it appeared that the valve was stuck at open, finally leading to the melting of the reactor core. At the control room of the Three Mile Island plant there were over 100 alarms in 10 seconds, causing the alarm printer to be two hours behind. There were also conflicting indicators, and some indicators appeared to be hidden (e.g. not shown on the operator’s process control monitoring screen) [Per84]. Obviously, due to the complexity of the installation, the operators were no longer able to bring the process to a safe state. To this day, this accident is considered to be the biggest accident in the nuclear industry in the U.S.

1.4 Need for enhanced Process Safety Management

The set of safety-related operational processes and activities, which results in a specific safety performance of a process installation, is covered by the term ‘process safety management’. (See also Chapter 5). A study performed by the British Health and Safety Executive (HSE) clearly illustrates that inadequate process safety management is the most essential factor that contributes to the number of hazardous events [HSE97]. 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):

- Equipment-related failures, such as a manufacturing failure, design faults, or incorrect specification.
- The lack of equipment and equipment, which should have been fitted to the plant, but was not.
- Poor maintenance and incidents resulting directly from poor maintenance/commissioning.
- Inadequate process safety management.

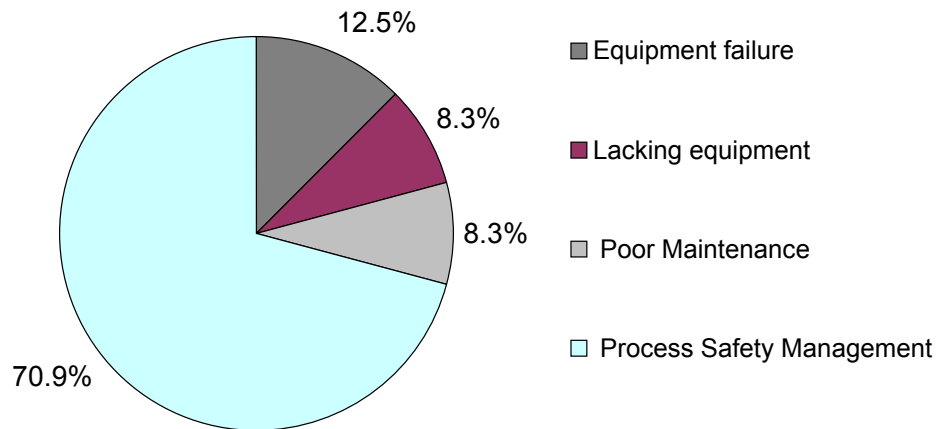


Figure 1 Contribution of failures to explosions in gas-fired plant [HSE97]

The overwhelming contributing factor that resulted in the explosions was inadequate PSM. A detailed analysis revealed that this deficient PSM was due to a lack of training, poor managerial supervision, and insufficient procedures [HSE97: Health and Safety Executive, clause 6.2 of Contract Research Report 139/1997, 'Explosions in gas-fired plant' United Kingdom 1997].

Bradley [Bra99] illustrates other examples of the causes of major industrial incidents. Based on his study, manufacturing and equipment failures contribute to only 10% of all investigated failures. The remaining contributing factors are operating errors, management errors, design/specification errors, and maintenance errors.

As part of another study, the HSE [HSE95] investigated 34 incidents which were the result of control system failures, occurred in the UK (see also Chapter 3). The primary causes of the control system failure were found to be specification failures, design and implementation failures, installation and commissioning failures, operation and maintenance failures, and failures to due changes after commissioning. In fact, failures appeared to occur during all phases throughout the lifetime of the control system. The task of the safety management system is to prevent these failures from occurring. (See also Chapter 5.)

A third example is concerns a study performed by the American Environmental Protection Agency (EPA). During many years, The EPA reviewed a large number of investigations of chemical plant accidents. The EPA's Chemical Emergency Preparedness and Prevention Office found, among other things, that operator errors were rarely the sole or even primary cause of an accident [Fel01], [Bel00]. Another maybe even more striking conclusion was the fact that often the hazard analysis did not consider known equipment failures:

'Shell Chemical's Deer Park, Texas analysis, for instance, did not consider the possibility of check valve failure, even though the problem had plagued several other Shell facilities. "If hazards are never reviewed or analyzed," Belke wrote, "then avoiding accidents is more a matter of luck than design." One of Belke's most damning observations is that "disasters are often preceded by a series of smaller accidents, near misses, or accident precursors"

“For most major chemical accidents, EPA and OSHA believe that it is rarely the action or inaction of a single operator that is the sole or even primary cause of an accident. The Safety Precedence Sequence illustrates that numerous barriers must fail before operator action can cause an accident” [Fel01].

In conclusion, the following trends are currently observed in the process industry:

- Industrial processes are becoming more and more complex.
- Expanding need of production capacity and flexibility.
- Increasing numbers of people and organizations are involved.
- Higher circulation of employers and employees.
- Growing appeal on information and communication means.
- High cost in case of an unwanted spurious process trip.
- Large consequences in case the process gets out of control.

The majority of accidents in the process industry are not particularly the result of failure of the equipment or installation, but rather the result of inadequate safety management. Therefore, control and improvement of the safety performance should not be attempted in the area of technological improvements of the equipment, but rather in the area of safety management. The focus and attention should be to enhance the control and organization of the safety-related business processes.

1.5 General problem description

As described in the previous section, the growing complexity of industrial processes has led to new kind of safety-related problems. These problems concern the management and control of the safety-related business processes. Based on hazard investigation reports it appears that the basis of these accidents is very often the result of problems with communication and information exchange [Fel01], [Bel00], [Cul90]. Obviously, in the course of time, many safeguarding measures have been developed. The task of these safeguarding measures is to protect the process installations from running ‘out of control’ and to mitigate the consequences in case of such an ‘out of control’ process. It is therefore, that every time an accident occurs, the investigation focuses on why these safeguarding measures did not fulfill their intended design function. As revealed by studies on accidents which were the result of failures of control and safeguarding equipment [HSE95], [HSE97] it also appears that with regard to this type of safeguarding measures, the majority of the problems were result of management and control of the related business processes. Enhancement of management and control of the business processes related to the application of this type of safeguarding equipment is therefore required.

History shows that during the last decade control and safeguarding equipment have gone through enormous development. The introduction of computer-based technology has led to a tremendous growth of automation and flexibility but has also resulted in increasing complex applied programmable electronic systems. Following the development of automated control and safeguarding systems, new safety standards [ISA96], [IEC61508], [IEC61511], [EN50126] are written concerning the specification, design, realization, and operation of these systems. One of the remarkable aspects of these new standards is the

definition of safety lifecycle models. Figure 2 shows as an example the Overall safety lifecycle of standard IEC 61508.

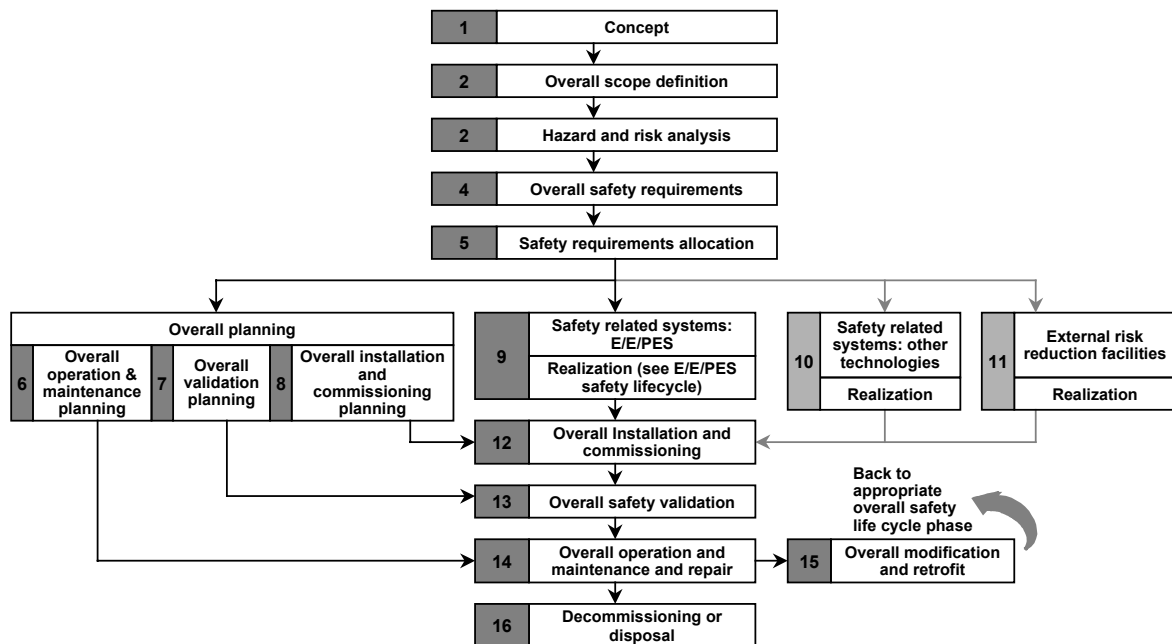


Figure 2 IEC 61508 Part 1, Overall safety lifecycle (see also Figure 7)

Each lifecycle consists of a number of phases, and for each phase specific requirements are defined in order to reduce potential risks for that particular moment in the lifetime. A second remarkable aspect of these standards is the requirement that, in order to comply with the standard, a lifecycle shall be implemented into the safety management system. Although it is not required to exactly adopt the lifecycle as defined by the standard, it is nevertheless required to allocate the safety measures to specific phases and, therefore, to a dedicated lifecycle. For instance IEC 61508 demands that the required safety-related information is operational (available) at the relevant stages of the safety lifecycle of the safety system. The standard, however, contains no requirements on how information distribution should be realized. Safety lifecycle models will be discussed in a more detailed level in Chapter 4.

2 Research objective, scope, and methodology

Based on the recently observed type of problems with regard to safety in the process industries, as described in the previous chapter, it is expected that new enhancements of the management and control of the safety-related business processes are highly needed. The objective of this thesis is to focus on a particular aspect of recent developments, namely the definition of safety lifecycle models in standards on control and safeguarding equipment. The question that arises is how these safety lifecycle models can contribute to a better control of safety-related business processes. With regard to this, the problem to be researched will be further specified and subsequently, the research questions, objective and scope will be defined. Furthermore, this chapter will describe and discuss the characteristics and justification of the research methodology used in this thesis. Finally an overview of the research program and its main steps will be given.

2.1 Research specification and scope

2.1.1 Research specification

It is currently observed that there is a growing need in the process industry to gain insight into the significant aspects and parameters to apply safety lifecycle models and to enable the process industry to operate in a more reliable and safer manner. It is generally expected that in the near future the process industry will switch to an approach where pure and only certification of the safeguarding instrumentation is not enough to ensure safety. Instead, a more integral view of process safety will lead to more validation and certification of the entire life cycle of the technical process installation, plant, and organization.

In order to use safety lifecycle models, companies have to specify a safety lifecycle model, implement the model into their organization, and utilize this model. It appears that companies are currently struggling with a number of problems related to the implementation and operation of safety lifecycle models. Often heard questions in the process industry are:

- How can a safety lifecycle be defined?
- What are the boundaries of the safety lifecycle?
- How can a safety lifecycle be implemented?
- What are the criteria for proper application of the safety lifecycle?
- How can proper implementation be verified?

These currently observed questions and problems in the process industry have resulted in the definition of four research questions. These questions are the following:

— Research question 1

The fact that the majority of recently published standards have adopted lifecycle models and the fact that these standards are developed by technical committees represented by the leading experts in their field, leads to the presupposition that these models are correctly defined. Therefore, the correctness of the lifecycle models as

defined in safety standards will not be further disputed. Upon this, it is questioned whether and how these lifecycle models can be used to improve safety-related business processes as comprised by these models.

— *Research question 2*

Basically, safety lifecycle models could be considered as being nothing more than a phasing of the life span of a safety system. From this point of view safety lifecycle models could be considered as a kind of ‘hollow’ structure, that only indicates the logic order of the safety system’s lifecycle phases. Therefore, it is questioned what exactly is phased (what is included in each phase), and if there are factors that determine the quality of what is included in each phase.

— *Research question 3*

Based on research question 2, it is subsequently questioned 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 consecutive phase. As it is already discussed in the previous chapter, it appears that many accidents are the result of problems with communication and information management. It is therefore questioned how the quality of information exchange between lifecycle phases could be controlled.

— *Research question 4*

The first three research questions concern how safety lifecycle models can support the management and control of process safety by controlling and preventing safety-related business process problems. The answer to these questions is expected to result in the development of models that indicate the relationship between the most relevant control aspects and parameters. A subsequent fourth question that arises concerns the manner how to measure these aspects and parameters in order to get to know whether these parameters need to be adapted.

In general this study carried out as a Ph.D. project, aims at setting forth a design how safety lifecycle models can be used to enhance process safety management. The design will on one hand focus on implementation concepts and on the other hand focus on the development of techniques that can measure the degree to which these concepts are implemented. Particularly, recently developed reliability-related information management techniques will be explored. It will be established whether and how these techniques can be applied for management and control of safety-related information. Insights gained from comparable research projects in the area of reliability management will be utilized.

2.1.2 Research scope

The research will particularly focus on the application of safety-instrumented systems and discusses the complete lifecycle of those systems from concept definition until disposal of such a system. The following aspects further discuss the reason to focus on safety-instrumented systems and define the research scope:

- *Control of safety*

The use of lifecycle models is not necessarily restricted to the safe control of people. For instance, other standards concerning the control of quality or the environment have also adopted lifecycle models into the applicable standards, such as the ISO 9000 series for quality control [ISO9000] and the ISO 14000 series concerning environmental pollution [EN14000].

To effectively implement requirements regarding safety and other standards, such as product quality and environmental pollution, it might be impractical to maintain separate control systems for all of these aspects. A single control system, which is able to harmonize the specific requirements of the different standards, might be preferred to prevent inconsistency.

Lifecycles are considered to serve as a structure and a framework towards this integrated approach. The expectation is that future standards can be relatively easily adopted and implemented in the existing lifecycle model- based control system.

- *Safety-instrumented systems*

Safety standards, such as IEC 61508, IEC 61511 and ANSI/ISA S84.01, are typical examples of standards that are characterized by the definition of safety lifecycle models. For instance, IEC 61508 contains the most detailed and extensive lifecycle models. For the reason that the previously discussed safety standards are initially developed for the application of safety-instrumented systems, the scope of the research will especially concentrate on the application of safety lifecycle models related to this type of safeguarding measures. Chapter 3 will further discuss the definition of a safety-instrumented system.

- *Process industry*

The process industry is one of the largest industrial sectors where safety-instrumented systems are applied. Not surprisingly, the process industry is currently working on the development of a sector-specific standard concerning the application of a SIS, namely IEC 61511. The author has visited many companies in the process industry and extensively discussed with those companies how this new lifecycle model-based safety standard could be best implemented. Therefore the research focuses particularly on the process industry sector. However, it is the expectation that concepts and models that are described in this thesis can be generalized and also applied to other sectors in industry.

- *Safety-related business processes*

Obviously, the implementation of a safety lifecycle model is not the final objective itself, but rather a means to better control the safety of people and the environment. A safety lifecycle model is expected to structure safety-related activities and the safety-related business processes. Particularly, the interaction and influences between consecutive lifecycle phases will be considered. The impact on the quality of the safety performance as the result of inadequate interfaces between activities and phases, i.e. related business process problems, is one of the basic attention points in this research.

Finally, since the determination of the required risk reduction to be achieved by a SIS depends on the achieved risk reduction of other safeguarding measures, the risk assessment and allocation of the safety requirements to the SIS can not be adequately analyzed without considering other safety measures. Therefore, the scope of this thesis will not be strictly limited to the above-described points. The various case studies described in this thesis will illustrate this.

2.2 Research type and methodology

2.2.1 Research in the area of industrial management

This section will discuss some aspects of the type of research and the applied methodology.

The observed kind of problems in the process industries concerning the application of safety instrumented systems are predominantly related to business process problems. Controlling safety-related business process problems clearly implicated that the research area concerns industrial management. A first question that should be answered is what exactly is industrial management and what is scientific research in this area? According to Veerman and Essers, industrial management is a scientific approach of problems which are related to (inter-) human thinking and acting, as is aimed at societal producing in organizational context; an approach that strives for an as strong as possible integration of the aspect-aimed points of view of fields of disciplines, with the aim to generate a more adequate solution for a problem than would have been possible on the basis of a pure mono-disciplinary point of view [Vee88]. Scientific research in the area of industrial management could therefore be considered as a kind of mixture of disciplines, whereas fundamental research developments are subsequently applied in the industries [Vee88]. As such scientific research in the area of industrial management could be qualified as applied science. As will be discussed in the next section, this type of research is often named design science.

2.2.2 Research typification

— Research types

In general it could be said that research goes beyond description and requires analysis. It looks for explanations, relationships, comparisons, predictions, generalizations and theories [Phi87]. Various literature on how to do scientific research, illustrates many different kinds of qualification and categorization of research types [Moo83], [Phi87], [Ake99], [Sol99]. For instance, Phillips and Pugh discern the following basic types of research, namely, distinction pure and applied, exploratory, testing-out and problem solving. Van Aken [Ake99] distinguishes three categories of scientific research, namely:

1. Formal sciences, such as philosophy and mathematics.
2. Explanatory sciences such as the natural sciences and major sections of the social sciences.
3. Design sciences, such as the engineering sciences, medical science, and modern psychotherapy.

The mission of a design science is to develop knowledge to be used in the design and realization of artifacts, such as solving construction problems, or the improvement of

existing entities, such as solving improvement problems [Ake99]. Based on the described problem area and the defined research objective, this research project will consist of what is called ‘positivist design research’ [Ake99], as opposed to causal and formal science based on theoretical and formal constructions of the solution of the problem, respectively. Another classification of this research project concerns a kind of research called applied research, which can be described as ‘interfering in practice and attempting to solve practical problems by designing theoretically sound solutions’ [Sol99]. As opposed to this, another type of research called *theoretical research* describes instead a generic theory by observing specific phenomena [Sol99].

This thesis will not further discuss the various types of research methods and strategies, but will instead discuss the design science type of research in more detail. This kind of research is considered to be best representative for the kind of research that is described and applied in this thesis.

— *Design science*

This ‘design science’ research type is intended to design and develop a model that initially explains and then solves a problem. The solution is intended to be expressed in the form of a prescription, meaning that the solution will be expressed as ‘an instruction to perform a finite number of acts in a given order and within a given aim’ [Ake99]. Prescription-driven research is solution-focused, rather than problem-focused. Of course, the problem should be analyzed, but the emphasis of the analysis is on those aspects which determine the choice and effectiveness of the solution. ‘The so-called technological rules or design prescriptions are based on both scientific-theoretical knowledge as well as tested rules (rule effectiveness systematically tested within the context of its intended use)’ [Ake99]. ‘A tested technological rule is one whose effectiveness has been systematically tested within the context of its intended use. Grounding a technological rule on explanatory laws does not necessarily mean that every aspect of it (and of its relations with the context) is understood. Typically, several aspects keep their “black box” character, but under certain conditions specific interventions give the desired results. Testing within the context is necessary to account for its effectiveness’ [Ake99]. With regard to process safety, the improvement of the safety level depends on many aspects which are related to social-technical and psycho-technical elements. Therefore, the influence of a particular aspect will be difficult to demonstrate. Furthermore, the demonstration and explanation might be difficult and complex because its influence might be related to the other aspects. Grounded and tested technological rules are therefore expected to be typical deliverables of this research.

2.2.3 Research methodology

According to Nagel [Nag79], most academic research in management is based on the paradigm that the mission of all science is to understand, i.e. to describe, explain and possibly predict. Subsequent question is which tools and methods could be best used to describe, explain and predict, and how to collect the necessary information. Moore recognizes the following research methods [Moo83]:

- | | |
|-----------------------|---|
| — Interviews | — Operational research |
| — Questionnaires | — Case studies |
| — Sampling | — Evaluation and performance management |
| — Experiments | — Action research |
| — Historical research | |

Based on the exploration and analysis of the problem, a theoretical solution will have to be defined. Due to the nature of the problem description and problem area, it is presupposed that case studies are the best way to validate the theoretical solution. According to Moore however, case studies provide the framework within which other methods are employed for specific purposes [Moo83]. As will be illustrated e.g. in the second case (see Chapter 8), where interviews are performed in order to collect the required information.

A logic question that arises is ‘what is a case study?’. Yin [Yin94] defines a case study as *‘an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident’*. Also according to Yin case study is but one of several ways of doing scientific research. Other ways include experiments, surveys, histories, and the analysis of archival information. In general, case studies are the preferred strategy when ‘how’ or ‘why’ questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context.

According to Moore [Moo83], case studies are chosen not because they are representative of all authorities, but on the grounds that they would shed some light on the general trends while at the same time being sufficiently comparable so as to provide a basis for generalization. Case studies are usually used when the research is attempting to understand complex organization problems, or the diffuse causes and effects of change. In essence it allows the researcher to focus on something which is sufficiently manageable to be understood in all its complexity.

An advantage of case studies is the fact that they provide a means of looking in some depth at complex problems. By using case studies it is possible to compare a number of different approaches to a problem in sufficient detail as to be able to draw out lessons which have general applicability. A disadvantage is that case studies lack the statistical validity of samples which have been properly sampled, and therefore the extent to which valid generalizations can be made depends on the degree to which the case studies themselves are typical and the care used in drawing conclusions [Moo83].

Judgment of the quality of the validation based on case studies is considered to be arbitrary and subjective. Yin [Yin94] suggests that ‘case studies should be selected with ‘theoretical replication’, and contradicting results are allowed under both stated reasons and by having predicted results’. According to Dapena [Dap01], ‘this can construct the generality for a wider scope of cases, thus expanding the domain for which the results are valid. When selecting the case studies, an attempt must be made to cover the problem domain as best as possible making explicit individual differences expected from the case studies’. According to Moore [Moo83], case studies should be selected to be broadly representative of the large group from which they are drawn, as much will depend on the degree to which it is possible to generalize from the particular results. During this research project specific case studies were carried out at various chemical and petrochemical companies. Furthermore, a number of cases were described based on the observation done and experiences gained during the many site visits and discussions with companies and organizations in the process industries. (See Chapter 8 and annex A, describing a total of 11 case studies conducted at different companies in the process industries that make use of safety instrumented systems.) The substantial number and wide variety of the described cases concerning their application areas were deemed to strengthen the validity of the theoretical solution. Based on the case materials and study results, the defined theoretical concept solution was further extended with guidelines on how to implement the theoretical concepts in practice.

2.3 Research program

The research started with an exploration of the problem area and the current state-of-the-art methodologies and techniques that were used to handle this problem area. Subsequently, it was established that this research followed the typical approach as defined by [Ake99] concerning ‘design science’. This type of research is characterized by the following cycle; problem analysis, definition of a solution choosing a theoretical case, planning and implementing practical cases (on the basis of the problem solving cycle), comparing the results to the theory and, finally, testing and refining the theory in subsequent practical cases [Dap01]. The main activities carried out in this research project are presented in Table 1:

Table 1 Main steps of the research project

Problem definition	
1.	Definition of the problem, and focus of the research scope and objective.
Problem analysis	
2.	Survey of existing literature and standards.
3.	Analysis of the problem, illustrated by practical cases, and analysis of current state-of-the-art of solutions, based on a reference criteria framework.
Solution design	
4.	(Theoretical) construction of models and parameters, which describe the utilization process of safety lifecycle models as a means to control safety-related business processes.
5.	(Theoretical) construction of a methodology in order to measure the degree to which the control models and parameters are implemented.
Solution validation	
6.	Empirical validation and verification of the methodology and guidelines of their practical use in industrial case studies.
7.	The validity involved in applying the methodology in practice.
Evaluation and feedback	
8.	Refinements and enhancements of the models and methodology.
9.	Verification of the developed solution in order to check whether the research questions are completely and correctly answered and the research objective is achieved.

Each of the main research steps of Table 1 are discussed in further detailed below:

2.3.1 Definition of the problem, and focus of the research scope and objective

An overview of the observed problem area, which resulted in the problem definition and a formal specification of the research objective and scope, has been defined in chapters 1 and in sections 1 and 2 of this chapter. Furthermore, the various industrial cases described throughout this thesis will illustrate the typical characteristics of the problem area. Particularly is referred to Annex A which describes 9 case studies carried out at different companies. Each case study starts with an introduction and a problem description.

2.3.2 Survey of existing literature and standards

Current standards and legislation will be thoroughly scrutinized together with an analysis of the methods and techniques described in literature to gain a clear understanding of the current state-of-the-art practices. Particularly, the field of process safety management will be explored and analyzed. In Chapter 4, safety legislation and standards concerning the latest safety-instrumented systems, which have included safety lifecycle models, will be analyzed in detail. Subsequently, Chapter 5 will in detail discuss the current ‘state of the art’ aspects of process safety management. Furthermore, in Chapter 5, the latest developments in the area of reliability information management and techniques that are applied will be discussed in order to determine their applicability in the area of safety management.

2.3.3 Solution design

The solution design will be split into two phases. Firstly, models and criteria will be developed which describe the most relevant aspects and parameters on how to utilize safety lifecycle models. As a result of this, an algorithm will be defined which describes a stepwise implementation route that results in a full implementation of a safety lifecycle model.

The second phase concerns the development of a methodology to analyze a company or organization and measure to which degree the safety-related business processes are correctly implemented. This (theoretical) methodology will be tested in practice on a number of industrial case studies, and the experiences gained during earlier case studies are accordingly implemented in order to complete and refine the methodology. (As will be described in Chapter 7, this has resulted in the development of a formalized analysis technique.)

2.3.4 Solution validation

Accidents in the process industry are characterized by a relatively low probability of occurrence, but may result in enormous consequences. Unfortunately, a statistical and accurate prediction of the number of future accidents within an organization is hardly possible. Deterministically, the total number of real accidents based on the installation life span is relatively small. Therefore it is nearly impossible to determine the probability of such accidents within an acceptable accurate confidence interval. Validation of the added value of each single safety measure with regard to its contribution to the final achievable safety level based on measurement of a reduction of the number of accidents is therefore considered to be not meaningful.

As a consequence of the difficulties and disadvantages of measuring the final safety performance (accident rate), special attention and effort must be paid to the measurement of relevant safety-related input parameters that affect the output parameter, or the accident rate. In order to analyze the added value of the application of safety lifecycles, the most relevant safety-related performance indicators need to be allocated and defined [Kap92], [Ker98].

As discussed in Section 2.2, case studies will be carried out at different companies in the process industry to validate the correctness and added value of the designed solution. This research program could therefore be expressed as being empirical [Yin94]. Furthermore,

throughout this thesis industrial experiences are described to illustrate the applicability and validity of the designed solution.

In order to closely measure results and gain maximum benefits, a close contact with the actual process industry is thus required. Finally, experiences obtained from the predefined industrial cases are expected to offer a new and better understanding and knowledge of the application of safety lifecycles and a contribution to an increased safety level in the industry.

2.3.5 Evaluation and feedback

Conclusions on the effectiveness and efficiency of the designed solution together with the observed added value of the utilization of safety lifecycle models will be discussed following the case studies. Refinements and enhancements of the initial concepts will be discussed based on these conclusions. Finally, a verification of the developed solution will be done in order to check whether the research questions are completely and correctly answered and the research objective is achieved.

2.4 Research expectation

As discussed in Chapter 1, the typical safety problems that the process industry is currently struggling with are particularly the result of the growing complexity of safety systems and organizations. In order to deal with these typical so-called ‘business process problems’ requires more clarity and understanding of these safety-related business processes. The adoption of lifecycle models in safety standards has led to the expectation that these models might serve a structure for these business processes. Therefore, it is expected that using these lifecycle models indeed do offer the highly needed clarity and understanding. With regard to correct implementation of a safety lifecycle model into the safety management systems, it is the expectation that relational parameters will need to be identified, which subsequently will result in additional and new safety management models.

In order to verify whether an organization has correctly implemented the safety management models, as described in Section 2.3, it will be required to develop a methodology to observe and solve the typical safety-related business process problems. It is expected that the measurement method, that needs to be developed, will be able to identify and allocate these problems and in combination with the new safety management models will enable the process of finding the necessary solutions.

2.5 Outline of this thesis

In this chapter an outline is given of the research scope and objective, the research methodology and research program.

The next chapter will give an overview of safety-instrumented systems, as a typical risk reduction measure, to protect process installations. It describes a safety-instrumented system as a specific layer of protection for process installations.

In Chapter 4 an overview will be given of current process safety legislation, and the recent standards on safety-instrumented systems. It involves safety standards that have defined lifecycle models.

Chapter 5 discusses existing techniques to control safety-related business processes as part of process safety management activities. Because of the observation in Chapter 1 that business process-related safety problems are the result of problems with management and control of the safety-related information, developments in the parallel field of reliability information management will be reviewed. Particularly attention will be paid to methodologies and techniques on the control, measurement and qualification reliability-related information flows.

In Chapter 6 the solution design will be described, which has resulted in the definition of the safety lifecycle management concept.

Chapter 7 describes the development of the MIR-based SLM analysis technique, which can be used to observe safety-related problems and analyze the quality of the control of safety-related information flows. This technique is intended to be used as a new additional means to assess safety management systems regarding the management and control of safety-related information.

In Chapter 8 two industrial case studies are described, of which the experiences are used to complete and refine the formalized MIR-based SLM analysis technique.

Finally, Chapter 9 summarizes and evaluates the conclusions and lists recommendations for further research.

3 Safety-instrumented Systems

This chapter will give an overview of safety-instrumented systems as a specific risk reduction measure. An acceptable safe operating process installation can only be achieved if all the applied risk reduction measures are adequate and controlled. The techniques to realize and control the risk reduction as achieved by the SIS, are expected to be also applicable to other risk reduction measures.

3.1 Layers of Protection

Obviously, the best strategy to prevent the occurrence of hazardous events is to design a process installation which is inherently safe. However, certain chemical reactions only take place dangerous at high pressures, temperatures, etc. Furthermore, some processes are comprised of hazardous substances which can be flammable, explosive, and/or toxic. Unfortunately, process installations, that are inherently safe designed, are not always justifiable. For example, the construction of a tank wall with a meter thick steel is normally not economically cost-effective. Therefore, in parallel with the development of technical process installations, a large variety of safeguarding measures have been developed. The combination of safeguarding measures is considered to result in a 'safe' operating installation. A 'safe' installation could thus be defined as the situation in which all risks are reduced to an acceptable level. Obviously, clear and unambiguous criteria need to be defined with regard to acceptable risk levels. The safeguarding measures can be categorized, and each category can be defined as a specific dedicated layer of protection. For example, to protect a particular unit of a process installation against over-pressure, the safety measures might consist of a first safety layer comprising a pressure transmitter, logic solver and actuator and a second layer of protection comprising a pressure relief valve. Both layers of protection form so-called Safety-Related Systems (SRS). The first layer of protection concerns an electric/electronic/programmable electronic SRS. This system will, in line with IEC 61511, from now on be named a Safety-Instrumented System or SIS. The second layer is typically a so-called mechanical SRS.

Figure 3 shows the concept of layers of protection and the compositions of the different types of safety-related systems, as defined in part 1 of IEC 61511. It must be noted that a clear distinction exists between the Basic Process Control System (BPCS) and the safety-instrumented systems as part of the Prevention and Mitigation layers. The primary objective of a BPCS is to optimize the process conditions in order to maximize the production capacity and quality. Safety-instrumented systems are primarily applied to prevent hazardous events from occurring (Prevention layer), and mitigation of the consequences of hazardous event (Mitigation layer). The motive for this distinction is due to the fact that a BPCS does not necessarily have to contribute to the risk reduction and sometimes might even pose a potential risk itself. (As explained, the relief valve, as mentioned in the previous example, obviously is a Mechanical Mitigation System as indicated in Figure 3.)

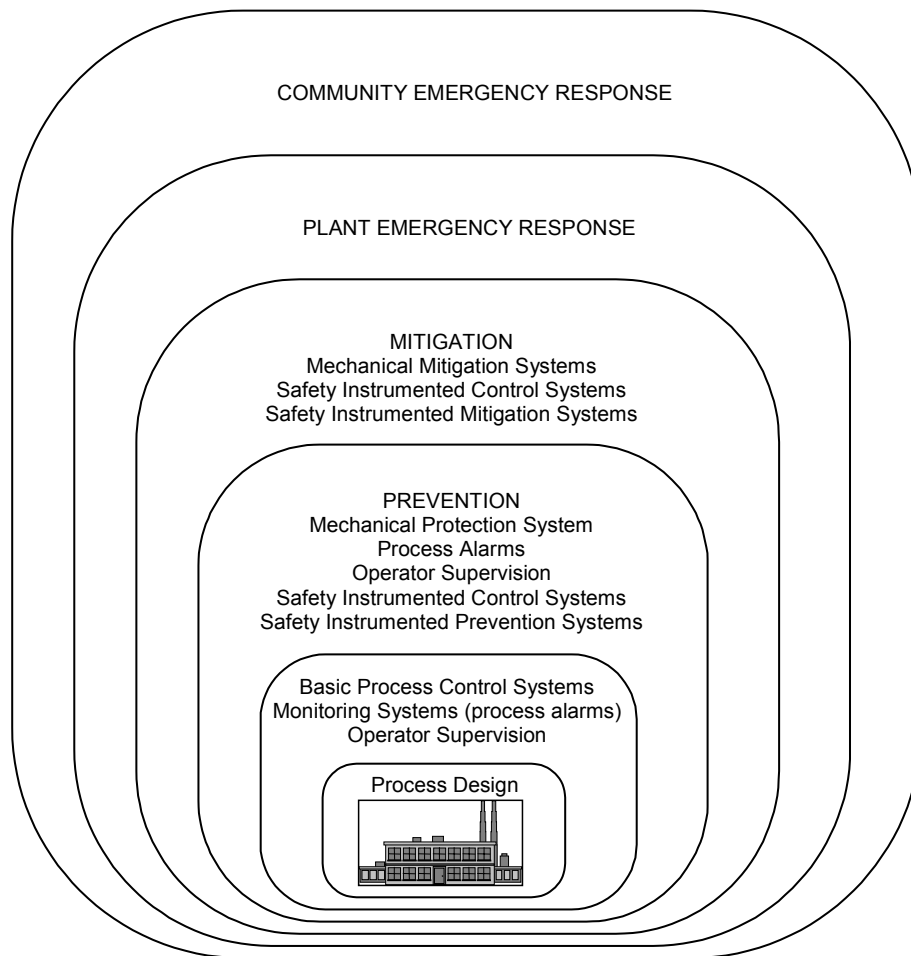


Figure 3 Concept of layers of protection [IEC61511-1]

3.2 Definition of a Safety-instrumented System

Standards like IEC 61508, IEC 61511, and ANSI/ISA S84.01 concentrate on the *functional* safety of the safety-related- or safety-instrumented system. Functional safety is defined by IEC 61508 as the ‘*part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities*’. All combined instrumentation, devices, and equipment that are required to fulfill an intended safeguarding function are considered to be part of the safety-instrumented system (see Figure 4). For the reason that the collection of safety instrumentation normally includes more than one safeguarding function (e.g. protect against over-pressure, temperature protection, flow control, etc.), the SIS could be defined as the collection of all safety-related sensing elements, all safety-related logic solvers and all safety-related actuators. On the other hand, the SIS could also be considered as per each safeguarding function separately. Based on the second definition, the SIS would comprise only the devices to protect the Equipment Under Control (EUC) against one single hazard. Consequently, the process installation would be comprised of a number of safety-instrumented systems. Because particular devices such as safety-related PLCs and shut-off valves deal with more than one Safety Instrumented Function (SIF), this thesis uses the

first definition, considering the SIS to be comprised of *all* safety-related devices of the subject process installation.



Figure 4 Safety-instrumented System

Figure 5 illustrates the definition of a safety-instrumented system and the safety-instrumented functions that are executed. This figure illustrates a safety-instrumented function that protects the process temperature and causes a shut-off valve to close in case of an out-of-control process temperature. Other safety-instrumented functions that are performed by the example SIS are the level protection and the flow protection.

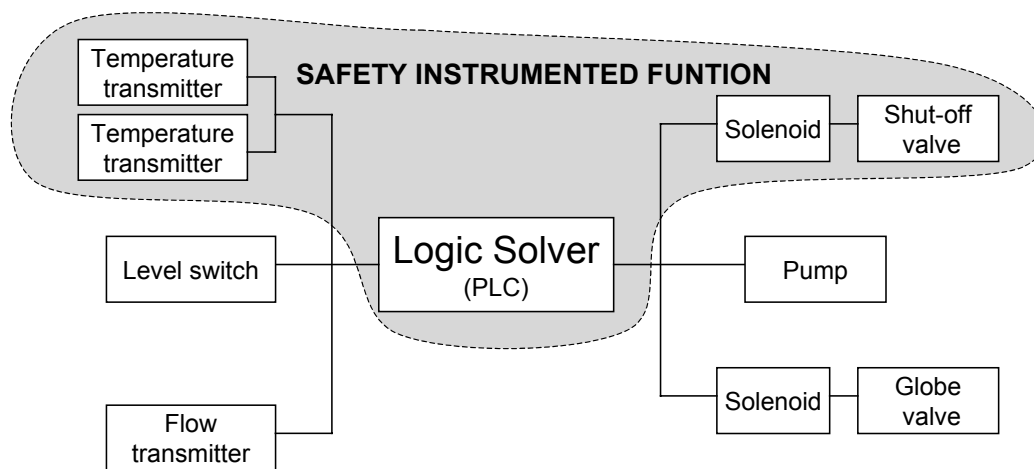


Figure 5 Safety-instrumented Function

3.3 Safety Integrity Levels

Once the required level of risk reduction to be achieved by the SIS is established, often expressed as the Risk Reduction Factor (RRF), this level or factor can be translated into the required Safety integrity Level (SIL). Each SIL represents a maximum allowed probability of failure on demand of the SIS. To comply with the requirements of a specific SIL, a number of qualitative requirements need to be implemented and a quantitative reliability analysis shall prove that the maximum Probability of Failure on Demand (PFD) is not exceeded [Kne98a], [Kne98b], [Kne99b]. Table 2 shows the relationship between the;

- Safety integrity level.
- The required availability of the safety-instrumented function.
- Probability of failure of the SIS on demand.
- Equivalent risk reduction factor.

Table 2 PFD requirements per SIL

SIL	Probability of failure on demand
1	$10^{-2} - 10^{-1}$
2	$10^{-3} - 10^{-2}$
3	$10^{-4} - 10^{-3}$
4	$10^{-5} - 10^{-4}$

Standards like IEC 61508, IEC 61511, and ANSI/ISA S84.01 require that a validation is carried out on the realized SIS, in order to determine that the required SIL is achieved for each SIF. Among other things, this validation consists of a check whether the functional safety requirements are met (a kind of qualitative validation), and a reliability calculation of the SIS (quantitative validation). Because the PFD is not a constant in time, the calculation shall be done for a predefined period of time. (For instance, for the expected operational lifetime of the considered SIS.) Therefore, the PFD is often expressed as an average probability.

To calculate the SIL of a safety function it is required that the complete ‘chain’ of instrumentation, necessary to perform the required safeguarding function, from sensor up to actuator is considered. Therefore, it is not sufficient to only analyze one section of the control process, such as the logic solver, and determine the realized SIL. Nevertheless, the logic solver still can be validated by calculation of its average probability of failure on demand. The calculated value indicates the contribution of the PFD of the logic solver (assuming independency of sensors, logic solver and actuators) to the complete SIF and it can, within certain assumptions, be established that the typical logic solver configuration is suitable for applications where a specific SIL is required.

3.4 Typical problems of safety-instrumented systems

In the early part of the eighties of the last century, computer-based programmable electronic systems entered the process industry. At first, general purpose PLC’s (Programmable Logic Controllers) were used to control process safety. Later on, dedicated safety PLC’s were developed. A study performed by the British Health and Safety Executive (HSE) illustrated the origin of a number of control systems failures leading to serious hazardous events in the UK [HSE95]. Figure 6 shows the primary causes of control system failures based on this study.

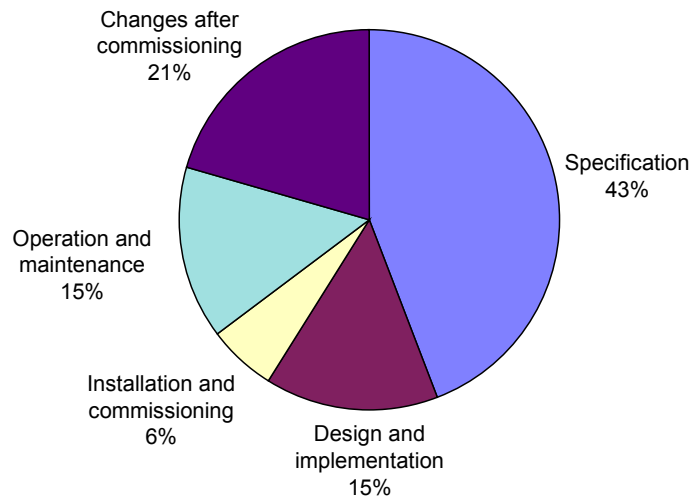


Figure 6 Primary causes of control system failures [HSE95]

The HSE determined that failures of control systems were not just the result of incorrect operation. In fact, failures were initiated throughout the various stages of the system's lifetime, as shown in Figure 1. Remarkably, 44.1% of all failures were the result of incorrect specifications.

Shell International Oil Products B.V. performed another illustrating study at the national LNG plant in Oman Middle East, which is partly owned by Shell [She98]. The complete production process was comprised of field recovery systems, a central processing plant, and a liquefaction complex. During a SIL-based safety study, it was concluded that;

- 67% of the SIF's appeared to be overprotected.
- 27% required no change.
- 6% of the SIF's appeared to be under protected.

Shell performed a number of these studies at different sites which represented comparable results.

The key question is what the underlying reasons for these safety problems, related to SIS failures, are. Presumably, failures could have been made during the risk assessment and specification of the safety requirements; failures could also have been made during the design and implementation of the SIS, or during the validation. In general, after reviewing the HSE study and the Shell LNG plant study, failures were concluded to be initiated at several different stages of the lifecycle.

As discussed in Chapter 2, to guarantee safe operation of the process installation during its entire lifetime, a mechanism should be in place that manages and controls the safeguarding measures. Safety-instrumented systems are probably one of the most important risk reduction measures. If a control mechanism can be specified that is able to properly manage the risk reduction as realized by the SIS, it can be assumed that the concepts of this control mechanism could also be applied to the other risk reduction measures. Ultimately, the application of such a mechanism should achieve and maintain a safe operating plant or process installation.

The following chapter will give an overview of legislation and standards on SIS.

4 SIS-related legislation, standards and lifecycle models

This chapter gives an overview of legislation and the relationship with SIS-related standards. Furthermore an overview is given of the latest developments of SIS-related standards, and typical aspects, namely safety lifecycle models, that are included in these standards.

4.1 Legislation on process safety

The goal of standards, codes, and regulations is to communicate the intentions of companies regarding minimum acceptable safe practice, and to assure that all operating locations within the company share a common approach to process safety [CCPS89]. Clear and unambiguous requirements of standards, codes, and guidelines need to be followed, so that everyone involved clearly knows which requirements apply. A variance procedure should be established to handle instances where specific local conditions necessitate deviation from accepted standards [CCPS89]. In some cases, operating or engineering personnel may wish to meet the objectives of a code or standard in a way other than that specified by that code or standard. Where this is an attractive option, the location seeking to use alternative approaches should be required to demonstrate that their approach is at least as safe as the applicable code or standard already specified [CCPS89].

The following sections will deal with legislation and standards in the United States and in the European Union, and the relationship between them.

4.1.1 OSHA 1910.119

The American Occupational Health Administration, which represents the American law, has defined a Code of Federal Regulation (CFR), namely the Occupational Safety & Health Administration (Standards – 29 CFR), containing a clause Process safety management of highly hazardous chemicals. – 1910.119 [OSHA 1910], concerning process safety management of highly hazardous chemicals. The regulation contains requirements for preventing or minimizing the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals. Such releases may result in fire, toxic- or explosive hazards. This regulation contains requirements on the management of process safety. Within this clause, the following aspects are considered:

- Process safety information
- Documentation
- Process hazard analysis
- Operating procedures
- Training
- Compliance audits
- Responsibilities
- Inspection and testing
- Quality assurance
- Management of change
- Incident investigation

4.1.2 Council Directive EU 96/082/EEC (Seveso II Directive)

Council Directive 96/82/EC of December 9, 1996 [EC96], deals with the control of major accidents involving hazardous substances. In practice, this directive is better known as the Seveso II directive, named after the 1976 disaster in Seveso, Italy. The aim of this

directive is preventing major accidents which involve dangerous substances, as well as mitigating the harmful consequences of these types of accidents for people and the environment, with a view to ensuring high levels of protection in a consistent and effective manner.

Council Directive 96/82/EC Article 1, Aim

'The directive is aimed at the prevention of major accidents which involve dangerous substances, and the limitation of their consequences for man and environment, with a view to ensuring high levels of protection throughout the Community in a consistent and effective manner.'

The operators of companies for which the Seveso directive is applicable shall take preventive measures against severe accidents and reduce the consequences for persons. At all times, the company shall be able to prove to the supervising authorities that they have taken care of:

- Determining existing risks of possible severe accidents.
- Taking appropriate measures.
- Safety-related information, training and equipment for the employees.

Roughly postulated, the following aspects need to be considered to comply with the Seveso II directive:

- What are the potential hazardous events and their associated risks, and what level of risk reduction is necessary to achieve an acceptably safe operating process installation?
- How can it be established and confirmed that the safeguarding measures and equipment indeed realize the required risk reduction?
- What activities need to be carried out to guarantee that an acceptable residual risk level is maintained during the entire lifetime of the process installation?
- Set up and administer appropriate documentation, which serves as evidence that the above mentioned points are adequately implemented.

4.2 Relationship between legislation and standards

Most countries have a law that protects their inhabitants from personal harm by forcing new plants, installations, equipment, tools, etc. to have a safety level that is at least at the level of the generally accepted technical level (good engineering practice). The generally accepted technical level is published in publicly accessible documents like magazines, official governmental publications, laws, (European) directives and in standards. In case of incidents, it has to be proven that measures had been taken to assure that the safety level was at least at the generally accepted technical level.

Since March 2000, OSHA has recognized the American ANSI/ISA S84.01 standard to be good engineering practice for the implementation of safety-instrumented systems. If companies document, as per OSHA regulation 1910.119, that they comply with ANSI/ISA S84.01 for SIS, and meet all ANSI/ISA S84.01 and other OSHA Process Safety Management (PSM) requirements related to SIS, the company will in that case be considered to be in compliance with OSHA PSM requirements for SIS.

The so-called ‘new-approach’ EU directives define the *essential requirements* that must be met before products may be sold anywhere in the countries of the European Union. The requirements are written in rather general terms. Appropriate application of harmonized EU standards gives the ‘suspicion of compliance’ with the specific directive (the standards themselves are not mandatory). Relevant EU standards are therefore added to the reference lists of the considered directives.

The seven parts of IEC 61508 were ratified by the CENELEC Technical Board in July 2001, so this standard will be published as EN 61508 by August 2002. The EN 61508 is currently not linked to any EC directive.

4.3 New developments of safety standards

Since the early sixties of the last century, the process industry passed through a tremendous growth and development. As a result of an increasing number of accidents and until that period of unknown accidents, the development and publication of standards and good engineering practices started. The first standards strongly focused on technical issues and requirements concerning the involved process installations and all kinds of technical protection equipment. Based on occurred accidents, the technical weaknesses of the designs were reduced by adding new technical requirements. During the eighties of the last century, it became apparent that many accidents still occurred and that the root causes of these accidents were hardly the result of technical failures but much more the consequence of inadequate organizational issues concerning the application of technical safeguarding equipment [HSE95]. This awareness resulted in the development of so-called performance based standards that do not anymore focus on detailed technical requirements, but rather focus on functionality, effectiveness, and efficiency of safeguarding measures. The CCPS however concluded that the application of performance-based standards also has negative side effects, compared with specification standards:

Many companies incline towards performance standards for process safety that identify only the desired result, rather than specification standards that stipulate both the results and the steps that must be taken to achieve that result. While it may be stifling to have overly specific process safety standards, accountability is more difficult to achieve with performance standards than with specification standards [CCPS89].

This was probably concluded based on the fact that performance standards are less specific and less concrete than specification standards. This leads to the idea that the performance-based standards are often more vague and subject to different interpretations.

The following sections will discuss the latest standards on safety-instrumented systems, their concepts and their impact in the industry.

4.4 Recent standards on safety-instrumented systems

In 1984, the IEC Technical Committee 65 began the task of defining a new international safety standard, which was intended to serve as a safety umbrella for all kinds of failures that might be caused by safeguarding instrumentation. This standard, IEC 61508 [IEC61508], focuses on the minimization of systematic failures which can occur in

electric/electronic/programmable electronic safety-related systems (E/E/PE-SRS). The safety standard IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE-SRS), is applicable for the industrial sector of manufacturers, system integrators, and end-users of electric/electronic programmable safeguarding equipment. The standard aims to supply proper specification of safety requirements, design and development, installation, and operation of an E/E/PE-SRS. However, to properly specify safety requirements, the hazard and risk analysis must be taken into account. As a result, IEC 61508 has been extended and contains requirements for various new aspects, including concept and overall scope definition, hazard and risk analysis, and allocation of safety requirements to the various ways of improving safety.

Based on the ‘generic’ standard IEC 61508, at this moment in time, sector- and application specific standards are under development: *‘The development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc) both within application sectors and across application sectors; this will have both safety and economic benefits’* [IEC61508]. For instance for the process industries, a sector specific standard IEC 61511 [IEC61511] is recently being drafted. (See annex B for a description.) Also applications of E/E/PE-SRS for the machinery industry are currently defined. More or less in parallel with the development of IEC 61508, the Instrumentation, Systems, and Automation Society of America (ISA), developed the standard ANSI/ISA S84.01 for the application of safety-instrumented systems for the process industry. Later on, the American National Standards Institute (ANSI) recognized compliance with this standard as good engineering practice. (See annex B for a description of the standard ANSI/ISA S84.01.)

As a result of the recent publication of the new international safety standard IEC 61508, and the earlier published American safety standard ANSI/ISA S84.01, many companies have been confronted with new developments in the area of safety management. The impact on organizations is far-reaching. In addition to the technical validation of the safeguarding equipment (e.g. by calculating the reliability of the equipment), a number of organizational measures need to be taken into account as well. In order to guarantee the target SRS performance, it is important, as already mentioned, not only to make use of reliable equipment, but to make sure that the equipment is developed and operated by competent people, using appropriate methods, and supported by proper management.

4.5 Safety lifecycle models

One of the typical ‘new’ requirements in IEC 61508 and sector specific standards based on IEC 61508, as well as in ANSI/ISA S84.01, is the definition of a safety lifecycle and its required implementation into the existing safety management system. Furthermore, safety-relevant documentation for all defined phases needs to be established and maintained. In this respect, it is to expect that lifecycles will play a larger and more significant role in the management of industrial safety, as well as having increased significance for quality and environmental concerns. An integral approach to the application of lifecycles as part of the management system could therefore contribute to meeting the process safety management requirements [Kne99c], [Kne99d]. This section will in further detail discuss the IEC 61508 Overall safety lifecycle. The following section provides a brief overview of the lifecycle-based safety standard IEC 61508. Appendix B gives an overview of other recently published safety lifecycle model based standards.

IEC 61508 considers the Overall, E/E/PES, and software safety lifecycle phases (e.g. from initial concept to design, implementation, operation and maintenance, up to and including decommissioning) in case an E/E/PES is used to perform safety functions. Management and technical activities that are specified in the safety lifecycle phases are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems (see Figure 7 below). Besides the Overall safety lifecycle model, IEC 61508 has also defined specific models for the realization of the E/E/PE SRS. One model describes detailed lifecycle phases of the specification, development and validation of the E/E/PE SRS. The other lifecycle model describes detailed phases for the specification, development and validation of safety-related software. These models are not further in detail discussed in this thesis.

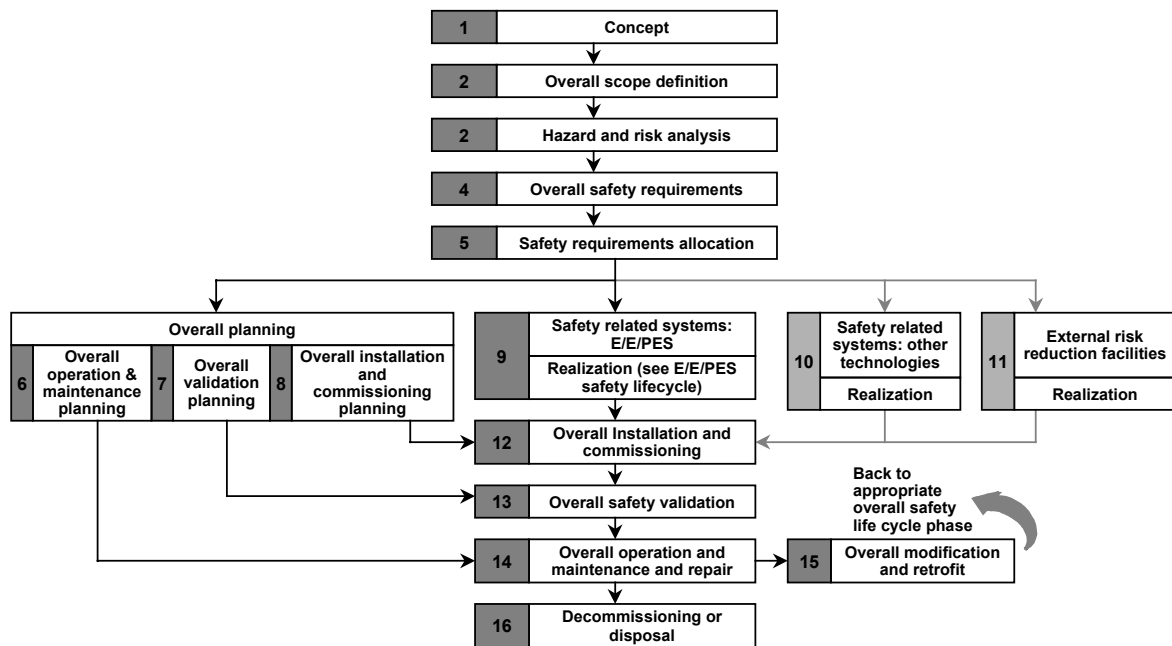


Figure 7 IEC 61508 Part 1, Overall safety lifecycle

An important requirement of IEC 61508 is that a safety lifecycle must be adopted and implemented into the safety management system. A precise definition of the sixteen phases of the Overall Safety Lifecycle is not required. A deviating safety lifecycle may be used, but must be defined with clear cross-references to the IEC 61508 Overall Safety Lifecycle.

Implementation of a lifecycle model such as the Overall safety lifecycle model from the IEC 61508 standard, questions may arise such as ‘what exactly is a safety lifecycle model and what is its purpose?’. The term lifecycle clearly implicates a certain time span. Logically, the following question is ‘time span of what?’. For a number of definitions that might help to answer these questions, is reverted to the standard itself. IEC 61508 defines a safety lifecycle as:

‘Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.’

It could be assumed that a safety lifecycle starts at the moment that safety has become an issue that needs to be further considered, until the moment that safety has been dismissed as an issue. This includes the moment that activities are started that involve safety aspects, until and including the disposal of these safety-related systems (SRS).

Obviously, a distinction can be made between the moment that safety becomes an issue and the moment that application of SRS becomes an issue. This difference is explained as follows; at the moment that an idea is created to produce a new product, the production process will be designed, the production installation will be designed and the location of the process installation will be chosen. During these steps, safety aspects need to be considered. For instance, potential hazards, that result from the process chemical reactions and process physical aspects. Subsequently, the impact and probability of occurrence of these potential hazards need to be determined considering the design of the process installation, and its location. These steps are intended to result in an, as far as possible, inherently safe operating process unit. In order to establish whether after these steps indeed an acceptable safe process unit is realized, a risk analysis needs to be carried out. Based on the outcomes of this risk analysis, it might be the conclusion that additional safeguarding measures still need to be taken.

A first observation is that the Overall safety lifecycle comprises phases during which the SRS does not yet physically exist. From this point of view, a safety lifecycle model can therefore be divided in three stages, which in a certain way also determines the scope of the lifecycle.

The first part of the lifecycle concerns the risk analysis during which the potential hazardous situations are determined, their impact and consequences are established and the probability of occurrence estimated. Consequently, the need for additional risk reduction measures is determined and the safety requirements are specified and allocated to safety-related systems.

The second part of the lifecycle concerns the technical specification, development and implementation of the safety-related systems. As can be seen from the Overall safety lifecycle model, phase 9, 10 and 11 concern the realization of the SRS. As already noted, IEC 61508 only considered technical detailed design requirements on E/E/PE-SRS (phase 9).

The third part concerns the utilization of the SRS. During this part, requirements are defined concerning commissioning, operation, maintenance, periodic tests, eventual modifications and decommissioning of the SRS.

In order to establish whether the lifecycle and its requirements are correctly implemented, standards have defined checks at different levels. IEC 61508 has defined the following number of checks:

- Validation *‘the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system’*. For example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification [IEC61508]. This validation only checks whether the safety requirements as specified in earlier phases are correctly implemented in the designed and developed safeguarding measures. It does not validate correctness of the requirements themselves.

- Verification, *‘confirmation by examination and provision of objective evidence that the requirements have been fulfilled’*. In the context of this standard, verification is the activity of demonstrating for each phase of the safety lifecycle (Overall, E/E/PES and software), by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase [IEC61508].
- Functional safety audit, *‘systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives’*. A functional safety audit may be carried out as part of a functional safety assessment.
- Functional safety assessment, *‘investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities’*.

Validation is defined as one of the lifecycle phases, whereas verification is part of all phases. Audits and assessments concern the lifecycle models, but also concern documentation and functional safety management in general. Together, these four types of checks are intended to control correct implementation of IEC 61508.

4.6 Parallels and similarities regarding safety lifecycles

All lifecycles described in annex B comprise the starting phases ‘hazard identification,’ ‘definition and specification of the safety requirements,’ ‘realization and implementation of the safety measures,’ and ‘operation and maintenance of these safety measures’ (including the safeguarding equipment). It is worth noting that the standards have defined an ‘overall’ safety lifecycle, but do not necessarily prescribe detailed technical requirements for each lifecycle phase. For example, ANSI/ISA S84.01 clearly indicates in its safety lifecycle, which phases are dealt with in depth, and which phases are merely mentioned without any further technical requirements being provided. The purpose of this approach is to offer a framework, which can be used to structure the safety standard requirements that are implemented into the plant (safety) management system. The safety lifecycle model could therefore be interpreted as a ‘hollow’ framework that only allocates the requirements of the SIS with regard to the overall safety requirements.

As already mentioned, the scope of these lifecycle models can be interpreted as the lifetime of the safety role of a safety-instrumented system, thereby including hazard & risk analysis phases and safety requirements specification phases. After these phases, the SIS will be designed, manufactured, tested, operated and maintained. In line with this definition, there are phases during which the SIS does not yet exist physically. This presents one of the difficulties in the comprehension of a safety lifecycle. Safety is an intangible concept and is thus susceptible to varying interpretations.

Considering the safety lifecycle models, it is observed that a stepwise approach is applied. Tables that are added to the safety lifecycle models of IEC 61508, once more emphasize this. These tables describe for each phase of the lifecycle model, the objectives to be achieved, the scope of the phase, the required inputs to the phase and the outputs required to comply with the requirements.

Lifecycle models are being applied in other management areas in the industry as well. ISO quality standards (ISO 9000 series), and environmental standards (ISO 14000 series), call for the implementation of lifecycle models into the existing quality or environmental management systems. The challenge for the industry is to make use of safety lifecycle models, and find out how these models could help to bring their process safety to a higher level.

4.7 Current problems with the implementation of safety lifecycles

To comply with legislation and meet the technical requirements of safety standards such as IEC 61508 and ANSI/ISA S84.01, the currently used safety management system may need to be adapted. Individuals who are part of the safety management system need to be aware of their responsibilities and must be able to correctly carry out the safety-related activities. Specific data, required for performing the safety-related activities, needs to be complete, up to date, and available. Thus, information flows need to be realized and controlled.

The rationale behind the definition and application of safety lifecycles is to create a structure with respect to a large number of requirements, and to become better able to implement them and maintain compliance. Integration of the ‘Overall safety lifecycle’ into the existing safety management system is considered to be a serious problem. Typical questions that arise are (as repeated from Chapter 2):

- How can a safety lifecycle be defined?
- What are the boundaries of the safety lifecycle?
- How can a safety lifecycle be implemented?
- What are the criteria for proper application of the safety lifecycle?
- How can proper implementation be verified?

As will be discussed as part of the case studies in Chapter 8 and annex A, companies that have adopted a lifecycle-based SIS standard, are nevertheless having difficulties with the implementation of the lifecycle model and do not know how to take advantage of using a safety lifecycle model. For instance, case 10 shows a company that has adopted IEC 61508 and has subsequently ‘translated’ this standard into a corporate standard, but has not defined or adopted a safety lifecycle model. Case 2 concerns a problem description of another company that has adopted the American ANSI/ISA S84.01 standard but also has not defined or adopted a safety lifecycle model in their corporate standard. Another example concerns the company described in case 3. The reason that this company was unaware of their problem was concluded to be the direct result of the fact that the involved departments were not at all aware that they played a role in a safety lifecycle. Case study 8 concerns the description of a problem at a company that is strongly characterized by an organization structure which strongly isolates the involved departments which hampers the implementation of a safety lifecycle model.

The inclusion of the tables describing the objective, scope, inputs and outputs for each lifecycle phase incline towards the adoption of the stage-gate concept [Bro01]. The advantage of this concept is its consistent and systematic approach. At the same time however, the effectiveness of the implementation of the requirements of a particular phase, directly depends on the quality of the implementation of the requirements of the previous phase. Weak links of the lifecycle model strongly determine the performance of the safety system (weakest link in chain principle). Standards like IEC 61508 nevertheless pursue a

holistic approach, through which the performance of the safety-instrumented systems is guaranteed. Requirements with regard to planning, competence, verification and validation, and functional safety assessments and audits reflect this holistic approach. Detailed technical requirements on how to do a functional safety assessment are nevertheless not included in these standards.

In order to help the process industry to implement safety lifecycle models in a way that they indeed prevent the kind of problems as described in Chapter 1, the relationship between process safety management, the control of the involved safety-related business processes and the use of lifecycle models will have to be demonstrated. Appropriate application of safety lifecycle models requires a thorough analysis of the currently defined models. A model-based comparison is considered to be an essential step towards effective and efficient application of safety lifecycle models. Therefore development of a reference model is considered to be highly needed at this stage. The next chapter will give an overview of currently applied process safety management techniques and principles. Furthermore, an overview is given of a new concept to control information flows of reliability-related business processes.

5 Controlling safety-related business processes

This chapter discusses aspects of process safety management, safety-related business processes, and how the control of these business processes influences the performance of the process safety management system. To better understand the functioning and control of these safety-related business processes, the basic principles of system theory and control engineering in combination with the application of safety lifecycle models are discussed. Subsequently, related parallel research in the area of reliability information management is discussed with regard to the applicability of lately developed reliability management concepts to enhance the use of lifecycle models for process safety management.

5.1 Process safety management

This section discusses process safety management (PSM). The objective of PSM is to ensure safe operation of the subject processes and their installations. The fact that the term ‘safe’ is subjective and strongly depends on the people’s perceptions, will be discussed. Therefore, this section will start with a survey on incidents and process risks. In case of unacceptable risks, these risks need to be avoided or reduced. This is further described as part of process risk management. Finally a description of the safety management system and its functionality will be given.

5.1.1 Incidents

Most countries have adopted laws that require that incidents that have led to serious harm to people or the environment shall be reported to the local authorities (Incidents could be defined a potentially hazardous events whereas accidents could be defined as actual hazardous events). Subsequently, it will be decided whether a thorough investigation of the causes of the incident needs to be carried out [EC96], [OSHA1910]. Incidents can be defined as unplanned events with undesirable consequences. In the context of process safety, incidents include fires, explosions, releases of toxic or hazardous substances, or sudden releases of energy that result in death, injury, adverse human health effects or environmental or property damage [CCPS89].

Because the principle purpose of process safety management is to prevent incidents, incident investigation is a key element in any effective Process Safety Management System (PSMS). Each incident should be investigated to the extent necessary to understand its causes and potential consequences, and to determine how future incidents can be avoided. An axiom of incident investigation is that incidents are the result of safety management system failure. Invariably some aspect of a PSMS can be found that, had it functioned properly, could have prevented an incident. However, experienced incident investigators know that such specific failures are but the immediate causes of an incident, and that underlying each such immediate cause is a management system failure, such as faulty design or inadequate training. Most benefit is gained from identifying the underlying root causes. This is because by addressing the immediate cause, one only prevents the specific incidents from occurring again. By addressing the underlying cause, one prevents numerous other similar incidents from occurring. If the incident is analyzed, the complete scenario of events leading to an accident will be modeled. All the root causes will be identified, their relationship leading to the dangerous event will be revealed, and the resulting consequences will be established. A strong relationship between the various

incident scenarios may be observed. A particular initial failure may be the root cause of a number of different hazardous events and may result in many undesired consequences. At the same time, a particular consequence may be the result of various hazardous events, which in their turn may be the result of a number of different initial failures. To control the ‘spaghetti’ of root causes, intermediate states, hazardous events and related consequences, it is obvious that appropriate management is required.

In light of the important function of incident investigations in identifying and correcting PSMS failures, incidents should be looked as opportunities to improve management systems, rather than as opportunities to assign blame [CCPS89]. Van der Schaaf [Sch92] has demonstrated the added value of using information of ‘near misses’ to improve process safety by systematically analyzing near misses and taking preventive measures.

5.1.2 Process risks

Literature contains many definitions of risks. (See for different examples of definitions [CCPS89], [Lee96], [IEC60051] and [ISA96]). For instance, the International Electrotechnical Vocabulary (IEV) of the IEC defines risk as ‘the combination of the probability of occurrence of harm and the severity of that harm’ [IEC60051]. In general, risk is mathematically expressed as the product of the expected frequency or probability that a hazardous event will occur and its consequences. This may lead to a situation where the consequences of a hazardous event might be very high, but the expected frequency that such an event occurs might be low enough for the risk to be acceptable. In that situation no measures are needed to further reduce the risk. The definition of risk is therefore subjected to those who are asked to give an interpretation of this definition of risk. A plant manager might have a completely different interpretation of risk than one of his employees, who might be daily present in the dangerous zone. The plant manager will express the safety level of his plant by the number of accidents and their cost or the number of injuries or fatalities, e.g. on a yearly base. The maintenance engineer will most likely be primarily interested in the probability that he, or one of his direct colleagues, might get injured or killed.

In every day life the expressions ‘safety’ and ‘risk’ are continuously mixed up with each other. The relationship between these two terms is probably best expressed by being the inversion of each other. ‘The lower the risk, the higher the safety.’ Based on this relationship, it is justified to use the one by the other. (IEC and ISO have defined safety as ‘freedom from harm [ISO51].) The choice to use the term risk instead of safety is most of the time applied in case one wants to emphasize the positive or negative sound of the chosen wording.

Figure 8 shows the concept of risk reduction. In case a process installation is considered, a risk analysis may be conducted to determine the risks. If it appears that the risks are unacceptable high, risk reduction measures should be taken. After having done this, the ‘new’ risk level should be established to be acceptable. If this is still not the case, additional measures have to be taken.

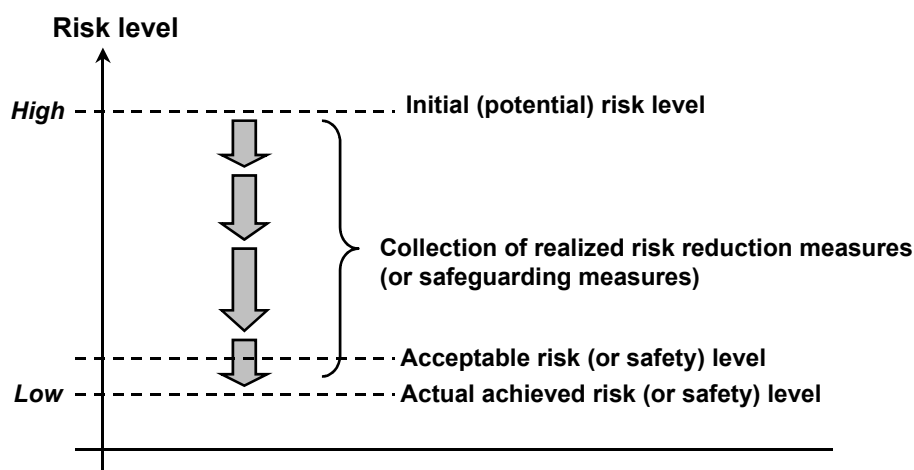


Figure 8 Concept of risk reduction

It must be emphasized that a clear distinction exists between designing an inherently safe operating process installation and the finally achieved risk level as the result of the application of various safeguarding measures. Obviously, it is normally the intention to design the process in such a way that no serious hazardous events can take place. This is done by e.g. considering the location of the installation, the physical process conditions (the process could perhaps be activated at a low pressure level by using a catalyst), and the size of the processing units (smaller and mutually isolated units will end up with less consequences in case of a hazardous event). At the moment that the design of the process installation is completed and fixed, an additional hazard and risk analysis will have to be carried out to determine possible residual risks to be reduced by additional safety measures.

5.1.3 Process risk management

In 1989, the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers published the 'Guidelines for technical management of chemical process safety' [CCPS89]. The CCPS recognized from its very beginning, that to prevent catastrophic events such as e.g. happened at Bhopal, improvements in chemical process technologies alone would not be sufficient. The CCPS has addressed the need for technical management commitment and technical management systems in industry to reduce potential exposures to the public and the environment [CCPS89]. These guidelines concentrate on the following three activities; risk analysis, risk assessment and risk control (see also Figure 9). The organizational process of these three activities is captured by the term 'risk management'.

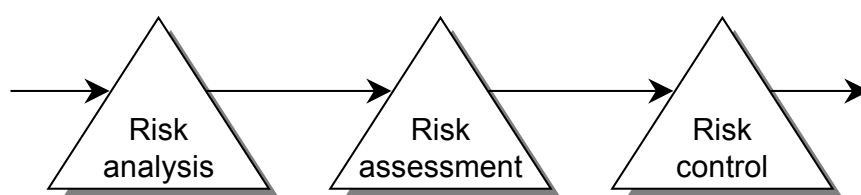


Figure 9 Main activities of risk management

The CCPS has defined risk analysis as the development of a qualitative or quantitative estimate of risk, based on engineering evaluation and techniques for considering the estimates of consequences and frequencies. Risk assessment is defined as the process by which the results of a risk analysis (i.e., risk estimates) are used to make decisions, either through relative ranking of risk reduction strategies or through comparison with risk targets. Risk management is defined as the systematic application of management policies, procedures, and practices to the tasks of analyzing, assessing, and controlling risk in order to protect employees, the general public, and the environment as well as company assets, while avoiding business interruptions [CCPS89].

As a result, process risk management involves the systematic identification, evaluation, and control of potential losses that may arise in existing operating facilities from future events such as fires, explosions, toxic releases, runaway reactions, or natural disasters [CCPS89]. Process Risk Management (PRM) requires recognition of possible risks, evaluation of the likelihood of hazardous events, the magnitude of their consequences, and determination of appropriate measures of reduction of these risks.

As discussed in the first section of this chapter, the term ‘safety’ and ‘risk’ are often mixed up. That also applies to the terms PRM and PSM (Process Safety Management). The CCPS recites twelve elements of Chemical Process Safety Management:

- Accountability: Objectives and Goals
- Process Knowledge and Documentation
- Capital Project Review and Design Procedures (for new or existing plants, expansions, and procedures)
- Process Risk Management
- Management of Change
- Process and Equipment Integrity
- Incident Investigation
- Training and Performance
- Human Factors
- Standards, Codes and Laws
- Audits and Corrective Actions
- Enhancements of Process Safety Knowledge

As mentioned in Chapter 2, this thesis will focus on the control of safety-related business processes and the added value that safety lifecycle models can have.

5.1.4 Safety management systems

An organization should put in place a safety management system (SMS) that will assure appropriate PRM. This safety management system might include review and approval programs, risk acceptability guidelines, business-area reviews, pre-acquisition risk reviews, and residual risk management [CCPS89]. Safety management systems for chemical process safety are comprehensive sets of policies, procedures, and practices, designed to ensure the barriers to major incidents are in place, in use, and effective. The safety management systems serve to integrate process safety concepts into the ongoing activities of everyone involved in operations – from the chemical process operator to the chief executive officer [CCPS89]. It should be recognized that process safety management systems are implemented in stages. While a comprehensive, integrated system is the objective, it needs not to be reached in one step [CCPS89]. Considering the definition of the SMS, it can be concluded that the SMS could be considered as being the equivalent of a Quality System (QS) as defined by the ISO 9000 series.

5.2 Safety-related business processes

As discussed in the 5.1.2, safe operation of industrial processes is only then achieved if the risks are reduced to an acceptable level. Safe operation implies that appropriate risk reduction measures are taken, and that these risk reduction measures are controlled during the entire operating lifetime of the subject process installation. Especially with regard to safety-instrumented systems, adequate application is only then achieved if these systems are correctly specified, implemented and operated. As can be concluded, based on the safety lifecycles earlier described and the comprehensiveness of the latest safety standards, an extensive number of safety-related activities shall be correctly carried out, i.e. according the numerous requirements as defined by these standards. At this stage, it is therefore concluded that the point of particular interest should not primarily be the standard requirements, but rather the required safety-related activities. If for instance a particular activity does not need to be carried out, also the accompanying requirements will no longer have to be implemented.

As described in Chapter 4, a large number of combinations of errors and failures often characterize the development of accident scenarios, its root causes and final consequences. For this reason, further attention is spent to the subject safety-related activities, also otherwise expressed as the safety-related business processes. It could subsequently be questioned what exactly business processes are. According to Brombacher [Bro00], a business process is a set of interrelated activities that is required to define, realize and utilize a product, process or service. In order to understand the (dis-) functioning of safety-related business processes is done by showing some examples of typical problems with regard to these business processes. Following examples concerns problems that are observed during the various case studies as described in detail in Chapter 8 and annex A. Subsequently, specific aspects of these kinds of problems are further discussed in this section. The observed problems concern the application of safety-instrumented systems according to lifecycle-based safety standards.

Example problem description of case 3 – Fertilizer plant in the Canada (see annex A for further details).

During the introduction on the new safety standards, a level of awareness and commitment was created among the attendants that the concepts of these standards really needed to be implemented. The following discussion on the industrial cases however, revealed some serious implementation problems. It appeared that HAZOP leaders were not able to determine the SIL requirements for the SIF's to be applied. On the other hand, the people from the instrumentation department seriously needed this information to meet the requirements of IEC 61508.

Example problem description of case 7 – A Hungarian refinery (see annex A for further details).

To start with the study, information was gathered on the process installation and instrumentation. Remarkably, it appeared that the American engineering contractor already added the SIL requirements (based on ANSI/ISA S84.01) of the safeguarding instrumentation to the P&ID's. On the other hand, no detailed narratives on the hazard and risk assessment and no explanations on the prescribed SIL requirements existed.

In order to be able to validate the SIF's, it was started to collect information among others about the off-line periodic test procedures, the maintenance procedures and application circumstances of the safeguarding instruments. This information was needed to do the quantitative reliability analysis. During the discussions that followed, it appeared that the people from the engineering department and the operation department had serious doubts concerning the correctness of the prescribed SIL requirements.

The described examples clearly show that correct execution of the safety-related business processes appears to be strongly depending of the existence of specific information. Without this information certain activities can not, and thus in practice apparently are not, correctly performed. Concerning the specific required information, two aspects are of essential importance. First of all, it needs to be known and defined which kind of information is exactly required. Secondly, it needs to be determined which person or department this information should provide or where this information can be found. Presuming that the safety-related business processes are considered to be an inter-related collection of safety-related activities, the successful execution of these business processes primarily depends on the quality of control of the safety-related information. Therefore, safety-related information could be defined as knowledge, data or facts that are obtained from study, experience or measurement, which needs to be used to determine the right and adequate actions or measures that influence or maintain the achieved safety level as discussed in Section 5.1.2.

It is noticed that the location where the requested information needs to be created and the location where the information needs to be processed, clearly need to be determined.

Considering the safety lifecycle models as defined in the latest safety standards, it is from this point on obvious that these lifecycle models in a certain way structure the involved safety-related activities. Based on that conclusion, it could subsequently be concluded that safety lifecycle models indeed offer a (rough) framework of inter-related activities and as such establish the need for information exchange (or information flows) between specific activities. As discussed in Chapter 4, the lifecycle phases could be considered as a sub-collection of safety-related activities that are more or less performed during the same time period. Information flows between lifecycle phases represent the collection of information flows between specific activities of consecutive lifecycle phases.

An aspect, which is not addressed by lifecycle models, concerns the kind and quality of information that needs to be transferred. The quality of safety-related information could be defined as its appropriateness or the degree to which the information is suitable to be able to determine and implement the right and adequate safety actions or safety measures.

Although the fact that certain safety standards such as IEC 61508 have established the kind or type of information that needs to be created in one phase and to be subsequently used in another phase, none of these standards prescribe quality levels of this information. Neither have these standards precisely defined what information needs to be created as the result of a specific activity and for which other specific activity it needs to be used.

In order to develop a better understanding of the basic concepts of safety management systems in relationship with the concepts of controlling safety-related business processes, relevant aspects of the system theory of control engineering are surveyed in the next section. Section 5.5 will elaborate on aspects of lifecycle modeling in order to form the required framework. Section 5.6 will discuss recent developments of parallel research in the field of reliability information management. It will subsequently be questioned whether and how developed techniques in the field of reliability management could be applied to control safety-related business processes.

5.3 System theory and control engineering

From an organizational point of view, process safety management can be characterized as the control and execution of a wide collection of safety-related activities. As defined, the considered activities have in common that they are safety-related. Adequate safety management is only then achieved if the involved safety-related activities are properly carried out. The ‘quality’ of each single safety-related activity depends on a number of aspects. It will be demonstrated that the quality of a specific safety-related activity directly depends on the ‘quality’ of other involved safety-related activities. It is therefore a priori postulated that effective and efficient safety management is achieved in case the quality of the individual safety-related activities as well as the interaction between these activities is properly controlled. Both aspects will be further investigated.

5.3.1 Open versus closed systems

Robbins [Rob90] describes organizations as systems. According to Robbins, a system is defined as a set of interrelated and interdependent parts arranged in a manner that produces a unified whole [Rob90]. A first level of characterization of systems is the distinction between open and closed systems. Open systems have inputs, transformation processes, and outputs. The open system recognizes the dynamic interaction of the system with its environment. Organizations obtain their raw materials and human resources from the environment. Without a boundary there is no system and the boundary or boundaries determine where systems and sub-systems start and stop. A simplified graphic representation of the open system is given in Figure 10.

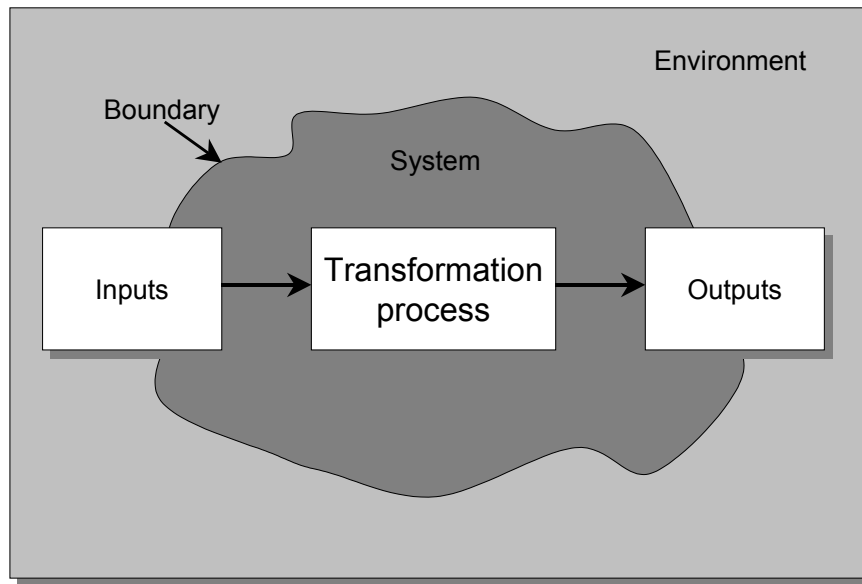


Figure 10 An open system with its boundary and environment [Rob90]

A closed system is considered to be self-contained. It essentially ignores the effect of the environment on the system. A perfectly closed system would be the one that receives no energy from an outside source and from which no energy is released to its surroundings [Rob90]. The transformation process (Figure 1) as defined by Robbins is often expressed by different wordings like ‘process’, ‘operation’ or ‘activity’. The wording ‘activity’ will be further used in the remainder of this thesis.

Safety management systems of process industry sector companies are considered to be open systems. The set of safety-related activities are characterized by clear interaction with their environment, such as the government who is responsible for the safety regulations to be applied.

Another example of the ‘openness’ of process safety management systems, concerns the interaction with the control of the process quality. , In this case, all kinds of economic factors might influence decisions such as choosing to do maintenance of the safety devices while these devices are put in override and the process continues to produce. In this example, this implies that it is not chosen to stop the production process for maintenance reasons, but to continue operation while at that moment the safety functions are disabled. This kind of conflicting interest of different kinds of systems (safety system versus production system) illustrates the complexity of their interaction and mutual influences.

5.3.2 Safety-related activities

Safety-related activities can very well be described by the system theory. For instance, a study during which the potential hazards are identified is considered to be a safety-related activity (Figure 11). The quality of the hazard identification study depends among other things on the applied identification technique. Well-known hazards identification techniques are for instance HAZOP (Hazard and Operability), SWIFT (Structured What If Technique), FTA (Fault Tree Analysis) and ETA (Event Tree Analysis). (Whereas e.g. a HAZOP study is a much more rigorous method than the SWIFT method.) Besides the selected identification technique, the quality of this safety-related activity also depends on the completeness of the required input information. If the P&IDs (Piping &

Instrumentation Diagram) are incorrect, it will obviously influence the output of the hazard identification study. concerns a graphical presentation of the system of hazard identification. The applied technique is the HAZOP method. P&IDs form the required input, and the resulting output concerns the C&E (Cause and Effect) diagrams.

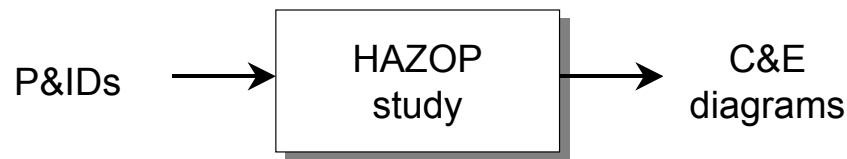


Figure 11 HAZOP study activity, required inputs and outputs

According to in 't Veld are models simplified reflections of the reality [Vel87]. This statement also applies to the above system. In reality the 'quality' of the hazard identification depends not only on the chosen identification technique, the quality of the P&ID's, but also on e.g. the competence of the involved people. Furthermore, it could be discussed whether the HAZOP technique should be in the box as representing the defined safety-related activity. Possibly, this activity might be better expressed as the 'hazard identification' and should the HAZOP technique subsequently be considered as an input as well.

Although the process of safety management is aimed at minimizing risks and preventing hazardous events, this 'safety performance' output may not be the best output parameter to control and thereby optimize the safety performance. The safety performance could for instance be expressed in terms of, number and size of explosions, severity and number of injuries, production loss, etc. Measurement of these outputs automatically means that corrective measures can only be considered as a kind of feed back, which might not be desired (prevention is preferred above healing). A feed forward optimization might in that case be more appropriate.

Organization theory researchers agree that technology refers to the information, equipment, techniques, and processes required for the transformation of inputs into outputs. That is, technology looks at how the inputs are converted into outputs [Rob90]. Thompson [Tho67] has defined three technology-structures, two of which are discussed further.

Long-linked technology applies when tasks or operations are sequentially interdependent. This technology is characterized by a fixed sequence of repetitive steps as shown in Figure 12.

Because long-linked technologies require efficiency and coordination among activities, owing to sequential interdependencies, the major uncertainties facing management lie on the input and output sides of the organization [Tho67].

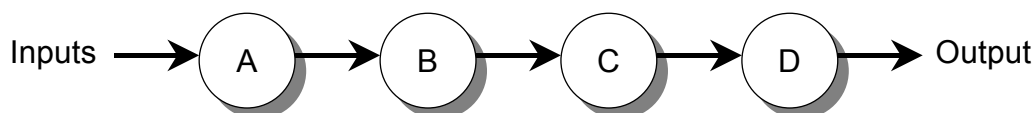


Figure 12 Long-linked technology [Tho67]

A typical example of long-linked technology concerns an organization that applies sequential engineering techniques [CFT94]. The development process of a new product is

characterized by the complete development of the first part of the product, before the development of following part will be started. Detailed information is available of the first part on which the development of the following part can be based. The advantage is that precise information is available, but disadvantages are the relatively long development process of the complete product and the growing inflexibility to make changes as the development process approaches its final phase.

Intensive technology represents a customized response to a diverse set of contingencies. Figure 13 illustrates that intensive technology achieves coordination through mutual adjustment. A number of multiple resources are available to the organization, but only a limited combination is used at a given time depending on the situation [Tho67].

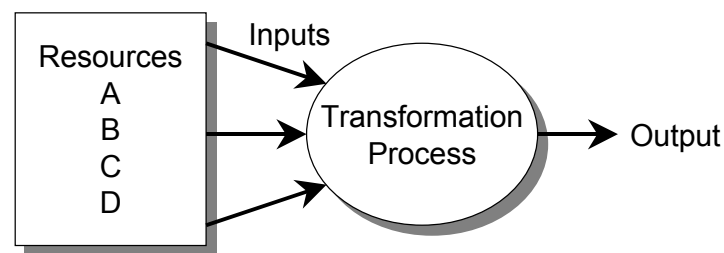


Figure 13 *Intensive technology* [Tho67]

A typical example of the intensive technology concerns the concurrent engineering process [CFT94]. As much as possible, the development of the various parts of a new product is done in parallel. At the moment that the minimum of information resulting from the development of the first part is available, although this development is not completed, the development of the following part can be started. The advantage is a shortening of the complete development process of the product. A disadvantage is the minimum of information that is available to continue other developments, which might result in conflicting situations at the moment that the detailed information becomes available.

The long-linked technology has clear similarities with the approach represented by the safety lifecycles as defined in current safety-related standards. Safety management is considered a chain of processes, which take place at different stages of the lifetime of the process installation and the lifetime of the safeguarding measures. However, the intensive technology model also reflects the processes of the safety management. Each transformation process, e.g. a HAZOP study, can only be successful if a selected set of resources is available. (E.g. P&IDs, different experts, etc.)

The process safety management activities as part of its safety lifecycle are therefore characterized as a combination of the long-linked technology and the intensive technology. The impact and graphical representation of combining these two models is further discussed in the next chapter describing the safety-related activity management model.

5.3.3 Input flows and output flows of activities

Transformation processes, systems, or activities are characterized by (a number of) inputs and outputs. Without proper inputs the transformation will not correctly take place, and will not result in the required outputs. The quality of the output of a transformation or a system will therefore directly depend on the quality of the input. Inputs and outputs are often represented as flows, such as information flows, material flows, energy flows, etc.

Molenaar et. al. [Mol01] distinguishes two kinds of main flows as part of a business process:

- Physical flows; the transformation process of ideas and (raw) materials into a working product.
- Information flows; information of the above products with respect to function, cost and quality. (See also Figure 14.)

Furthermore, activities are characterized by an enabler or control factor and by conditions. Concerning PSM of the SIS, the business driver is clearly defined by safety functionality and safety integrity. Molenaar states that traditionally the main emphasis in quality control has been on the control of the physical flow and control of information flows is still lacking. (Figure 14) In line with that conclusion, this thesis will therefore in a more detailed level focus on the control of information flows.

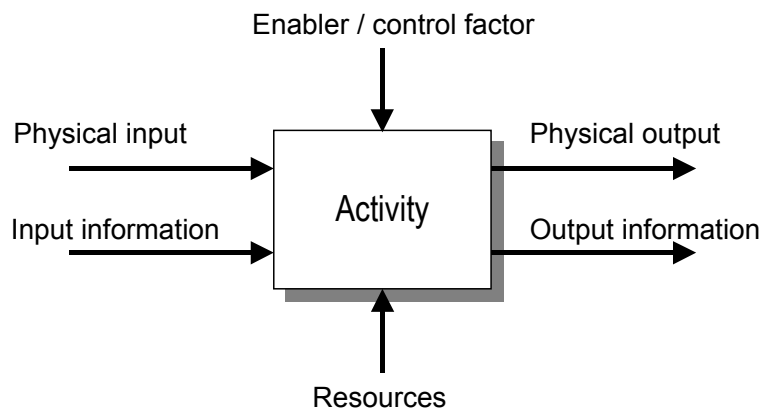


Figure 14 Activity model with required inputs and outputs [Mol01]

Furthermore, Molenaar speaks of information disruptions at the moment that the required and correct information is not available to the right person, at the right moment in time. As will be discussed in Chapter 7, these disruptions may for instance be the result of barriers. Different kinds of barriers will be further discussed in Chapter 7.

As discussed in the previous section, a safety management system could be considered as a collection of safety-related activities. Furthermore, such a system comprises a number of flows, which might e.g. be the output of one activity and needed as input for another activity. Without these flows, these activities will not be carried out successfully. Especially information flows play an important role in order to control the performance of a transformation or activity. Management and control of the quality of information flows is therefore considered to be the primary concern and prerequisite to manage and control the safety-related business processes of a SMS. If for instance the quality of the physical input deviates from the required or expected input, this knowledge is expected to be part of the input information flow. Adaptations to the transformation process might thereupon be based on this information in order to produce the required output. If e.g. the required physical output is not produced, then this knowledge should be part of the resulting output information flow. Adaptations of following activities can be made or expectations of the system performance adjusted.

Based on these observations the following interim recapitulation is made. Management of process safety implicates control of the safety-related business processes. Controlling

these business processes implicates control of the safety-related activities and the control of involved information flows. In order to control these business processes, thorough overview and understanding of the SMS-related activities need to be developed. Particularly concerning the relationships between the safety-related activities, structures will need to be established. The next section will discuss the ability to make use of safety lifecycle models that are defined in the SIS-related standards, as a basis to develop the required structures.

5.4 Lifecycle modeling

Robbins [Rob90] defines a lifecycle as a pattern of predicable changes. Also organizations are proposed to have lifecycles whereby they evolve through a standardized sequence of transitions as they develop over time. For instance, at the moment a new product is designed, it will subsequently be developed, tested, manufactured and sold. By applying the lifecycle metaphor to organizations, it can be concluded that there are distinctive stages through which organizations proceed, that the stages follow a consistent pattern, and that the transitions from one stage to another are predictable rather than random occurrences. The target of application of the safety lifecycle models is for instance clearly described in IEC 61511 part 1, clause 6 [IEC61511]:

'The objectives of the requirements in this clause are to organize the technical activities into a safety lifecycle, and to ensure that there is adequate planning for making sure the safety-instrumented system meets the safety requirements exists, or that this planning will be developed. A safety lifecycle incorporating the requirements of this standard is to be defined during safety planning. Each phase of the safety lifecycle will be defined in terms of its inputs, outputs, and verification activities.'

One of the objectives of the application of safety lifecycle models is to distinguish clear milestones, which indicate at what moment a set of related activities commences, and at what moment they are completed. The added value of this aspect is that safety-related activities are easier managed which results in easier verification of the SMS. The application of safety lifecycle models helps to coordinate, communicate and transform information flows between safety-related activities. If such a group of related activities is carried out properly, this will lead to the achievement of the safety-related objective(s) with regard to that particular lifecycle phase. For example, the HAZOP technique is a tool to execute a hazard analysis. The hazard analysis itself is an activity (therefore a hazard analysis is often called a HAZOP study). The final objective of the particular phase during which the HAZOP study is performed is to identify all potential process hazards. The HAZOP study can be considered as one singular activity, but could also be seen as a collection of related activities, such as the collection of safety-related documentation (e.g. P&IDs, flow diagrams), application of the checklists, etc. Therefore, a lifecycle phase could be defined as a time span comprising a subset of directly related activities which start a specific moment in time and which are completed at a later moment. A following subset of safety-related activities will not be started before the first subset is completely finished. E.g. first the complete set of activities concerning the HAZOP study needs to be finished before the C&E diagrams are set up. Section 7.4.1 will further discuss aspects of lifecycle phases.

Obviously, PSM involves many safety-related activities, which do not by definition take place in a consecutive way, but may also take place at the same time. This aspect of parallel processes is better known as ‘concurrent engineering’. Concerning the application of safety lifecycle models to structure the SMS, it is stated that the defining of the boundaries between lifecycle phases is a subjective process, and strongly depends on the perception and interpretation of the experts.

One of the aspects that determine the number of lifecycle phases is the complexity of an organization. Complexity refers to the degree of differentiation that exists within an organization [Rob90]. Horizontal differentiation considers the degree of horizontal separation between units. Vertical separation refers to the depth of the organizational hierarchy. Spatial differentiation encompasses the degree to which the location of an organization’s facilities and personnel are dispersed geographically. (The next Chapter will discuss and illustrate examples of horizontally and vertically oriented organizations.) An increase of any of these three factors will increase an organization’s complexity [Rob90]. The most visible evidence in organizations of horizontal differentiation is specialization and departmentation [Rob90]. If this span is wide, managers will have a number of subordinates reporting to them. The smaller the span, the taller the organization. Also organizations, which are responsible for the PSM are characterized by a plain level of specialization. Specifically larger companies have departments of specialists. The more complex an organization, the greater the need for effective communication, coordination, and control devices [Rob90]. This thesis will not further discuss criteria on how to determine appropriate lifecycle phases and their boundaries. It will nevertheless observe boundaries of safety management systems during various case studies and analyze how these boundaries may influence the control of safety-related information flows.

A hypothetical example is shown in Figure 15, in which three safety lifecycle phases are represented. This lifecycle could be considered to be part of the SIS safety lifecycle, containing the three phases ‘hazard identification,’ ‘risk assessment,’ and ‘specification of safety measures’. The subjective character of the defined boundaries is illustrated by referring to the IEC 61508 Overall safety lifecycle model. This lifecycle model combines the ‘hazard identification’ phase and ‘risk assessment’ phase into one single phase. Ultimately, to comply with IEC 61508, it is important that each requirement is met. Therefore, one is not necessarily restricted to apply the lifecycle exactly as it is specifically laid down in the standard. It is as such possible to create a safety lifecycle composed of more or even fewer phases, as long as all of the remaining standard requirements are met [IEC61508].

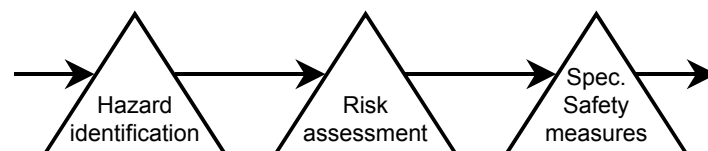


Figure 15 Example of related lifecycle phases

It is assumed that the definition and application of a safety lifecycle model will depend on the involved industrial processes, environmental circumstances, complexity of the organization, company policy and culture, local regulations, etc.

5.5 Related parallel research in the field of reliability management

Terms as safety, reliability and quality are in a certain way connected with each other. In everyday life, it is often said that a product, which is of a high quality, is thus reliable and safe. Not surprisingly, it appears that various techniques that are applied in the field of reliability engineering are also applied for the determination of safety integrity levels and a similar relationship consists between reliability engineering and quality control techniques [Rou01]. It is therefore assumed that control aspects and techniques of safety-related business processes will most likely have close relationships with control aspects and techniques of reliability-related or quality-related business processes.

Brombacher [Bro00] and Huiben [Hui98] emphasize on the need for controlling business processes concerning quality, and in addition to this, also concerning the reliability of business processes. Particular attention is paid to the control of information flows as part of these business processes.

This section will discuss the control aspects and techniques of reliability-related business processes and the applicability of these concepts and techniques to control safety-related business processes. Particular attention is paid to the MIR (Maturity Index on Reliability) concept as a means to control reliability-related information flows. Firstly, as an introduction, the risks of unreliable products are discussed versus the risk of unsafe operating process installations.

5.5.1 Risks of unreliable products versus risks of process installations

Reliability of products, processes and services is becoming a more and more important issue. End-users expect a continuously increase of the reliability of what they have purchased [Bro00]. If the reliability of a product does not meet the customer's expectation this may lead to;

- rejection of batches during production processes,
- an increase of the re-call rate, during the warrantee period,
- call back of production batches out of the field,
- a decreasing market share as a result of growing competition and
- in certain situations to large insurance claims.

Obviously, the above mentioned points sometimes result in large financial consequences. In this context, risk could be expressed as the number of problems multiplied by their consequences. Risk in the process industry is characterized by relatively few serious accidents, but enormous consequences related to high cost. Risk concerning the quality and reliability of consumer products is characterized by most times relatively small cost per single product, but high volumes of these products led to extreme cost. Within the consumer products, a strong competition drives manufacturers to continuously improvement of the quality and reliability of their products. A strong emphasis is laid on the time to market of these products, putting a lot of pressure on those who are responsible for the control of the reliability of these products [Bro00].

5.5.2 Development of the MIR concept

One of the major problems of developing products in a strongly competitive market is that manufacturers will have to meet with a large number of conflicting requirements. Basically four different trends can be identified [STT01]:

- Increasing product complexity
- Increasing pressure on ‘time to market’
- Increasing complexity of business processes (globalization)
- Increasing demands from customers on product quality and reliability

Companies will only be able to survive if they are able to meet all requirements simultaneously and successfully manage the resulting conflicts [STT01]. As discussed in the first chapter, especially the first, third and fourth aspects currently play an important role in the process industries. (Not withstanding the validity of the remainder aspect.)

Brombacher [STT01]:

‘In order to meet the above requirements it is important to prevent iterations in the product development process, especially in the later phases. (See Figure 16 for the cost impact of design stages as a function of the development phase.) This has especially to do with the fact that in the late phases a much larger logistical chain is involved in the change process compared to earlier phases. Preventing such a change much earlier in the development process, however means that predictive techniques will have to be used to anticipate and prevent these late design changes. For stable and mature technology, techniques like Failure Mode and Effect Analysis (FMEA) and related methods can be used. These methods, however, require detailed knowledge of failure mechanisms that may occur in the future product.

For products with a strong degree of innovation this will be much more difficult. Not all failure mechanisms will be predicted correctly. Therefore it is likely that product development processes that have to deal with a certain degree of innovation, both in the product and the business process, will have to adopt rapid learning mechanisms in order to feed back information of those events that were not predicted back into the development process of future products. Therefore the cornerstone of future development processes will most likely be:

- *The use of adequate predictive techniques.*
- *The use of fast learning cycles.*

The faster a company is able to learn from unanticipated events the sooner they will be able to apply the lessons learned into the development of future products.’

This has resulted in the development of the MIR concept and the definition of the MIR levels. The development of the MIR levels was originally inspired by the definition of the CMM (Capability Maturity Model) levels for software development by the Software Engineering Institute (SEI), as led by Humphrey [Hum89]. The following passage is taken from the MSc thesis of K.A.L. van Heel [Hee99a]. This passage gives a short overview of the MIR index:

‘The Maturity Index on Reliability (MIR) [Bro99] [Hui98], [San00] reflects the capability of an organization on controlling reliability-related information. The purpose of this method is to analyze the reliability/safety lifecycle of a product/process installation and identify missing or incomplete reliability/safety information flows of a product/process installation lifecycle. The MIR concept is based on two aspects:

- *The availability of closed-loop information flows where reliability information is involved.*

- *The inherent quality of the information in this information loop.*

The basic concept of an analysis can be illustrated by modeling each process as a network of sub-processes or activities that are interconnected with each other. For large processes, subsets are defined according to logical phases in the process. As first step a flowchart of the product lifecycle is created. A flowchart expresses the sequence and logic of procedures using symbols to represent different types of input/output, processing, and data storage. A flowchart can:

- *visualize communication procedures and controls and the sequence in which they occur,*
- *compare the actual vs. ideal flow of a process to identify improvement opportunities,*
- *examine which activities may impact the process performance,*
- *serve as an aid to understand the complete process, and*
- *include objectives, documentation and information flows.*

To analyze the product/process lifecycle and measure the MIR level of the organization, the product/process lifecycle will be converted to a flowchart looking to the following items:

- *The phases.*
- *The processes.*
- *The information flows.*
- *The learning cycles.*

In a product lifecycle, a phase can be seen as a process where input is transformed into output. A phase can have one or more phase(s) (supplier(s)) which supply the input needed in this phase. For a phase it has to be known what must be achieved (objectives), how this should be achieved (activities/requirements) and why this should be done. this phase may also be connected to other phases (customers) that use the information created during this phase.

To identify all the process phases and information flows, several steps should be taken. Firstly, determine which process has to be considered and the result that must be achieved by this process. Subsequently determine the phases with related objectives and activities and how they follow each other. All needed inputs must be uncovered and the output must be known. Confirm that the input for one phase is the output of the phase that must supply this input. Confirm also that the created output is the input that is needed in the connected phase. Assign the information flows between the linked activities. Identify the outputs going outside of the process to other processes and the input from outside the process. At last, add the learning cycles to the process. At this moment the flowchart can be completed and it is possible to analyze the product lifecycle to identify missing or not complete items.

Depending on the information flows that are realized, it is possible to assign a MIR level to the company's procedures. The four-level scale, which reflects the increasing capability of an organization to analyze, predict and improve the reliability/safety of its current and future products, is the following:

1. *Quantification (measured): The business process is able to generate quantitative information on a per-product basis, indicating the number of failures in the field and production.*

2. *Identification (analyzed): The business process is able to determine the primary and secondary location of failures:*
 - *Primary (organization): Location of the cause of the failure within the business process.*
 - *Secondary (position): Location of the failure within the product.*
3. *Cause (controlled): The business process is able to generate detailed information for all dominant failures on root-cause level. This can be translated into repairs/modifications in current products and anticipated risks for future products.*
4. *Improvement (continuous improvement): The business process is able to learn from the past in installing business processes and working methods to anticipate reliability risks for future products and eliminate these risks as part of new product creation.*

MIR analysis has proved to be a very useful method for analyzing the lifecycle of a product [Bro99]. The flowchart gives a clear overview of a product lifecycle. It shows all relevant information flows that have to be achieved to operate in a right way. With regard to reliability management, the Maturity Index on Reliability (MIR) concept offers an approach to analyze the reliability of a product through analysis of the organization [Bro99]. Each MIR level represents the extend companies have organized a comprehensive product lifecycle.'

The above-discussed four-level scale is considered to be still very generic of nature. Various MIR studies that were carried out during a number of years, including the ones described in this thesis, have resulted into new insights concerning the application of MIR levels. Whereas initially a strong focus existed on analysis of the business processes of an organization as an integrated entity, today a more differentiated attention is given to the analysis of specific information flows. Evidently, this has also resulted in adaptations to the definitions of the MIR levels (as described in Table 1 of Section 7.2.6).

It is during these case studies observed that complex business processes comprise a wide variety of information flows. These flows may comprise reliability-related information of different categories. It is by definition presumed that the 'higher' the MIR level, or the more information on the considered reliability aspect, the better the information flow meets the requested information to be put into a particular activity. This brings along that, with respect to the wide variety of existing information flows as part of the considered business processes, every single information flow will need to be considered separately. For each flow, the actual realized level and the needed level of information shall be determined. Such a reliability-related information flow analysis will reveal discrepancies between realized and needed MIR levels. It will depend on the specific purpose of each considered information flow, what MIR level will be needed, and thus will need to be realized. For instance, the person who is only responsible for the repair of a failure will only be interested in information concerning what has failed, and what needs to be repaired or replaced. This person will, considering his profession, not be interested in information on how to prevent such failures in future.

The presumption, that the 'higher' the MIR level of an information flow is automatically considered as being 'better' information, is not per definition correct and can even have disadvantages concerning 'overflow' or increasing fuzziness of the information. (The receiver of information needs it for certain purposes, nothing more and nothing less. Any additional information added to the requested information might result in a difficulty for the receiver to filter the needed information.) In Chapter 7, four modeling cases will be

described that illustrate the different kind of quality levels of safety-related information. These modeling cases have resulted in a more specific definition of the MIR levels as is presented in Table 4 of Chapter 7.

5.5.3 Applicability of the MIR concept for PSM

As discussed, it is not enough to step by step perform the involved activities and requirements of each successive phase, and ‘hope’ that the final validation will be successful. Instead the business processes need to be controlled in such a manner that it is already in advance almost certain that the validation will be successful. (Unfortunately, especially if a new design of a SRS is realized, which needs to comply with additional and new functional requirements, there is always a probability that something was ‘overlooked’ that could not have been predicted based on the existing knowledge.) The classical way to structure this process according to Brombacher [Bro00], is to use the so-called functional development process. Brombacher:

‘In a functional development process the different transformations (or activities) are clustered as groups with similar characteristics or functionality. These activities are operated sequentially according to well-defined procedures and guidelines.

In a functional process so-called milestones separate the activities of different functionality. These milestones (or gates) are used to decide whether the process can proceed to the next phase. Although the functional development structure is currently criticized for a number of reasons, the functional structure has also certain advantages. In a functional development process all activities that relate to a given aspect are concentrated in one phase. Due to this structure, there is usually little distance, time-wise, geographical, and with respect to the people involved, between a decision and the consequences of this decision. All decisions on production processes are, for example, taken in the pre-production phase. When something goes wrong during pre-production the milestone to the next phase is not passed and all efforts are concentrated on resolving the problem.’

One of the negative consequences of the functional development structure concerns the relatively high probability of being forced to make design changes during the later phases of the development process, which result in increasing cost. Figure 16 illustrates the relationship between the phase of the development process and the cost of a design change (Source: Cost of non-quality, Business week, April 30, 1990).

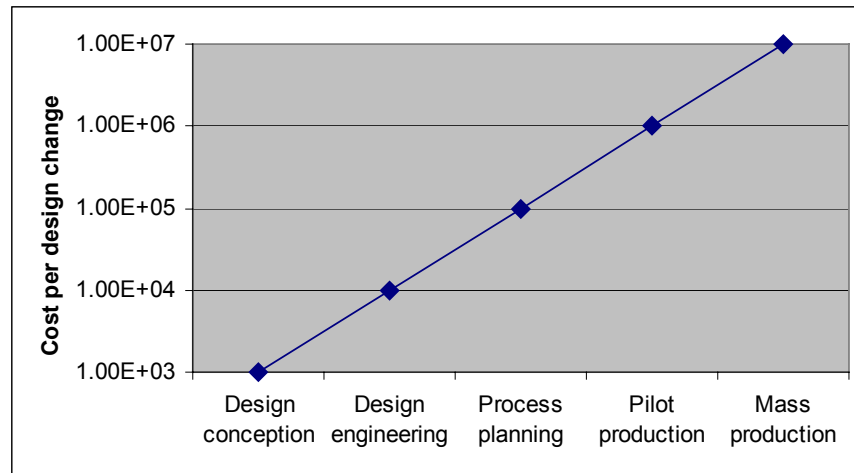


Figure 16 Cost impact of design stages as a function of the development phase

Brombacher [Bro00] phrases this problem as follows:

'The major problem of the functional development process is that it assumes independency of the individual functions. Ample literature is, however, available that decisions in the early phases of the process can seriously affect the performance of the later phases of the process. Bralla demonstrates, for example, in his book Design for Excellence [Bra96] that early, or upstream, activities can dominantly influence the performance of downstream activities such as production. Decisions made in the early phases of the development process can result in products, with the same functionality that are either very easy or almost impossible to manufacture.'

'The management of prevention of failures or minimize their consequences puts considerable demands on the organization structure and the communication processes within that structure. People have to be able to make decisions on problems long before they happen during phases of the process when the specification of the product is defined in far less detail than people are used to [And87], [Car92].'

As a methodology to control the requirements of the software development process, IEC 61508 recommends the application of the V-model. This model which is illustrated in Figure 17, is characterized by 4 aspects, namely requirements specification, develop the validation plan and in parallel realize the requirement (software), and perform validation activities (testing the software).

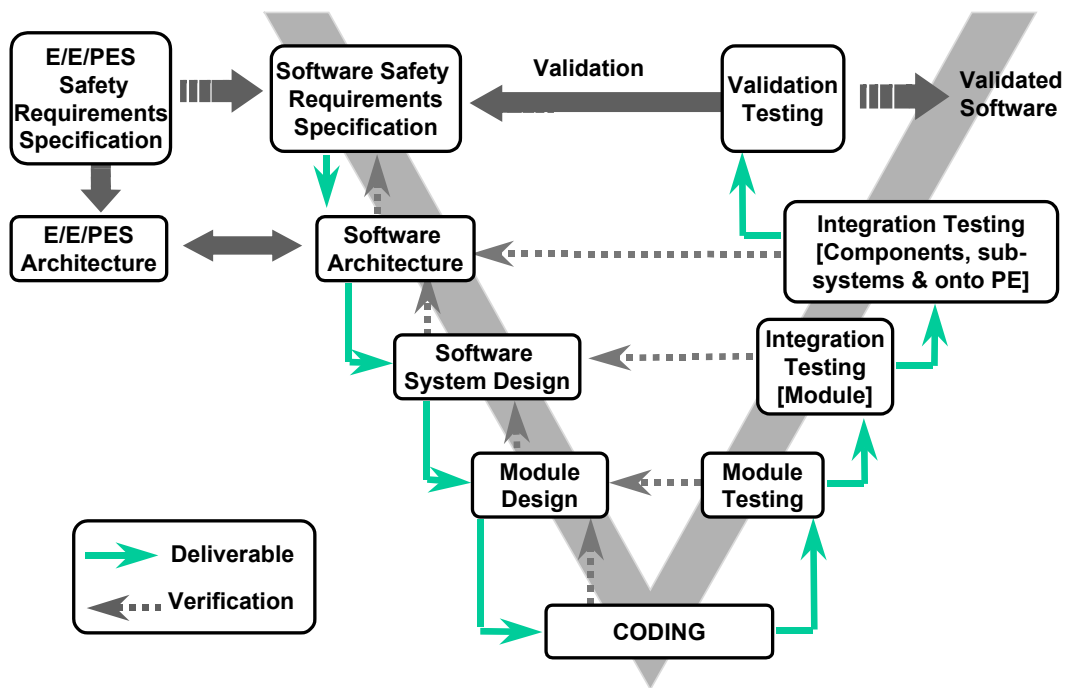


Figure 17 The V-model

The difference with the functional development process is that, consecutive departments execute not solely a sequence of safety-related activities, but the very same departments are involved in reverse order to perform the validation activities. Also with regard to application of the IEC 61508 Overall safety lifecycle model a comparable procedure is followed. During the very first phases, the end-user will determine the need for additional risk reduction measures (e.g. the application of a SIS). Subsequently an engineering contractor will normally be responsible for the technical specification of these risk reduction measures, after which an integrated system will take care of the realization of the SIS from ‘fluid to fluid’. Manufacturers of safeguarding equipment (safety-instrumented subsystems), will supply the required hardware and software. After the realization and integration of the subsystems, and validation and testing, the end-user will start with the operational activities of the SIS and be responsible for e.g. maintenance (See also Rouvroye [Rou01]). For example Figure 18 illustrates the shared responsibility for the specification, realization and utilization of the SIS.

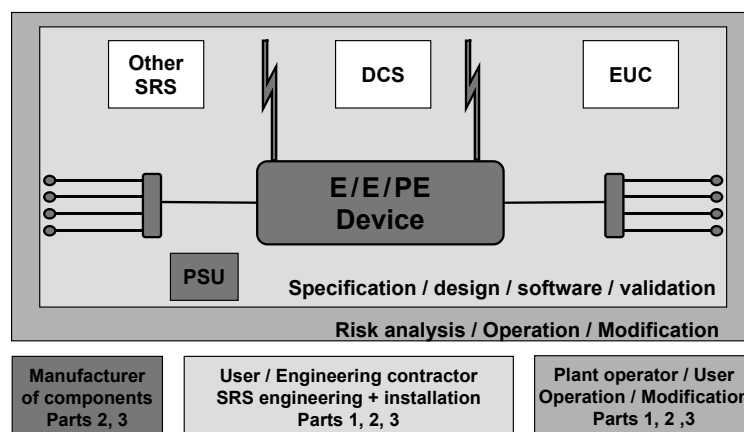


Figure 18 Shared responsibility for the specification, realization and utilization of the SIS

The challenge of an end-user in the process industry is to adapt its process safety management system in such a way that the business processes of the early phases of the defined safety lifecycle are controlled in interaction with the way the business processes of the latter phases are controlled.

The methodology of safety lifecycle management, which will be discussed in the next chapter, has been developed to cope with this challenge and to control the interactions between involved safety-related activities on an integral base.

Concluding, it can be stated that the characteristics of controlling safety-related business processes are closely related to controlling reliability-related business processes. The MIR concept which strongly focuses at the control of the subject activities and their intermediate information flows, is expected to be an adequate concept to enhance the implementation of safety lifecycle models. Various cases that are discussed in this thesis abundantly and clearly demonstrate the impact of poorly managed safety-related activities during the initial phases of safety lifecycles on the final safety performance. The need for dedicated control of the various safety-related information flows is therefore considered as essential to successfully carrying out consecutive activities. Qualification by categorization of these information flows is therefore a valuable means to better generate and compound, transfer, and process the right information.

5.6 Further specification of the research

5.6.1 Recapitulation

Chapter 4 discussed a new concept introduced by safety standards to allocate and control the requirements on SIS's. This concept concerns the application of safety lifecycle models. With regard to the safety lifecycle models, these standards have described the objectives, inputs and outputs of each lifecycle phase.

This chapter discussed aspects of process safety management. In the process industries, the application of a SIS is most of the time only one of many safeguarding measures. As part of the PSM activities, the application of a SIS needs to be integrated into the overall strategy of all safeguarding measures. Therefore, the concepts of applying the safety lifecycle model needs to be implemented into the SMS.

Section 5.4 introduced the basics of system theory of control engineering. These basics form the building blocks of controlling safety-related business processes. Presumably the most important control parameter is the quality level of the safety-related information. Various information flows might be needed as input to a particular lifecycle phase in order to be able to correctly carry out the subject safety-related activities. Therefore the quality of safety-related information flows directly influences the quality of the safety-related activities and thereby the degree to which the specified objectives of that particular lifecycle phases can be realized.

Currently, standards on the application of a SIS only give a description of the inputs (among other things input information) and outputs (among other things output information). The MIR concept as described in the previous section gives guidelines to the classification of quality levels of reliability-related information flows. Application of

the MIR concept in the consumer electronics has proven that this theory is a valuable means to analyze and solve reliability-related business process problems.

5.6.2 Further research on qualification of safety-related information

Contemplating the research questions as discussed in Chapter 2, at this stage it is questioned whether and how the MIR concept as developed for and applied in the area of reliability management, could be adapted to control the safety-related business processes. As discussed, particularly concerning the safety-related information, the MIR concept is expected to be a suitable basis for the measurement and control of the quality of this information. Therefore, in line with these research questions, this thesis will particularly concentrate on classification of safety-related information. Next to the earlier defined research questions, a fifth question, which concerns the applicability of the MIR concept in the area of process safety management, could be added.

— Research question 5

Assuming that safety-related information can be qualified, how should this be done?

Subsequently, criteria will have to be defined in order to distinguish the different quality levels. Consistent and reproducible application of the analysis of information flows of the safety-related business processes, as based on the criteria to be defined, requires a certain degree of formalization. Therefore a formalized analysis technique needs to be developed, as will be described in Chapter 7.

Although the fact that the MIR concept itself is still subject to research developments, this concept will nevertheless be considered as established. Therefore, the theory based on which the MIR concept is developed will not be further researched in this thesis. What will be considered, is the applicability and usability for the control of safety-related business processes, and possible required adaptations to the MIR concept with regard to this.

The expected added value of classification of information flows is better handling and control of that information. Classification brings along that a better understanding is created concerning the specific need of that particular information. Consequently, sources where this information is created and sources where this information is needed are expected to be easier to allocate, together with easier establishing the medium that is used to transfer the information between these sources.

As a result of this, classification of information flows is expected to improve the process of implementing safety lifecycle models into the PSM. The formalized Safety Lifecycle Management (SLM) analysis technique, to be developed, is intended to become an additional means to measure the performance of the PSM and its safety-related business processes. Experiences, both with MIR assessments in the consumer products industry, as well as experiences, as gained during many SMS assessments, will be incorporated in this analysis technique. Case studies will be carried out to test the power of the developed SLM analysis technique.

The following chapter will introduce the principle of safety lifecycle management, where the ‘performance indicators’ of an activity and interaction of safety-related activities, are described.

Chapter 7 will describe the formalized analysis technique to assess a SMS with regard to the application of safety-instrumented systems. This formalized analysis technique should indicate the degree to which a safety lifecycle model is implemented into the SMS, and the degree to which the safety-related information flows are correctly controlled. Particularly concerning the development of this analysis technique and the definition of degrees of implementation, the MIR concept is considered to form the basis. Chapter 6 will not yet discuss the utility value of the MIR concept.

6 Safety Lifecycle Management

This chapter will in more detail describe the business process aspects of safety management. To be able to measure and analyze the safety-related business processes, two models, SAM model (Safety-related Activity Management model (not be used confused with the Safety Argument Manager [Kel99])) and SLAM model (Safety Lifecycle Activities Management model) are developed and defined in this chapter. These two models describe the involved safety-related activities and their characteristics. These characteristics are transformed into measurable parameters, which influence the performance of the involved safety-related activities.

The term Safety Lifecycle Management (SLM) is defined as a type of safety management that is based on the SAM and SLAM modeling concepts.

Finally two fundamental control concepts of safety lifecycle models are discussed.

6.1 Introduction to the management of safety-related activities

6.1.1 Introduction

In every day use, the term management is applied in many different contexts. With regard to process safety, the term management is best compared with another term, namely control. To achieve process safety, the safety-related activities need to be controlled. Accordingly, the terms management and control are split up into a number of aspects they should possess. These aspects, or steps, are in a logic order described as follows:

- *Measurement* of the momentary performance of the safety-related activities. Relevant parameters need to be measured to obtain a clear overview of the actual safety performance (e.g. to check if due to changes the safety performance has improved).
- *Analysis* of the measurement result. To understand the background causes leading to the measured performance of the safety-related activities, the results need to be analyzed and influencing factors need to be determined.
- *Determine* improvement strategy. Once the analysis results have revealed the background causes of the safety performance of the safety-related activities, decisions shall have to be made on how to improve the safety-related activities. (Assumed that their current performance is not acceptable and needs to be improved).
- *Implementation* of improvements. To take care that the improvement strategy is successfully implemented an appropriate set of improvements need to be defined and carried out.

As described in Chapter 2, one of the objectives of this thesis is to develop a description of the mechanism and construction of a model that supports the first two management steps. Such a model can support the measurement and analysis of safety-related business processes and, as such, can be applied on any randomly chosen company or organization. As described in Chapter 2, the latter two management steps are left out of the scope of this thesis. It depends on the particular circumstances, what the most appropriate improvement strategies and actions are. Nevertheless, the resulting model inarguably impacts these latter steps and generic conclusions on improvement strategy and actions will be drawn.

This section will discuss the objective and aspects of safety-related activities. Based on these aspects, in Section 6.5, the SAM model will be developed in order to control these activities.

6.1.2 Relationship between fault management and safety-related activities

During the course of the defined life span in which safety is a matter of concern, all sorts of different failures may occur [HSE95]. (IEC 61508 defines a fault as an abnormal condition that may cause a reduction in, or loss of, the capability of a unit to perform a specific function. A failure is defined as the termination of the ability of a functional unit to perform a required function. These terms are often mixed up. Fault management aims at the prevention of faults that might result in a failure of the considered part.) These failures are categorized into various types of typical problems that can happen during particular phases of the lifetime. In addition, a failure can also be classified according to its specific character: technical, human, organizational, etc. [Sch92]. Process safety management is therefore not infrequently expressed as fault management [Kem98].

To achieve safety during the entire lifetime, various activities need to be carried out to prevent any potential failures. Standards like IEC 61508 and ANSI/ISA S84.01 could be considered as a collection of requirements. If all requirements are correctly implemented, the conclusion is that compliance with such a standard is achieved. As discussed in Chapter 4, these latest standards make use of lifecycle models to structure and allocate the requirements. The objective of each requirement as part of such a standard is to prevent the occurrence of a fault, which may result in a hazardous event. Companies, plants and organizations, who have decided to implement these standards, need to adapt their business processes and implement requirements of standards. This brings along that a shifting takes place from fault management into requirements management, and from requirements management into management of business processes or management of safety-related activities.

6.1.3 Role and scale of safety-related activities

The success of a safety-related activity depends on the quality of the performance of the activity itself and on the quality of its input (e.g. necessary information), in order to result in the required quality of the output. Before a safety-related activity is analyzed, it is important to create a level of understanding of the scale of such an activity. On a macro level, PSM itself could be considered as one all-embracing activity, where at the same time, on a micro level, maintenance of an Emergency Shut Down valve (ESD valve) could also be considered as a safety-related activity. The following two examples are elaborated to illustrate the similarities and differences between a micro level activity (e.g. a HAZOP study), and the macro activity (e.g. process safety management).

Parchomchuk [Par 00] clearly describes the keys to successful Process Hazard Analysis studies (PHA) (a HAZOP study is a kind of PHA). The aspects include management, expertise, methods, and process safety information. Figure 19 shows the HAZOP activity together with its input and output. Obviously, the quality of the output depends on the quality of the input and the quality of the activity.

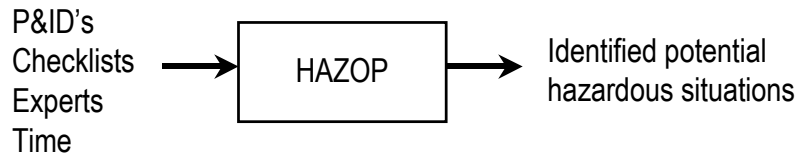


Figure 19 HAZOP, a safety-related activity

Whereas the HAZOP study is characterized as one single safety-related activity, process safety management is interpreted as the complete collection of safety-related activities required to achieve safe operation of the involved process installation during its entire life span. Once again, Figure 20 illustrates the activities relating to process safety management, and the required inputs, such as documentation and information, methods and tools, human resources, expertise, standards, and the safety management system. The output is a process installation that operates safely during its entire lifetime. As is the case for the HAZOP activity, the success in achieving the desired output depends on the quality of the input and the quality of the activity.

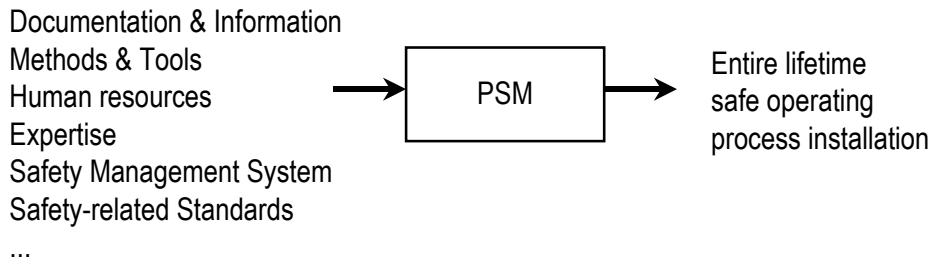


Figure 20 PSM, a collection of safety-related activities

Contemplating the two different levels of the safety-related activities, on a macro level (the PSM activity) and on micro level (the HAZOP activity), the capability to realize process safety for an entire life span depends on the quality of each single safety-related activity on micro level. (Apart from the fact that validation activities are performed to detect failures or problems in earlier phases.)

One of the aspects which contributes to the quality of process safety management is the level of suitability and availability of output information for one particular activity which is then to be used as input information for the next safety-related activity. Management of the collection of safety-related activities on micro level, by means of input control, activity control, and output control is considered as the basis for safety lifecycle management.

The definition of a safety lifecycle model offers a framework in which the required safety-related activities are allocated. This framework helps to structure applicable safety requirements. For this reason, the safety-related standards, as discussed earlier, have assigned safety requirements to specific phases of the standard safety lifecycle.

The implementation and management aspects of safety lifecycle models will be discussed in the following sections.

6.2 Elementary lifecycle management aspects

As discussed in the previous chapter, a complete lifetime safe operating process installation is only achieved if the involved business processes are properly controlled. With regard to this conclusion, a priori the following questions arise:

1. Which business processes are part of the IEC 61508 Overall safety lifecycle and need to be controlled?
2. What are the criteria to establish proper operation of each business process?
3. How is the relationship between these business processes implemented?
4. How is the operation of these business processes validated?

A SLM model (Safety Lifecycle Management model) will be defined that can be used as a means to find the answers to above-mentioned questions. The derivation of this SLM model is the result of combining two other models namely the SAM model (Safety-related Activity Management model) and the SLAM model (Safety Lifecycle Activities Management model), which will be discussed in the next sections.

6.3 Scope of the involved lifecycle management activities

The importance of a clear and unambiguous definition of the scope of the involved SIS-related activities, concerns its fit into the more comprehensive involved business processes with respect to other safety-related activities, which also include other risk reduction measures or even non-safety-related activities (e.g. quality-related activities). For instance, a risk assessment is considered as a safety-related activity of a specific phase in the discussed safety lifecycle, but in practice, many companies perform more than one session of risk assessments. It depends on the design stage of the involved process installation whether the risk assessment is performed to determine design changes to realize an inherently safe installation, or whether the risk assessment concerns the determination of additional risk reduction measures such as a SIS. Especially concerning borderline cases like HAZOP studies, clear definition of the scope of the involved safety-related activities prevent the possibility that certain crucial activities are overlooked [Kle99].

As described in Chapter 4, the latest SIS related standards have defined a safety lifecycle and require that such a safety lifecycle is implemented into the SMS. This thesis focuses on the management of the SIS. As indicated before, special attention will be given to the IEC 61508 Overall Safety Lifecycle for the reason that this lifecycle is the most comprehensive one with regard to the lifecycles of ANSI/ISA S84.01 and IEC 61511.

6.4 Development of the lifecycle management model

Although SIS related standards require the definition and application of a safety lifecycle model, these standards do not insist that exactly the same lifecycle model as specified in the standard shall be adopted. Obviously, all requirements with regard to achieving the objectives of each lifecycle phases shall be correctly implemented. This implies that it is the responsibility *and* freedom of the involved organization to define a safety lifecycle model that is best suitable to the specific circumstances.

A safety lifecycle model consists of a sequence or string of safety-related activities. Furthermore however, it is very well possible that at the same time, more than one activity is being carried out. In theory this might result in a situation that at any random moment in time, more than one activity is being carried out. Such a characteristic of overlapping activities means that possibly no distinctive moments exists that a first set of activities is finished before a following set of activities is started. If however, such distinctive moments exist, they could subsequently be interpreted as being the boundaries of phases of the involved safety lifecycle.

At this stage, based on the overview of all safety-related activities, a first subdivision needs to be made. The involved safety-related activities need to be grouped in order to determine which and how many phases are to be distinguished, and how the safety lifecycle model is chronologically composed. Subsequently two aspects need to be considered which impact the overall safety performance.

- What determines whether a safety-related activity is successfully carried out?
- How are necessary information flows between safety-related activities realized?

The first aspect is in detail discussed and addressed by the definition of the Safety-related Activity Management model (SAM model). The second aspect is dealt with by the definition of the Safety Lifecycle Activities Management model (SLAM model). The next sections will detail these two models.

6.5 Safety-related Activity Management model

6.5.1 Fundamentals of activity management

As discussed in the previous chapter, the quality of the inputs and the quality of the mechanism that is responsible for the transformation, determine the performance of a process and thus the quality of the output. With regard to safety-related activities, the quality of the output depends on a number of inputs and the characteristics of the transformation itself. Obviously, it is important to determine which inputs are required and which characteristics the concerned safety-related activity needs to have. Based on the above, to properly describe a safety-related activity, it would be a first step to make a division between inputs and transformation mechanisms. The model described in this thesis, however, may also consider on a meta-level, inputs as well as transformation mechanisms as inputs.

For instance, during a safety integrity level classification (safety-related activity), the required safety integrity level of the safety-instrumented systems shall be determined. The transformation may be carried out by the application of e.g. a risk matrix or by a risk graph [IEC61508]. The quality of this activity depends on the quality of the input information (e.g. HAZOP results), and the quality of the transformation (e.g. risk graph). This risk graph however could be considered as being a tool or methodology and could therefore be considered as a kind of input. The SAM model applies this approach and visualizes inputs as well as transformation mechanisms as ‘ingoing flows’. Ishikawa or fishbone diagrams give a commonly applied graphical presentation of this approach (see Figure 21).

A subsequent division that has to be made concerns the categorization of the inputs. Based on the fact that many safety-related activities might need to be carried out and all these activities have their own typical inputs, it is obvious that many different inputs can

be distinguished. The application of the SAM modeling concept is intended to be generic and therefore applicable to different processes and circumstances. Therefore the SAM modeling concept will be restricted to the definition of a limited number of categories of inputs. The categorization criteria that can be applied are by definition subjective, but are nevertheless based on the categories as defined by IEC 61508 and alike standards such as the ISO 9000 series.

Although it is concluded that the categorization is by definition subjective, it is assumed that the specified categories cover all relevant inputs. A second important statement is that a safety-related activity can only be successfully carried out if all inputs of all defined categories are allocated. At the moment that with regard to a particular input category no input is allocated, the safety-related activity can not be carried out properly. This immediately illustrates the added value of applying the SAM modeling concept, if a relevant input is lacking, this will be immediately diagnosed. Based on such a diagnosis, a corrective action can be taken.

6.5.2 Determination of SAM modeling parameters

In order to define appropriate input categories, a general question could be considered namely: ‘What determines whether a certain safety-related activity will be carried out at all?’ The subsequent question will be: ‘What determines whether this activity is carried out successfully?’

Literature on management of organizations [Min92], often starts with general questions, such as the well-known W-questions. A non W-question that is added concerns ‘how’.

- Why needs a safety-related activity be carried out?
- When should it be carried out?
- What are the required inputs to the activity?
- What is the desired result of the activity?
- Where should it take place?
- Who are the people that should carry out this activity?
- How is the safety-related activity performed?
- How is the result of the activity validated?

With regard to reliability-related activities, such questions can be applied to determine relevant input categories. Brombacher [Bro00] distinguishes 4 input categories, namely:

- Company mission
- Capabilities development/production
- (Expected) customer wishes/demands
- Material properties

IEC 61508-1 clause 7 describes the Overall safety lifecycle model and an overview table with generic aspects to be allocated for each lifecycle phase. These aspects are:

- Objectives
- Scope
- Requirements
- Inputs
- Outputs

Based on the above discussed W-questions, the categories distinguished by Brombacher, IEC 61508 and the experiences of the author gained during his site visits, a deduced set of input categories is defined as represented in Figure 21.

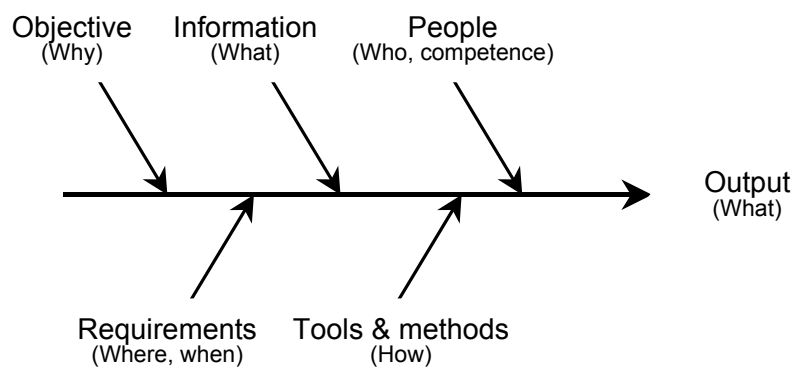


Figure 21 Ishikawa diagram showing input categories resulting in the output

The Ishikawa diagram of Figure 21 appears to be an excellent method to graphically illustrate the relationships between input parameters and output parameters. However, what is not shown in such a diagram, is the transformation mechanism as described by the system theory using transformation boxes, inputs and outputs. Furthermore, it is experienced to be a complicated task to create Ishikawa diagrams describing all inputs and all outputs for each safety-related activity and combine them into one comprehensive model, which will become relatively complex and therefore subject to errors and shortcomings.

For these reasons it is chosen to not further specify detailed Ishikawa diagrams but to make use of the system model theory as described by Robbins [Rob90] as discussed in Section 5.3.

An additional advantage of the system theory is the ability to relatively easily combine system models into larger models and establish relationships between these models. These models are not restricted to singular output-input connections but offer the possibility to apply e.g. single outputs to multiple inputs on various locations. The Safety-related Activity Management Model, as described in the next section, will therefore be based on this system modeling theory.

6.5.3 Specification of the SAM model

The Ishikawa diagram of Figure 21, showed the main parameters that determine the output performance. This output performance is obviously the result of a particular activity or set

of activities. This Ishikawa diagram is further used to define the, from now on to be named, Safety-related Activity Management model (or SAM model). The SAM model parameters correspond with the defined clauses of IEC 61508 part 1. This part of the standard addresses the competence of persons, requirements on documentation and has defined a table based on the Overall safety lifecycle model. Furthermore, IEC 61508 has defined a large set of requirements to be implemented and has allocated a number of tools and techniques of which the standard prescribes which SIL these tools and techniques can be applied. As the result of the application of the SAM model together with the MIR concept, within a number of companies in the process industries (case studies 1 and 2, as described in Chapter 8), the SAM model deviates a little bit from the earlier presented Ishikawa diagram. The major difference is the splitting of the output into two categories, namely general output information (that is required as input for a successive activity), and output documentation (that needs to be stored as a track record of evidence material that the required safety-related activity is indeed properly carried out). The reason for this split will be explained together with the description of the categories.

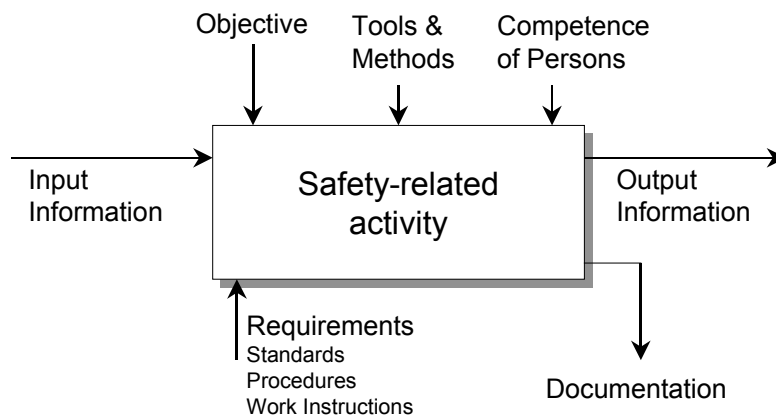


Figure 22 Safety-related Activity Management (SAM) model

In the box of Figure 22 the safety-related activity is located. To ‘safely’ carry out this activity, a number of aspects need to be controlled:

- Objective(s) : What is the purpose of the safety-related activity?
- Output information : What are the needed results, outcome or information?
- Competence of persons : Requirements concerning the competencies of the involved persons.
- Tools & Methods : Tools, methods, techniques, equipment and other aids.
- Input information : Required input information and documentation.
- Requirements : Limiting conditions, e.g. procedures and work instructions.
- Documentation : Any required information that needs to be documented.

Following, aspects will be described of each category concerning its quality characteristics. Because of the close relationship between input and output information (both are information and both may serve as input as well as output), and documentation (which is a form of container of information), these three categories are discussed together.

– *Objectives*

Without the existence of clear objectives, no safety-related activity will probably ever be executed correctly. Objectives that cover the scope of all the involved activities need to be defined. As PSM normally involves a high number of safety-related activities and many people are involved, it may be important to subdivide the overall objective (e.g. realize a safe operating plant with not more than one injury per 10 years), into dedicated objectives. Each of these dedicated objectives should cover the scope of the involved safety-related activities and indicate the relationship between other objectives and the relation to the overall objective.

The control of the resulting set of objectives will help to verify successful performance of each involved activity and it will help the communication between different departments, which each have their own specific objective as a department. (Case 3 of annex A illustrates the classical problem of two departments (in this case the HAZOP people and the instrumentation people) who both were perfectly motivated to achieve the dedicated objective of their department. Due to lack of adaptation of these two objectives to each other and due to lack of an association to the common objective that should be controlled by the manager of both departments, a serious mismatch existed, which resulted in an impossibility to implement the concept of safety integrity levels.)

A very important element of the defined objective should be the explanation of the reason why it is important to properly carry out such an objective. It will help the communication and motivate the involved people to take care that the objectives are achieved if they are aware of the relevance of achieving the objective and thus the relevance of properly performing the involved safety-related activities.

– *Competence of persons*

Although the technological developments result in growing automated systems, people are still involved in every phase of the IEC 61508 Overall safety lifecycle. Obviously, the level of competence of these people strongly depends on the availability of all kinds of tools and methods. If, for example, during the SIL validation a reliability calculation needs to be performed, the level of expertise may vary, depending on whether such calculations are performed manually (e.g. applying the Markov modeling technique) or by using a specific software package. Requirements on competence of persons concern their basic schooling and education (qualifications), specific courses and training programs to be followed, their expertise and experience. Besides competence, also responsibility or accountability needs to be addressed. According to the CCPS ‘accountability’ is the obligation to explain and answer for one’s actions that are related to company expectations, objectives, and goals. Accordingly, it is a powerful element of an effective SMS. Accountability begins with a clear, explicit, and reasonably specific statement of a company’s expectations, objectives, and goals. Reasonable specificity is needed to avoid situations where goals are so general that they become subjective and confusing [CCPS89].

A SMS falters when individuals who have production or other responsibilities that have an impact on process safety are not explicitly assigned responsibility for process safety matters. Accountability for the continuity of process systems in terms of obtaining the resources and funding needed for adequate process safety, should involve a level of management beyond the process unit in question. This can be accomplished by assigning process safety accountability to various job functions or units for each phase in the lifecycle of a process system, from design to demolition [CCPS89]. For

example, a person who is responsible for maintenance and testing of a fuel pump may need to follow a dedicated training program and be certified to be allowed to do such kind of maintenance.

The disaster at the Thai Oil refinery in Thailand, in December 1999 illustrated how things can go seriously wrong if operators are not qualified and not aware of the impact by ignoring alarms, etc. [Tha99].

- *Tools and methods*

The relevance of applying the correct set of validated tools and methods is probably best emphasized by the establishment that during each phase of the IEC 61508 Overall safety lifecycle, tools and methods need to be applied. This may vary from the application of a checklist during the HAZOP study, to the use of SIS development software package, or to the use of calibrated maintenance and test equipment. The relationship between the use of tools and methods and the competence of the people who need to apply them is already shortly discussed in the previous section and should therefore be considered in relation to each other. It is obvious, that in case a dedicated safety PLC is applied as logic solver of a SIS, the operators who have to work with this PLC need to follow a specific training course on how this PLC should be operated. At the moment that such a PLC becomes replaced by a new generation PLC's, once again a specific training course should be followed.

- *Requirements*

The Safety-related Activity Management Model of Figure 22 shows the category 'requirements' with subscripts namely standards, procedures and work instructions. Although the SAM model deviates from the SIS standards from focusing on requirements control to the control of business processes, it nevertheless remains important to take care that standard requirements are still properly implemented and complied with. As it is also described as part of the category 'information and documentation', compliance with specific standard requirements is an important element to prove that good engineering practice is applied and thereby a correct operating SIS is realized. Many companies (e.g. the company described in case study 11 of annex A) have implemented an integrated quality system and safety management system. Such a system is characterized by the fact that requirements of standards like the ISO 9000 series as well as the requirements of safety-related standards like IEC 61508, are implemented into this singular system [Kne99a]. In daily practice, the requirements of these standards are translated into usable procedures or instructions. These procedures and work instructions are characterized by the fact that they are adapted to the particular application and environmental circumstances. This results into a situation where generic (sometimes very abstract) requirements are transformed to a level that is better understandable by the people who have to obey them.

- *Information and documentation*

As discussed above, good arguments exist to split the output into 'information' and a separate category of 'documentation'. The CCPS is very clear on this: "*Preserving and making available the knowledge within a company are both important for process safety for a number of reasons, including preserving a record of design conditions and materials of construction for existing equipment, which helps assure that operations*

and maintenance remain faithful to the original intent.” The management system for process risk management decisions must be designed to capture information that describes not only what decision was made but also why it was made. However, if the reason for having adopted this practice is not documented, later generations of supervisors may resurrect ineffective alternatives, not knowing that they have already been tried. In addition, while it is important to know the current status of the operation, it is also important to be able to look back and learn from the operation’s history to improve process safety continuously [CCPS89].

The importance of appropriate categorization of output information and documentation is probably best done by describing the different types of information and documents that were allocated during the second case study as described in Chapter 8. First of all, it is important to mention that a document is normally considered as a kind of information source. Information flows can be realized by a number of communication means, of which the distribution of documents is only one kind. Other examples could be verbal communication e.g. during meetings, films or videos, computer interfaces like monitors, etc. The physical characteristics of information flows are therefore aspects that should be considered when information flows are implemented or analyzed. A completely different subdivision of information flows relates to the difference of its particular purpose. Again, a number of purposes are distinguished, leading to the following overview:

- Input information that is required for the activity.
- Generated output information that is required (e.g. as relevant input for a successive activity).
- Output information that is applied as feedback to optimize the involved safety-related activity or as feedback to earlier carried out activities, of which the output is inputted into the concerned activity.
- Output information that is stored into a database and serves as a kind of track record as evidence that the involved activity is properly carried out and the applicable standard requirements are correctly implemented. Such a database of documents may serve as the basis for safety assessments to verify standard requirements and to see whether the standards are complied with. Such a proof may be required to obtain a license to operate and to demonstrate that a ‘safe’ operating plant is realized. This might be required by the authorities, which periodically may check the process plant. A second group of interested parties concerns the insurance companies. Particularly, the smaller companies in the process industries pay a yearly insurance premium of which the height may depend on whether certain standards are met. The last argument concerns the situation in which a hazardous event has occurred. Proper documentation will in that case serve as the ultimate proof that every measure had been taken (good engineering practice) to realize a safe operating plant. This may impact the number or height of claims, in case of people are injured or killed or in case of pollution the environment.

The degree of how successfully a certain activity is performed is obviously not entirely restricted to the quality of the available information. If, for instance, the person who is responsible for the execution of a particular activity is not motivated (for what ever the reason may be), this may seriously impact the quality of his performance. (Together with the level of expertise, experience, training and education, influence his or her

performance.) This thesis will not discuss psychological aspects, such as motivation of employees and the relationship with their personal performance, although it is recognized that psychological aspects often play an important role.

6.5.4 Application of the SAM model

To control safety-related business processes, the involved activities need to be identified, their scope and objective needs to be defined and the success factors concerning inputs and outputs need to be addressed. If one of the SAM modeling categories is not properly addressed, the probability may dramatically increase that the concerned activity is not carried out as required, or may not even be carried out at all. This will impact the final performance. Verification activities should take place at the right moment in time to allocate any possible shortcomings. (Such kind of verification activities and assessments are likewise required by standards such as IEC 61508 and IEC 61511.)

6.5.5 Recapitulating the SAM model

The SAM model can be perfectly applied as a means to implement safety lifecycle models into the safety management system and achieve compliance with standards by controlling the activities, their objectives and requirements. Furthermore, the SAM model can be used as a means to analyze the individual fundamental activities as part of safety-related business processes. Case studies, as described in Chapter 8 and annex A, will illustrate the added value of using the SAM model as the analysis method.

An important aspect that is not considered in detail, concerns the relationship between the various safety-related activities. Obviously comprehensive lifecycle safety of a SIS is only achieved when *all* safety-related activities are properly carried out, something which can only be realized if the interaction between these activities is controlled as well. The next section will describe the control concepts of activities, which are related to each other, for instance because their inputs and outputs are connected. These concepts are incorporated into the development of the Safety Lifecycle Activity Management model as will be defined in section 6.7.

6.6 Development of the Safety Lifecycle Management concept

6.6.1 Definition of Safety Lifecycle Management

As required by standards like IEC 61508 and IEC 61511, a safety lifecycle shall be defined and implemented into the (existing) Safety Management System (SMS). To comply with such a requirement and to be able to actually implement this requirement, one should have a good understanding of the definition of a SMS. During the years that the author was, as a consultant, involved with the implementation of IEC 61508 within the organizations of end-users of the process industries and thus end-users of safety-instrumented systems, no clear and explicit definition of a SMS was observed. Nevertheless, to be able to help these end-users a definition was formulated by a group of experts within the Honeywell Safety Management Systems organization. This definition has clear similarities with the definition of a quality system as described in standard ISO 8402 [ISO8402]. A safety management system is thereby defined as follows:

The organizational structure, responsibilities, procedures, processes and resources to carry out all activities related to safety of people, preservation of the environment, and the prevention of capital and operational loss. It concerns safety-related activities carried out at all stages of the lifecycle of the considered company, plant, installation or product.

As the result of the new approach that managing technical aspects shall be realized through management of the business processes which make use of safety lifecycles, a definition of Safety Lifecycle Management (SLM) is added:

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.

The term safety lifecycle management does not originate from existing literature or standards, but is brought into use by the author. SLM is best interpreted as the combination of the terms ‘PSM’ and ‘safety lifecycle’. Its characteristic is that, as a result of appropriate PSM, the safety lifecycle model is successfully implemented into the SMS. Obviously such an implementation, together with the control of the safety lifecycle, is only achieved if the emphasis is put on the control of the involved safety-related business processes.

Next, the relationship will be discussed between the various safety-related activities and the importance of proper information control. Similarities between SLM and the MIR concepts will be revealed and the applicability of the MIR concept will be established. Section 6.7 will introduce the Safety Lifecycle Activities Management model as a methodology to analyze the SLM related business processes.

6.6.2 The SAM model, the building blocks of SLM

Comprehensive lifetime process safety will depend on the weak links of the safety lifecycle. One can imagine that in case the potential hazardous situations are not accurately identified and appropriately documented, it will have a serious impact on the quality of the following risk analysis. If, subsequently, a lot of effort is spend on the specification of the safety requirements, this will not result into a significant increase of the finally achieved safety level during the operational lifetime of the process installation. (The risks of a number of hazardous situations are not analyzed and risk reduction measures are not defined.) It is for these reasons that a well-balanced effort, time and expertise should be spend on each safety-related activity as part of the overall safety lifecycle. (Obviously, first of all, it is of essential importance that *all* required safety-related activities are identified.) Furthermore, an appropriate communication system of safety-related documentation, information, procedures and work instructions, needs to be in place to take care that all safety-related activities can be performed correctly. From this point of view it is concluded that all involved safety-related activities play an essential role in the achievement of safety of the process for its entire lifetime.

6.6.3 The importance of the control of SLM-related information

The importance of having realized the required information flows is one of the most essential elements. The success of achieving the objective of a particular safety-related activity depends almost completely on the availability of the required input information. Especially, in case the earlier mentioned ‘w’ questions are considered, the general establishment is that these questions typically ask for a certain kind of information. (This also applies to the added question ‘how’.) The need for control of information sources and information flows to assure the availability of required safety-related information, could therefore be considered as the glue (or cement) between the SAM model building blocks. What is considered as being relevant information, concerns for instance information on the required competence of persons which are responsible for the involved safety-related activities. Also information flows, concerning the explanation why a particular activity needs to be carried out, may directly impact the achieved performance. This kind of information flows do not only help the employees to better understand the need of carrying out the activity, but indeed may also motivate the people involved. Obviously, the added value of appropriate control of information flows is not only related to ‘streamlining’ the safety-related business processes, but may also have psychological influences. (The term ‘information’ should therefore be considered as a kind of container term.)

A striking example of how things can go terribly wrong is the Piper Alpha disaster [Hon90]. An oil and gas producing platform in the North Sea was destroyed by a devastating fire due to an ignited gas leak. This gas leak was caused by the activation of a pump which was actually under maintenance at that time. The information that the pump should not be used, was put on the desk of the operator in charge, but did not attract the attention of this operator, maybe for the reason that the concerned maintenance document was ‘hidden’ between a pile of other papers. Information was ‘sent’ but not ‘received’. Section 7.3 will further elaborate on the management and control of safety-related information.

6.7 Safety Lifecycle Activities Management model

One of the characteristic points of the IEC 61508 Overall safety lifecycle model, is the limited amount of information given concerning information flows, responsibilities, activities, information and documentation sources, etc. These are considered to be company specific. The Overall safety lifecycle has, not surprisingly, an added note underneath the model stating: *‘Activities related to verification, management of functional safety and functional safety assessment are not shown for reason of clarity but are relevant to all Overall, E/E/PES and software safety lifecycle phases.’*

The concept to develop the Safety Lifecycle Activities Management model is for an important part based on the conclusion that graphical overviews of business processes appear to be an excellent means to analyze and control such processes. The development, characteristics and attributes of the SLAM model will be described and explained by a step by step approach. As earlier mentioned, the SAM model forms the fundament of the development of the SLAM model. The first development ‘step’ is therefore the connection of two consecutive safety-related activities.

Step 1: Identify required connections of input and output information flows

Probably the most relevant aspect of SLM concerns the allocation of required connections between the identified output information flows and identified input information flows. Figure 23 illustrates such a connection between two phases M and N. It may very well be the case that one output is needed as input at more than one place to be able to carry out several activities. Also the opposite is imaginable, e.g. during the validation a lot of information from various sources is needed to properly conduct such a validation. Scan methods, such as checklists, could be applied to systematically determine necessary connections.

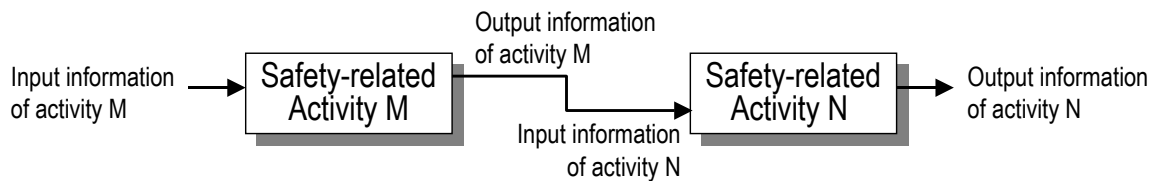


Figure 23 Information flow from activity M to activity N

Obviously, the quality of the output information of activity M determines the quality of the input information of activity N. Therefore, the offered output information of activity M will have to meet the requirements of the input information of activity N. Techniques that are applied in the field of quality control, like Quality Function Deployment and the Houses Of Quality [Sul86], have proven to be excellent means to translate customer demands into product requirements. Obviously, similar transformation processes are required to translate e.g. risk assessment results into the specification of safety measures. Information that is produced during the HAZOP study, like Cause & Effect diagrams are needed as input for the determination of the required SIL. (As already mentioned, IEC 61508 has defined a table in part 1 with required inputs and outputs per lifecycle phase.)

Step 2: Identification of information sources

After having completed step 1, it could be very well that not all required input information flows are fully covered by the existing output information flows. It may very well be the case that additional information is required from sources outside the scope of the produced information of the involved activities (e.g. external information sources such as international standards or documentation of earlier developments, see Figure 24). Furthermore, as also discussed during the description of the SAM model, it might be needed to properly store information. Through the allocation of sources of information, it will be possible to determine whether these sources are truly accessible by the right persons.

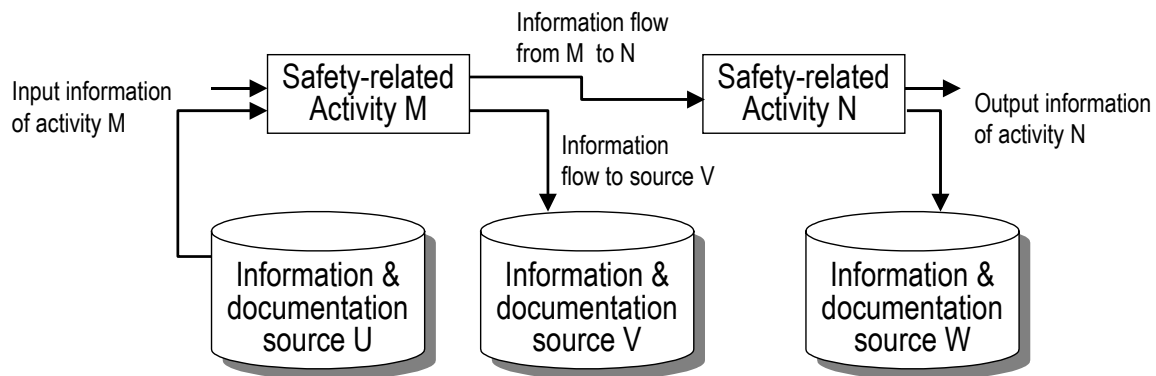


Figure 24 Identification of information sources

Step 3: Assign the people who need to be involved in the execution of a safety-related activity

Although this step could be considered as an aspect that is already addressed in the development of the SAM model, the added value to repeat this step is that persons, who are involved in more than one activity, can easily be identified. One way to realize an information flow is through communication of e.g. two persons who are involved in two successive activities. Another way is to involve one or more persons from one activity into the execution of a successive or preceding activity. Figure 25 illustrates the involvement of people.

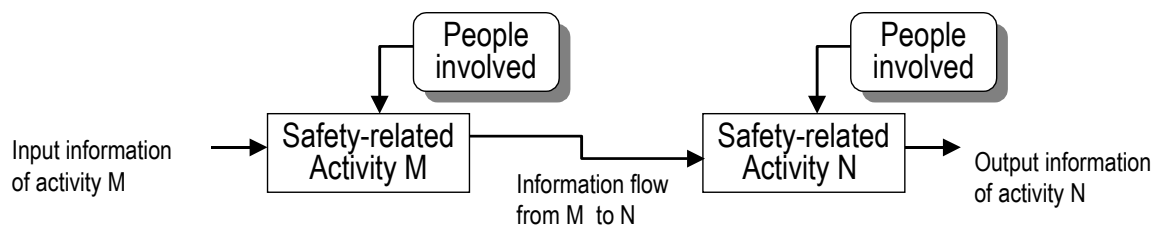


Figure 25 Allocation of involved people

A good example of how such an assignment and allocation can be realized, was established during a SIS related SLM study at a chemical plant in the Netherlands (See also case 2 of Chapter 8). It appeared that a diverse team of experts with different backgrounds carried out all safety-related activities. It also appeared that a substantial part of these teams were overlapping each other. In fact, it was concluded that a 'single' team carried out the succeeding activities, which was adapted during the course of time. The composition of these teams could be found on the local computer network. This computer network was accessible by all employees.

Even though the corporate standard on the application of SIS did not deviate significantly from a number of other company's standards, the company is considered to have realized highly safe operating plants. (One of their slogans is to be the safest company in the world.) Track records of accidents indeed show a highly safe operating level. This may be attributed to amongst others the use of overlapping teams.

Step 4: Determine the persons who are responsible for the definition of the objectives and the execution of the safety-related activities

Especially in the field of SIS, it appears that the technical experts make important decisions on these kinds of systems. It is not unusual that the technical experts become a kind of guru and their superiors fully rely on their knowledge and wisdom. In that case, it then depends on the local circumstances and culture whether these experts (who most of the time run their own department), cooperate in an integrated manner. It may in certain cases be necessary to explicitly assign and allocate the person who is responsible for both departments and who takes care that the general objective of SLM is achieved. (E.g. the Health Safety and Environment (or HSE) manager, as illustrated in Figure 26.)

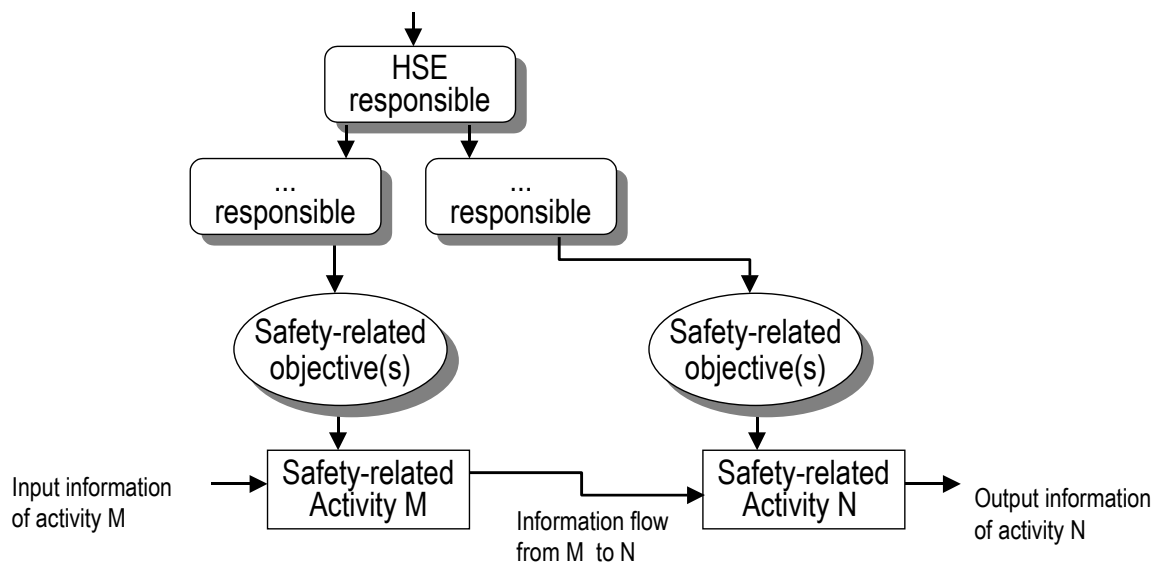


Figure 26 Relationship between people and safety-related objectives

During an introduction course on IEC 61508 at a fertilizer producing plant in Canada (See case study 3 in annex A), it appeared how the presence of different departments with both their own experts can lead to conflicting interests. The author was invited by the head of the instrumentation department, together with people from the HAZOP department. At a certain moment, the concept of safety integrity levels was explained, and it was emphasized that it was of essential importance that the people from the HAZOP team adapted their risk assessment procedures in such a way that for each defined safety-instrumented function, a required SIL would be determined. It appeared that the people from the HAZOP department, at that time, were not motivated at all to collaborate. Collaboration would in their eyes implicate that their current procedures were inadequate. The fact that their (common) manager was not attending this discussion, was experienced as a serious lack to be able to solve this problem.

Step 5: Allocation of lifecycle phase boundaries

The fifth and final step concerns the allocation of the boundaries of the lifecycle phases. The reason to take this step at the end, is because of the fact that the grouping of safety-related activities should not be purely based on the common characteristics, but should also be based on the common objectives, sources of information, the people that are involved, etc.

The added value of performing step 5, is that it results in a framework of lifecycle phases and therewith brings order and overview into the, often complex, relationships between the many safety-related activities. Subsequently, verification and assessment activities will become easier.

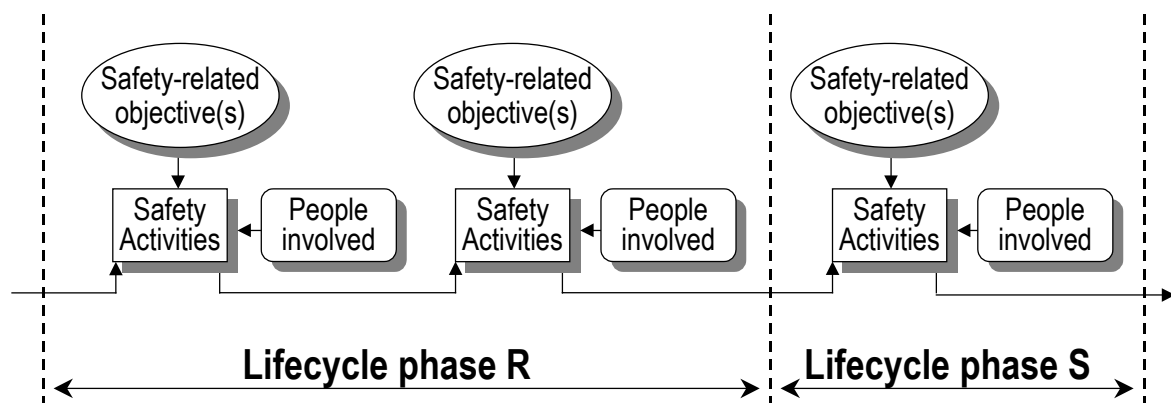


Figure 27 Allocation of lifecycle phase boundaries

Until so far, the two defined SAM and SLAM models could still be considered as being theoretical principles of Safety Lifecycle Management. The question that subsequently arises, is how organizations might implement these models. This will obviously depend on the organization structure, hierarchy, culture and history. The following section will therefore describe two different basic organizational models and discuss their advantages and disadvantages with regard to the ability to implement the SLM principles.

6.8 Organizational structures and the SLM concept

As discussed in the introduction of this chapter, it is of essential importance to thoroughly discuss and plan the organizational aspects that will affect the efficiency and effectiveness of the applied technical safety measures. As discussed, a systematic approach is required to prevent various problems during all phases of the process installation, which could, in turn, result in a potentially hazardous situation. The repetition of previous occurred accidents, as well as 'new' dangerous situations (e.g. near misses), need to be prevented by systematic safety management. The organizational structure of a company influences its ability (the efficiency and effectiveness) with regard to the implementation of the SLM concept. This section will therefore discuss the most commonly applied management structures, as described by Mintzberg [Min92] and Kerklaan [Ker98]. These two models represent the so-called vertical or line management approach, and the horizontal or process management approach. Subsequently, the lifecycle-based management approach is discussed, which represents a kind of hybrid model of the vertical and horizontal approach.

6.8.1 Line management

A first concept to achieve total lifetime safety is the “line management approach” or “vertical approach”. This management approach is characterized by a clear, central organized structure of responsible persons who are responsible for specific objectives. This kind of approach intends to realize a profound relationship between various objectives. The intention is to bring the various objectives in line with each other. This is done by translating general management objectives into the objectives to be achieved at lower levels in the organization. Well-known techniques to achieve this are Policy Deployment, Management by Objectives and One-page management [Ker98]. This kind of management technique is often characterized as a top-down approach.

The organization is controlled by the primary responsible, for example the ‘health and safety manager’. A variety of experts on the multiple aspects of safety lifecycles are duly appointed and responsible to achieve safety-related objectives for the phases involved. In addition, a team of people is associated with the execution of the safety-related activities for that particular phase.

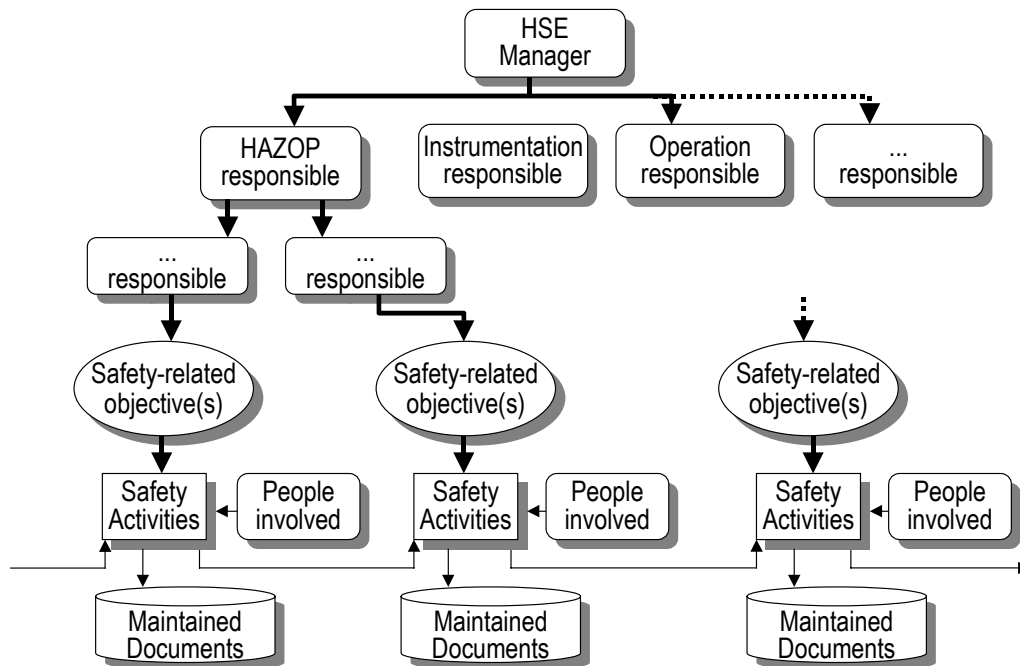


Figure 28 Line management, the vertical approach

Figure 28 shows the organizational structure of responsibilities of the people who are involved, in order to achieve the different sets of safety-related objectives. The vertical communication lines are clearly indicated by thick arrows and show their mutual relationships, which are determined and managed by the main responsible. The first case described in Chapter 8, illustrates an organization that is characterized by the vertical approach. Due to relatively frequent reorganizations, the people that are involved in the safety-related activities primarily focus on meeting the expectations of their superiors.

6.8.2 Process flow management

Elaborating on the definition of safety lifecycles, its phases, and related activities per phase, one way to achieve total lifetime process safety is by applying the business process oriented organization model or “horizontal approach”. This organization model is characterized by a sequence of groups of safety-related activities. The goal is to perfectly connect the inter-related activities. A well-know example concerns the Quality Function Deployment [Ker98]. Each group of activities is managed and carried out by people as part of one single team or department, and all of these people together aim to meet the needs of the inter-related activities. To successfully achieve this, the necessary information and documentation needs to be available. The final result of the involved activities subsequently results in new documentation and other output information.

The horizontal communication lines are clearly indicated by thick arrows and show the relationship between the different teams, which can be compared with the relationship between a vendor and a customer. Figure 29 shows the relationship between the different teams, their objectives and the required input- and output information and documentation flows.

As stated before, the success of achieving all the safety-related objectives largely depends on the presence and quality of the information and documentation flows. If output information is not (entirely) suitable as input information of the subsequent phase(s), this will have a negative impact on achieving the objectives of activities that follow.

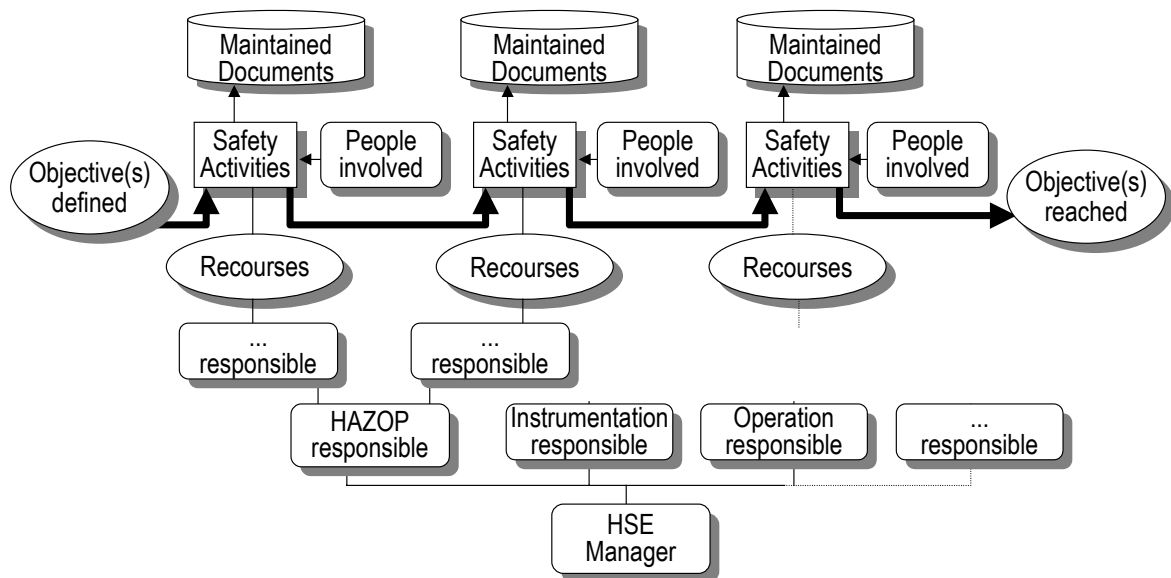


Figure 29 Process management, the horizontal approach

Quality systems usually comply with ISO 9000 quality standards, and are characterized by a process work flow oriented approach. To adapt the existing quality system and make it suitable for IEC 61508 certification, implementation of the safety lifecycle is required. The second case as described in Chapter 8 illustrates an organization that is characterized by the horizontal approach. The safety-related activities are performed by teams, which cooperate on the basis of a supplier–receiver principle.

6.8.3 Lifecycle-based safety management

The safety-related standards mentioned in this thesis, which demand the application of a safety lifecycle, do not prescribe *how* such a model should be implemented and managed. In practice, various models are applied to manage process safety. It is the challenge to manage a safety lifecycle based on their PSM model.

One of the starting points is to devote well-balanced attention to each individual phase in order to optimize the efficiency and effectiveness of process safety lifecycle management. In situations where much attention and effort is spent on the identification of potential hazardous situations, but hardly any on the definition of the safety requirements, one can easily imagine what the finally achieved safety level of the operating process installation will be. Poor communication can also have such an effect on plant safety.

The techniques that can be used to manage safety lifecycles largely depend on the integration of the involved lifecycle phases. Figure 30 shows a hybrid model of the process oriented and line management approach.

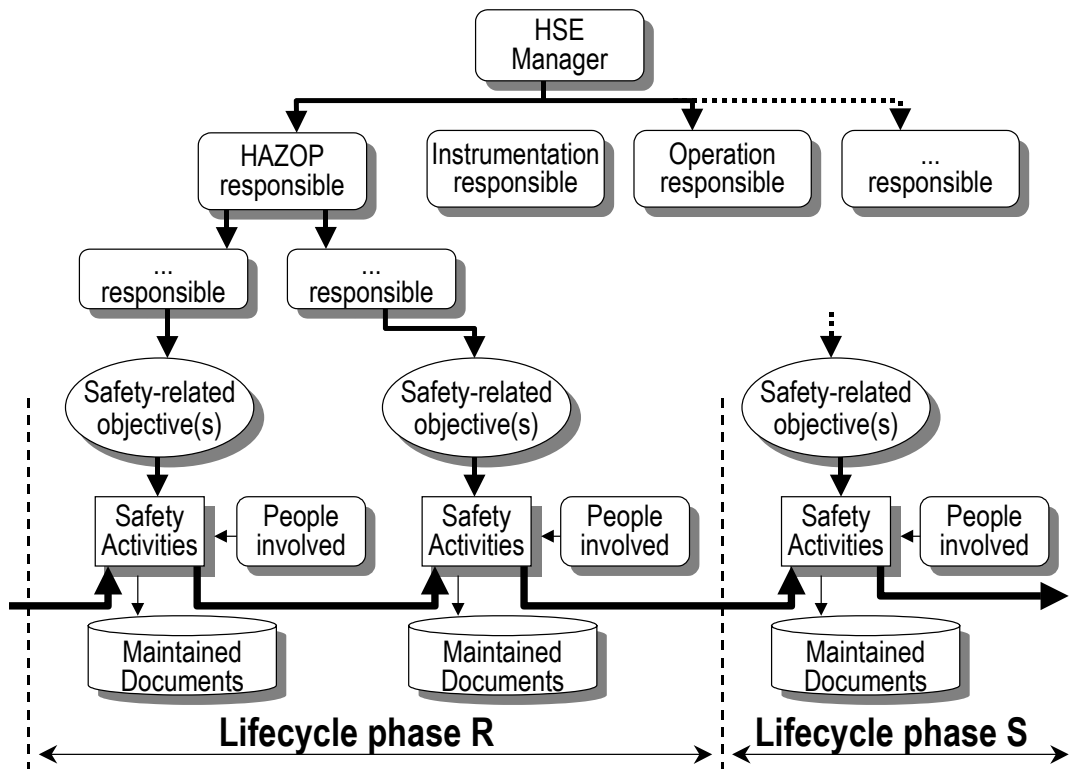


Figure 30 Lifecycle-based management approach

A first step to develop expertise on management of safety lifecycles might be through specific lifecycle oriented assessments of the safety management systems that are currently in place. Recent case studies indicate how safety lifecycles could be analyzed using dedicated flow chart techniques [Hee99]. However, these techniques are still characterized as being exploratory. The challenge is to enhance such techniques to a level where process safety can be managed using safety lifecycles on a proactive basis. Case 11 of annex A illustrates a company that has defined a safety lifecycle model and implemented that model into their organization.

6.8.4 Evaluation of the organizational structures

The previous sections discussed three types of control concepts, the line management, process management and lifecycle-based management approach. The advantage of the line management approach is the fact that clear understanding exists on the responsibilities for the involved safety-related activities. However, a disadvantage is that relatively little attention might be paid to making the output of the involved activities suitable as input for other safety-related activities. This disadvantage is better solved by the process management approach. A disadvantage of the process management approach, however, is that no clear overview exists of which persons are responsible for which activities. The lifecycle-based approach has therefore the advantage that much attention is paid to the identification and allocation of all involved and required activities as part of the complete lifecycle. Obviously, every real existing organization is characterized by specific aspects or by a mixture of the described organizational structures. This explanation is to alert organizations that at the moment a company decides to implement the SLM concept, it should be aware of these advantages and disadvantages.

6.9 Evaluation of the SLM concept

This chapter described the developed theory of the SLM concept. Firstly, a model to describe safety-related activities (the SAM model) has been defined. Subsequently, the SAM model has been integrated in the safety lifecycle model resulting into the SLAM model. The five steps that described the development of the SLAM model are intended to assist the process of adoption, implementation and control of the concept of SLM concept. The motive of the development of the SAM and SLAM modeling concepts is to better understand the actual safety-related business processes and offer the ability to allocate potential safety-related problems. Therefore, the SLM concept is considered to form a new fundament of the lifecycle oriented SMS and offer a new structure to control its related business processes. Finally a number of existing organizational structures were discussed concerning their advantages and disadvantages with regard to the implementation of the SLM concept.

This thesis will not further in detail analyze the advantages and disadvantages of the different organizational models. Although, at this stage, it is clear that many aspects concerning the implementation of the SLM aspects are not in detail discussed, this thesis will not further focus on these aspects. Instead, in the next chapter, the development of the formalized MIR-based SLM analysis technique will be described that can be used to analyze the safety-related business processes of the SMS. The contribution of this chapter is meant to serve as a basis to explain the purpose of and need for the formalized MIR-based SLM analysis technique, and thus what aspects of the business processes of the SMS shall be considered when applying this analysis technique.

As already discussed in Section 5.6.3, this formalized analysis technique should indicate the degree to which safety lifecycle models and thus the SLM concept is implemented into the SMS, and the degree to which the safety-related information flows are correctly controlled. Particularly concerning the development of this analysis technique and the definition of degrees of implementation, the MIR concept is considered to form the basis.

7 Development of a MIR-based SLM analysis technique

In this chapter the relationship between the SLM concept and the MIR concept as described in the previous chapters, will be discussed. Subsequently, a formalized MIR-based SLM analysis technique will be defined to measure and analyze the quality of the SLM-related business processes. The development of the formalized analysis technique is strongly influenced by experiences gained during various SMS analysis studies concerning the application of SIS's, and experiences acquired from earlier MIR studies. Based on a number of industrial case studies (described in Chapter 8 and annex A), the objective and added value of the application of the formalized analysis technique will be demonstrated.

7.1 The objective of a SLM analysis technique

Companies may have adopted different systems, strategies and policies to manage their process safety. Also with regard to the implementation of safety standards, different systems might be applied. A different approach may for instance be the result of difference in safety culture, the local safety legislation, the kind of process and differences in products. To develop a detailed plan to implement the SLM concept, is considered to be a dedicated and customized process, which is expected to be only possible if it is done company specific. Nevertheless, these companies obviously need to know whether their SMS appropriately has implemented the SLM concept and correctly has implemented the requirements from the lifecycle-based safety standards. Therefore, the development of techniques is needed to become able to 'measure' and 'analyze' e.g. whether the concerned 'plant' positively or negatively complies with lifecycle-based standards, and as a result of having adequately addressed the relevant SAM and SLAM modeling parameters. More precisely, it is the intention of the analysis technique to measure the quality of the safety-related business processes and, with that, reveal and allocate weak points which might entail a potential safety problem. Regarding the observation that the nature of these problems are mainly the results of the complexity of the business processes, the analysis technique to be developed, will particularly focus on the quality of safety-related information management. This kind of utilization of the analysis technique to be developed, could be considered as step I, as indicated in Figure 31. The second intended added value of the analysis technique is based on the principle of using these models to actually 'control' and 'improve' safety-related business processes. This is indicated as step II in Figure 31. It will be focused on the development of a formalized measuring and analysis technique. Section 7.6 will in further detail discuss the expected benefits of the developed analysis technique.

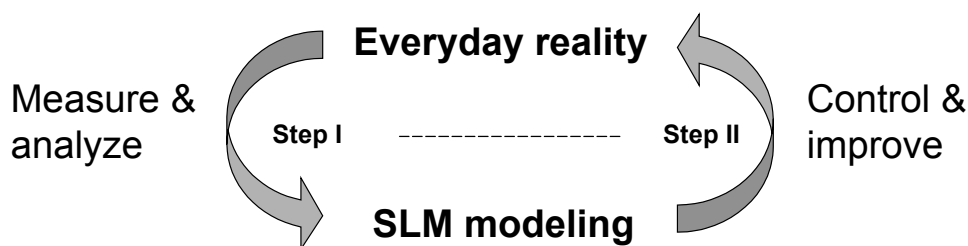


Figure 31 Steps from every reality to SLM modeling and visa versa

As mentioned before, a safety assessment is considered to have many similarities with a ISO 9000 quality audit. For instance, IEC 61508 does not use the term ‘audit’ but instead uses the term ‘assessment’. Other terms that could be applied are ‘verification’ or ‘validation’. However, verification and validation are also defined by IEC 61508 for other safety-related activities. (Verification concerns the confirmation by examination and provision of objective evidence that the requirements have been fulfilled, and validation concerns the confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled, as also described in Chapter 4 [IEC61508].) For the reason that the term ‘assessment’ is considered to be most appropriate and corresponds with the definition of IEC 61508, the following definition is formulated:

Safety Lifecycle Management analysis:

Systematic and independent examination to determine whether the procedures specific to the functional safety requirements and SLM concept comply with the planned arrangements, are implemented effectively, and are suitable to achieve the specified objectives.

This definition is based on the definition of a ‘functional safety audit’ by IEC 61508. The term ‘independent’, as defined in IEC 61508 in part 4, means in case an independent person, department or organization is responsible for the examination.

7.2 Usability of the MIR concept for SLM analysis

As discussed in Chapter 5, the MIR concept focuses on the business processes that impact the reliability of products. This concept has been applied in the high volume consumer products, but was also once applied at a manufacturer of safety-related systems. The MIR analysis technique appeared to be an excellent means to allocate missing reliability-related information loops or inefficient information loops.

Also in the area of SIS management, adequate information of reliability problems is of primary importance to e.g. realize and maintain the required safety integrity levels. (If safety-instrumented systems are not reliable, they will probably not fulfill their intended safeguarding function in case of a demand.) Because of the strong relationship between reliability of SIS and their SIL, the usability of the MIR techniques for SLM analysis is further explored.

As also discussed in Chapter 5 the MIR concept distinguishes 4 ‘climbing’ maturity levels. Literature on the MIR concept [Bro99], [Bro00] does not explicitly argue which MIR an organization should aim for. (Although it is clear that only MIR level 4 entails the ability to improve, which may be needed to achieve e.g. compliance with a standard.)

The SLM concept helps to achieve and maintain compliance with lifecycle-based standards. Compliance with such standards undoubtedly requires the achievement of a particular MIR level. Therefore, it is assumed that the ability of a company to achieve compliance with these standards could be established by focusing on the specific criteria of a particular MIR level. (It must be noted that compliance with a safety lifecycle-based standard like e.g. IEC 61508 is not restricted to appropriate control of reliability related information flows, but also aspects such as competence of persons need to be considered.)

The SLM concept is therefore extended with the other relevant SAM modeling parameters as described in Section 6.5.3.

The significant difference between safety in the process industry, and the reliability of e.g. a consumer product, is the fact that process safety is not subject to competition between different companies. If a company has a safety problem at his plant, it does not immediately lead to a deterioration of its competitive position, whereas reliability problems with a particular consumer product, for instance a automobile, immediately leads to a reduction of sales. Only indirectly, it could be reasoned that poor process safety is related to extra cost of accidents and therefore negatively influences the financial position and thus competition between companies.

Another, maybe more interesting, relation can be found between the achieved safety level of an SMS and the quality of the products as produced by the involved company. Many experts support the thought that a company, which operates very safely, can only achieve this if relevant knowledge on process variations and process risks are acquired. This kind of knowledge-based information is thus usable to optimize the process conditions impacting the quality of the products, and is at the same time required for the reduction of hazardous events, leading to benefits on both safety management and production.

7.2.1 Theoretical model cases of the four MIR levels of a lifecycle-based SMS

For the reason that IEC 61508 is typically a so-called performance based standard, the intention of this standard is to achieve a specific safety level. It will depend on the typical application and the local circumstances whether compliance with such a standard is achieved and relevant requirements are implemented correctly. For instance, the company as described case 11 of annex A develops programmable logic solvers. These logic solvers are used in different industrial sectors, which results in different performances. If such a logic solver is applied off-shore on an oil rig in the North Sea, it may have a different reliability than in case it is used at a refinery in the desert. A comparison can be made with regard to ISO 9000 series quality standards. Compliance with ISO 9000 is not a ‘black or white’ decision, but the judgment significantly depends on the perception and interpretation of the auditor.

Something similar applies to the determination of the MIR levels. The determination of the achieved MIR level of an organization could be done on a macro level and on a micro level. For example, on a micro level it could be concluded that between phase k and phase m an excellent reliability information exchange is realized. The information exchange between phase m and phase n however, might be very poor. On a macro level, the conclusion could therefore be conservative, resulting in a MIR 1 or optimistic in ‘almost’ MIR 4. The conclusion with regard to the achieved MIR level itself, is therefore not of ultimate importance but is more an indication of what ‘elements’ are still lacking or are very poorly implemented.

Suppose a situation where a company intends to comply with IEC 61508. The company has defined a SIS safety lifecycle and determines the SIL’s of the needed SIF’s. The SIF’s are subsequently realized (phase 9 of the IEC 61508 Overall safety lifecycle), installed and commissioned (phase 12 of the IEC 61508 Overall safety lifecycle), and validated (phase 13 of the IEC 61508 Overall safety lifecycle). During the validation phase it is concluded that all SIF’s comply with the required SIL’s. The following phase concerns ‘Overall operation and maintenance and repair’ (phase 14 of the IEC 61508 Overall safety

lifecycle). One of the requirements of IEC 61508 during this phase concerns periodic functional safety tests and maintenance (as described in Section 7.15.2.3 of part 1 of IEC 61508).

‘Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems shall be maintained which shall contain the following information:

- *the results of functional safety audits and tests;*
- *documentation of the time and cause of demands on the E/E/PE safety-related systems (in actual operation), together with the performance of the E/E/PE safety-related systems when subject to those demands, and the faults found during routine maintenance;’*

Organizations however, can implement such generic requirements in several ways. Examples of a number of different implementation will be discussed. The following theoretical case illustrates how the four MIR levels can be applied on a SIS lifecycle-based SMS, and how the MIR concept fits into the SAM and SLAM modeling concepts.

7.2.2 Modeling case 1

As mentioned before, during the operation phase, normally the safeguarding devices are periodical maintained and tested. In case malfunctioning of a device is detected, the failure will be repaired and process operation will continue. Hypothetically, it could be the case that a failure is not instantly repaired. E.g. for the reason that such a repair is not immediately required (the SIS is for instance designed to be fault tolerant) and repair is related to extreme high cost due to e.g. production loss. In this particular situation it is imaginable that test procedures are executed and test results are subsequently stored (See Figure 32).

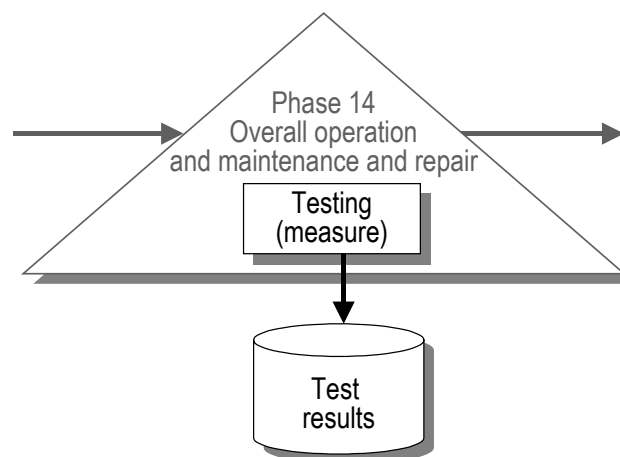


Figure 32 Storage of test results

This particular situation corresponds with MIR level 1. (Obviously, also a case with MIR level ‘0’ could be defined where no tests are done.) The conclusion that the test results are only stored and not further analyzed is more likely to occur in the high-volume consumer products market than within the process industry. This level is therefore not considered to be really representative for the actual common practice. It must be noted that IEC 61508 requires adequate evaluation of the test results in order to take appropriate corrective

actions (as will be described in modeling case 2). Companies, which are characterized by the above-described case situation, are therefore not considered to be compliant with IEC 61508.

7.2.3 Modeling case 2

A more realistic (and very often observed) situation concerns the following scenario. The test results are analyzed with respect to whether a fault is detected yes or no, and whether in that case a repair action needs to be taken. An essential difference with modeling case 1 is the fact that information of the direct cause of the fault is created. The detected faults are only partly analyzed and, based on the outcome, it is only decided to do a repair action. This case is illustrated by the flowchart of Figure 33, showing the repair loop and the storage of the test and repair results. The observation, that a partial analysis is conducted, could be considered as meeting MIR level 2. The fact that the root cause of the failure might not be discovered and the responsible department, activity or lifecycle phase might not be allocated, obstructs the possibility for controlling or improving the SIS with regard to the detected faults.

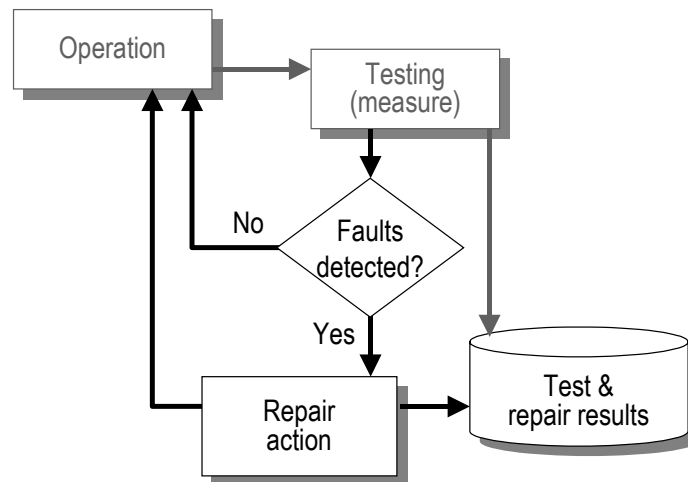


Figure 33 Testing and repair actions

7.2.4 Modeling case 3

Modeling case 3 (Figure 34) describes a situation where the test and repair results are not only stored, but are analyzed in such a way that an appropriate action is taken to guarantee that the required SIL will be met. For instance, it could be decided to shorten the off-line proof test interval (TI) because this action directly reduces the probability that the observed failures continue to exist in the system and thus directly influences the PFD. According to Gits [Git84] described as:

‘The requirement of safety of the production process and its environment, results in prescribed preventive maintenance, possibly in combination with a specific reliability to be achieved with respect to a specific failure. This requirement dominates in the determination of the maximum maintenance interval after which the maintenance operation should be carried out’.

Another action could be a modification of the SIF architecture to increase the level of fault-tolerance. Both actions will improve the PFD performance of the SIS, based on the actual measured failure rates. This kind of actions still does not require information about the precise failure modes or root causes. From this point of view, it is concluded that a mechanism is in place to control the SIS performance and guarantee the safety level. It is established that modeling case 3 corresponds with MIR level 3.

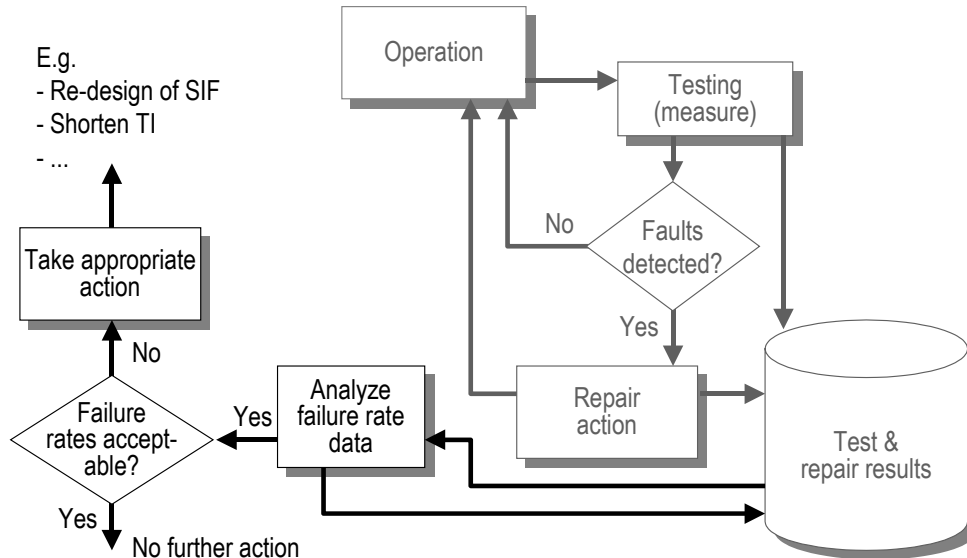


Figure 34 Analysis of failure rate data

7.2.5 Modeling case 4

Modeling case 4 describes a situation where the reliability problems and failures are measured, analyzed and evaluated, in such a way that the typical failure modes and root causes are discovered (see Figure 35). Furthermore, a knowledge database is maintained and available to the people who are involved in the other safety lifecycle phases. This offers the opportunity not only to control the performance of the current SIS, but also to learn from reliability problems, and use this knowledge to anticipate on these kind of problems during the development of a future SIS's. This requires not only the set-up and maintenance of such a database, but also requires the realization of structured information loops to the other safety lifecycle phases. Therefore, an adequate infrastructure needs to be in place that realizes and controls these information loops. For instance, it appears that the validation is often based on failure rate data obtained from the suppliers of the safety devices. The particular circumstances however, might deviate significantly from the generic data obtained from the supplier, which was based on 'average' user circumstances. Such information should be stored and fed back to the design department. The failure rate of the subject safety device should not just be adapted with this newly gained information, but also the typical circumstances the safety device is used in, shall be appropriately addressed. It could very well be that the 'old' failure rate is still valid for other applications and circumstances. It is established that modeling case 4 corresponds with MIR level 4.

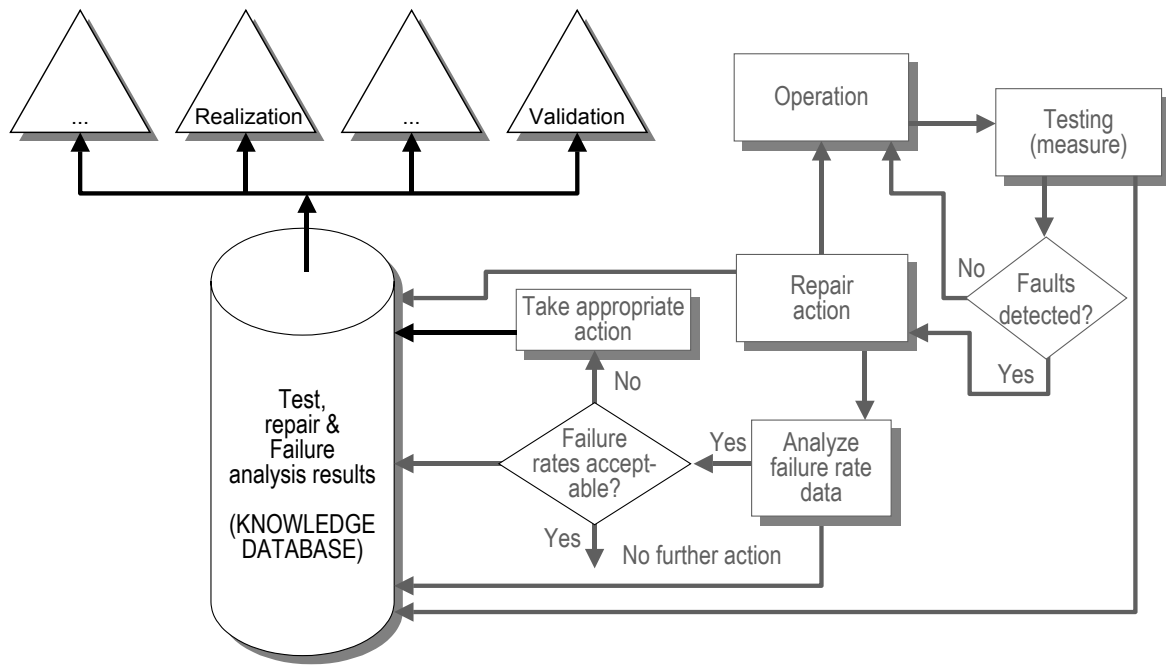


Figure 35 Development of a knowledge database

Although the described cases concern hypothetical situations, the author has many times experienced that companies struggle with these particular problems. The problems that are described in second modeling case reflect therefore very much the current situation. Almost all companies in the process industry, that were visited by the author, are more or less characterized by case 2. Based on activities in SIS standardization committees and SIS user groups it is a well-known fact that most companies currently do not maintain a database of failure rates of various failure modes of safeguarding equipment, which is needed for SIS validation activities.

7.2.6 Conclusions on the theoretical model cases

The 4 modeling cases show that the MIR concept is very well applicable to analyze a safety lifecycle-based SMS. Concerning the different MIR levels, it must be noted that, based on the generic description of these reliability maturity levels, a specific dedicated description for SLM analyses is highly needed.

Based on the described cases, the company's SIS-related SMS can roughly be divided into three groups.

- Companies that only test and verify the direct causes, and carry out necessary repair activities.
- Those companies that verify the root causes of the reliability problems and take corrective action to maintain the required SIL.
- Companies that analyze the reliability problems completely, and use this information to increase their knowledge and use it for future activities.

However, the first split that could be made is between an uncontrolled and a controlled SMS. Table 3 illustrates the relationship between, on one hand, the controlled versus uncontrolled SMS and on the other hand the MIR levels. It is presumed that companies strive for a controlled SIS-related SMS and consider compliance with IEC 61508 as a

means to achieve this. Compliance with IEC 61508 is therefore by many companies considered as being a prerequisite to achieve a controlled SIS-related SMS. As indicated by the Table 3, a MIR 3 is required to achieve a controlled SMS.

Table 3 Description of MIR levels based on modeling cases 1 - 4

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

It must be noted that even a company that only meets MIR level 1 or MIR level 2, could appear to be very well be able to meet the assumed failure rate, and therefore meet the PFD requirements. The weakness of this organization however, is that it is not aware of this, and does not have the required infrastructure to control or improve their SMS.

Based on the discussed cases it is considered that compliance with lifecycle-based standards can only be guaranteed if the reliability-related information flows are adequately controlled. The necessary information flows are of elementary importance in order to establish that the appropriate output from one activity is correctly put into specific other activities. Without these information flows, the SMS would become unstable and thus uncontrolled, resulting in among other things non-compliance with safety lifecycle model based standards. These reliability-related information flows can therefore only be controlled if all the necessary information loops (feed forward as well as feedback) are correctly realized and managed. This can only be achieved if an appropriate infrastructure is implemented and in order to establish that reliability related information is communicated in a structured way across the SMS organization. Therefore, communication channels have to be allocated and verified on effectiveness, efficiency, and completeness.

7.3 Elaboration on safety-related information management

In the previous section, the different levels of reliability-related information flows are discussed. It was concluded that these information flows play an elementary role with regard to the ability to control the performance of the SMS. The levels of information flows have been categorized, based on the MIR levels (Table 3). The generic definitions of the MIR levels however, are initially developed for analyzing the reliability of products, e.g. high volume consumer products. To utilize the MIR technique for analysis purposes of a SLM, this technique will need further development and adaptation to the different fields of usage. This section will elaborate on the safety-related information flows.

The first question that needs to be answered is whether a particular safety-related information flow is required. In that case, a number of aspects of such an information

flow will need to be addressed. First of all, the kind of information, where it needs to be created, and at which place this information is required, needs to be determined. Subsequently, the concerned SMS needs to be observed, to find out whether the information flow is indeed realized. In case such a flow is allocated, the flow needs to be analyzed to determine whether the right quality of information is generated, forwarded or fed back, and correctly processed. In case this information flow is not allocated, the question needs to be answered why it has not been realized, and whether certain barriers exist.

7.3.1 Aspects of information flows

An information flow can globally be subdivided into four parts (see also Figure 36).

- The source i.e. the location where the safety-related data is measured.
- The analysis that transfers data into information.
- The medium or system of information distribution such as channels and information carriers.
- The location where the information is needed, and is processed.

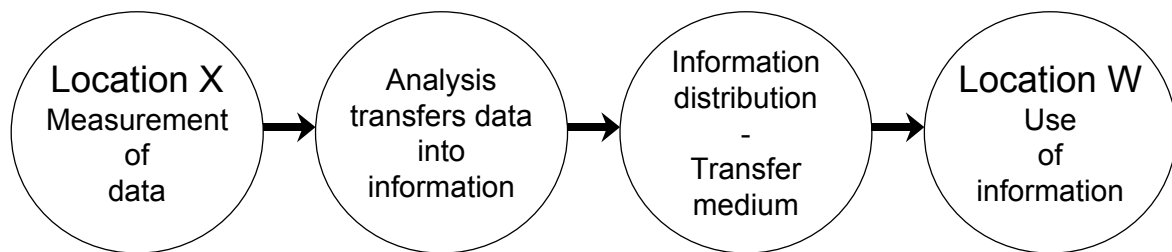


Figure 36 Aspects of information flows

The added value of an information flow depends on the quality of the measurement, the quality of transfer data in to information, the quality of information distribution and the quality of processing this information. All four qualities need to be determined.

7.3.2 Primary versus secondary information flows

With regard to the defined SAM and SLAM modeling concepts, a distinction can be made between ‘normal’ feed forward information flows that are required to perform successive safety-related activities. E.g. output information from the risk assessment is needed as input for the realization of the risk reduction measures. This kind of information flows could be considered as primary flows.

A second kind of required information flows, are those that are necessary for problem solving. At the moment that, during a particular activity, it appears that one of the safety-related objectives is not achieved, this information needs to be processed in a way that the problem will be solved. To be able to detect problems, the performance of the safety-related activity needs to be measured. Also in a situation that no problems are observed, this information needs to be processed to be able to establish how ‘well’ the performance was. This kind of flows is defined as secondary information flows. The primary flows are considered to be mainly feed forward flows, and the secondary flows are considered to be most times feedback flows. The MIR concept as described in Chapter 5, particularly

focuses on the quality of the secondary information flows. An SLM analysis however, needs to examine both primary as well as secondary information flows.

Case 3 of annex A describes a typical problem of an inadequate primary information flow between two departments that are responsible for two successive safety-related activities. For the reason that the HAZOP team did not define SIL requirements, the instrumentation department was not able to correctly realize the safety-instrumented systems.

7.3.3 Quality of information

At the moment that a problem is observed, information on the problem needs to be suitable for further processing. The problem description should therefore contain a number of attributes. First of all, a clear description shall be given of the nature of the problem. With regard to safety-related problems the nature can for instance be mechanical (e.g. a failure), software related, competence of persons, disturbance of the SR activity, etc. (In fact, all parameters discussed in the Ishikawa diagram of Figure 21 Chapter 6, could be subject to problems.) This description concerns the effects of the problem. In order to solve the problem, and take appropriate actions, the information of the effect and its immediate cause offers only the ability to take corrective actions. To be able to take preventive actions, information about the root cause needs to be revealed.

To classify the quality level of the safety-related information of e.g. problems, for each MIR level a description of the aspects of the information is given in Table 4. Each safety flow can subsequently be classified according this table.

Table 4 Description of quality levels of safety or reliability problem-related information

MIR	Description of information quality level
0	No data about problems collected (no information flows exists)
1	Number of problems registered (what, when, where, how much)
2	Direct causes of the problems analyzed (e.g. in order to determine corrective repair actions)
3	Information about the root causes of the problem allocated, and how to control these problems (why, how)
4	Information on how to prevent similar problems in future

In case the MIR level of an information flow is established, one obviously wants to know whether the outcome is reproducible. Therefore, the method that is used to establish the MIR level will have to be systematic and consistent.

Considering the complete set of business processes of an organization, many information flows could be observed. In particular closed-loop information flows could be considered as a chain of separate information flows. The original approach of the MIR concept was to establish the ability of an organization to control the reliability of the product that is produced [San00]. For the reason that it was observed that an organization consists of many information flows, it could be that these information flows achieve various MIR levels. Subsequently, the MIR level of the complete organization needs to be established. This last step often appeared to be difficult to perform. It was for instance concluded that

an organization for certain aspects achieved a MIR 2, where it achieved a MIR 3 for other aspects. This observation has led to the conclusion that the indication of the realized MIR level should not be done for the complete set of business processes of an organization, but much more for specific information flows. This redefinition implies a more narrow approach of the application of MIR levels.

A subsequent aspect concerns the ease to establish a MIR level of an information flow. One can imagine that the ease to establish the achieved MIR level is not just as simple for each MIR level. A MIR level 1 is considered to be relatively easy to establish, as the concerned information needs to consist of concrete and measurable data. This makes it easy to reproduce and therefore easy to establish MIR level 1. In case of a quality level of information of MIR 2, data on direct causes of the problems need to be established in order to take e.g. a repair action. It might be difficult to find the direct causes, but at the moment that such information is available, it will still be relatively easy to establish the MIR 2 level. Information of quality level of MIR 3 needs to contain data on root causes of problems. Root causes are even more difficult to determine as it is considered to be subjective at what moment one can speak of a root cause. There may be many root causes and these causes may have a completely different origin. Also the definition of corrective measures that prevent this type of problems will be more difficult. Therefore, the quality of the information about the root causes and corrective measures will also be more difficult to judge. It is accordingly concluded that it will thus be more difficult to establish a MIR 3 level of an information flow. The ability of an organization to prevent observed problems in future for comparable situations is considered to be the most difficult to define. This difficulty is related to the fact that it is far from easy to judge whether the estimated ability indeed leads to the expected result. A MIR 4 level will therefore be most difficult to establish. Overall, it is concluded that the higher the MIR level is, the more difficult it becomes to establish this MIR level.

7.3.4 Barriers

One of the major threats for the capability of an organization to implement the SLM concept, is the existence of barriers [San00]. Such barriers obstruct relevant information and documentation flows, communication channels and knowledge transfer. Because a barrier can have different properties, the following categories are distinguished in Table 5.

The next sections of this chapter will discuss how barriers can be detected. Obviously, the first indication that a barrier may exist, is in case that a low MIR level for a particular safety-related information loop is diagnosed. An even more obvious situation concerns the case that a particular information flow is not existing at all.

To be able to solve existing barriers, one needs to consider the management of the company. Determining and taking the required management decisions is considered to be outside the scope of this research.

Table 5 Description of barrier types

Barrier type	Example description
<i>Within an activity</i>	If for instance two people who are involved in the execution of this particular activity for certain reasons do not cooperate. Such barriers are not further discussed in this thesis because this kind of barriers is considered to be much more the result of social and psychological cooperation problems, than being the result of an inadequate infrastructure of information flows and communication channels but for certain reason not realized.
<i>Between activities</i>	At the moment that different persons are responsible for successive activities, appropriate information flows between these activities may be required.
<i>Between departments</i>	At the moment that different teams of experts from different departments need information from each other, the difference in expertise may lead to communication barriers.
<i>Between lifecycle phases</i>	Especially in a situation where different departments or even different organizations are responsible for different safety-related activities. This has been observed at a Belgian refinery where different sub-contractors were responsible for different lifecycle phases of the SIS. At the moment that the second sub-contractor started its operations, the first sub-contractor already had delivered its project results and was no longer present at the refinery.

7.4 Earlier experiences with SLM and MIR techniques in other applications

Over the last years, the theoretical considerations and modeling as discussed in the previous section and in Chapter 6, have been tested and verified in the industry frequently. The SLM analysis in relationship with the MIR concept has been carried out on a number of SMS in the process industry. An even higher number of dedicated MIR assessments have been conducted during the last years. These assessments were not restricted to the applications of reliability assessments of products within the consumer electronics, but assessments have also been performed at companies within the process industry sector.

This section gives an overview of experiences gained by Brombacher et al. [Bro99], [Bro00] during the development and various assessments of the MIR concept, and gives an overview of a collection of experiences gained by the author during the implementation projects of lifecycle-based safety standards at different companies. The experiences are subdivided into typical technical experiences of the different SLM and MIR analysis activities like for instance the definition and verification of the safety lifecycle model, and typical experiences of the use of common analysis techniques, such as interviews, flowcharts, questionnaires, etc.

These practical experiences have resulted in the definition of a formalized analysis technique as will be discussed in the following section.

7.4.1 Experiences with technical aspects of MIR and SLM analyses

Scope definition of the SLM analysis

In practice, all companies active within the process industry carry out certain safety-related activities. As mentioned in the previous chapters, this research primarily considers the application of safety-instrumented systems. The scope of the SLM analysis as described by the cases in Chapter 8 and annex A was therefore restricted to the utilization of safety-instrumented systems and related business processes. The identification of the safety-related activities, was started by considering the company's defined safety lifecycle model for safety-instrumented systems. Experiences have learnt that many companies are still not aware of the publication of standards like IEC 61508 and therefore have still not defined such a lifecycle model yet. It appeared to be an excellent method to start with the safety lifecycle model, as defined in the particular safety standard that the company intends to comply with. (E.g. the safety lifecycle of ANSI/ISA S84.01 to be implemented by a company in the USA.) Based on the chosen safety lifecycle, the involved departments, safety-related activities, and involved people were allocated. In some cases companies had already started with the implementation of e.g. IEC 61508, and had already defined a company-specific safety lifecycle model. In these situations, obviously this lifecycle model was used to allocate the involved departments, safety-related activities, and people.

Definition and verification of the safety lifecycle model

One of the aspects of the definition of the safety lifecycle is the specification of the boundaries of each lifecycle phase. The criteria that determine the boundaries of the lifecycle phases will, among other things, depend on the structure of the allocated departments and the allocated safety-related activities. It appeared that some companies prefer to synchronize the transition from one phase to another phase in line with the division of the safety-related activities as taken care of by a particular department (see also case 1 of Chapter 8). A safety lifecycle that has already been defined by the company should obviously be verified. (E.g. against a specific standard.) Two most divergent applications of safety lifecycles concern, on one hand, the end-user of a SIS and on the other hand the manufacturer of a safety-related sub-system. For instance, an end-user like an oil refining company may define a lifecycle, which strongly corresponds with the Overall safety lifecycle of IEC 61508. The realization of the E/E/PES SRS as defined in the Overall safety lifecycle is captured into one single phase 9. A manufacturer of dedicated safety PLCs however, may define a more detailed split-up of this realization phase, into specific lifecycle phases according the E/E/PES Safety Lifecycle (IEC 61508 part 2) and the Software Safety Lifecycle (IEC 61508 part 3).

Without the definition of a dedicated safety lifecycle model, the 'leitmotiv' is missing. It appeared a serious threat, that not all SIS safety lifecycle related activities were adequately allocated. (See e.g. case 1 of Chapter 8) Furthermore, the mutual relationship between depending activities was not always allocated. Especially in case concurrent engineering techniques are applied, it is of essential importance to allocate the milestones of start- end endpoints of the safety-related activities.

Verification of the SR activity bound objectives

The need for adequately defined safety-related objectives is already discussed in Chapter 6. Verification of these objectives is necessary to determine that all lifecycle phases and involved activities are covered by clear unambiguous objectives. Especially the presence of contradictions in these objectives needs to be verified. For instance, it was once observed that the objective during the safety requirements specification phase was to apply all 4 SIL's (thus including SIL 4), although in reality it appeared not possible to acquire a suitable SIL 4 certified logic solver.

Another striking experience of inadequate objective management concerned the situation that a safety-related device was designed to be part of a particular SIF. To achieve the required SIL, this device would need to be tested once per year. In reality however, it appeared that testing of this device was only possible during a major plant shutdown. However, such a shutdown was only done once per four years, and it appeared for all kind of economic reasons impossible to increase the number of shutdowns. Adequate objectives management can prevent from such conflicting objectives during the execution of the safety lifecycle activities.

Quantitative analysis of the quality of information flows

Probably one of the most difficult aspects to control safety-related business processes appeared to be the level of detail of information that should be communicated. For example, during the risk assessment, the safety integrity levels of the necessary safety-instrumented functions shall be determined. Based on these safety requirements, the safety-instrumented systems are realized and during the validation phase, these safety-instrumented systems shall be validated in order to determine that the required SIL is indeed achieved. It was frequently experienced that a global method is applied to make an estimate of the required SIL, whereas the very same company spends a lot of time and effort on conducting a detailed validation study. One can doubt the added value of a detailed validation for such a situation. This kind of reliability problems can be quantitatively analyzed using Monte Carlo simulation techniques, which are in detail described by Rouvroye [Rou01].

The complete chain of safety-related activities as part of the safety lifecycle, is intended to achieve a safe operating plant. As discussed in Section 5.1.2, the actually achieved safety level depends on the achieved level of risk reduction. However, this level of achieved risk reduction itself depends on the quality of the chain of safety-related activities.

A plant has achieved an acceptable safety level if the required time and effort that is spend on safety management is adequately (not necessarily uniformly) distributed over the various safety-related activities. Assuming that the quality of the involved safety-related activities are adequately controlled, this may lead to a situation that the time, effort and expertise that is spend on the subsequent safety-related activities is not necessarily equally distributed.

Techniques and methods to quantitatively analyze the amounts of time, effort, and expertise that should be spend on each safety-related activity will not be further discussed. This subject is recommended as future research.

Structuring of information flows

One of the most important enablers of performing a safety-related activity concerns the existence, availability, and accessibility of the required information. The accessibility depends on the realized information and documentation flows, while the existence depends on instructions that prescribe the creation and maintenance of such information and documentation.

During one of the SLM analyses, a first distinction was therefore made between the process-related information and the product-related information. The process-related information concerns regulations, standards, work instructions, and procedures on how to carry out the safety-related activities. Product-related information is split into three categories, namely safety-related input information, safety-related output information and archived information or documentation. Figure 37 illustrates four categories (or types) of information (see also 6.5.3).

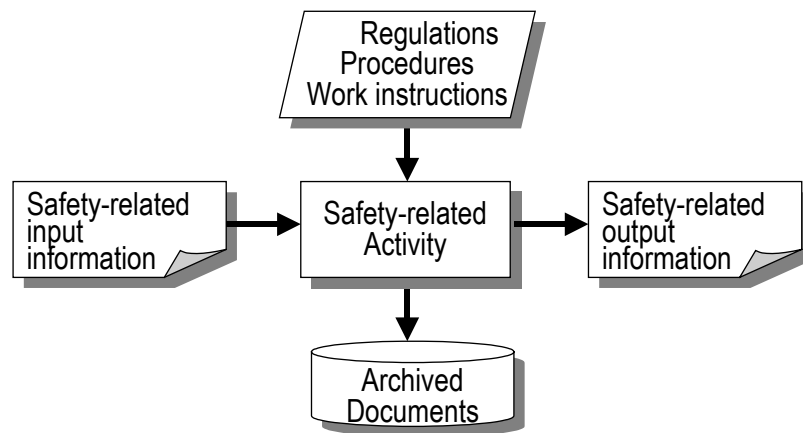


Figure 37 Categories of information

The following safety-related information must be checked for completeness and consistency:

- Information that shall be used for the safety-related activity.
- Information that shall be produced as part of the safety-related activity for further use during following safety-related activities.
- Information that shall be archived versus actually archived information.
- Comprehensiveness of the archived information and documentation as required by standards and regulations.

7.4.2 Experiences with common analysis techniques

During the various MIR and SLM analyses, a number of common techniques were used to collect the required information, and to structure and analyze the information. The techniques used to collect the required information were twofold, namely interviewing the involved people and analysis of the safety-related documents. Based on the collected information, activity flowcharts of the safety-related business processes were set up, in order to analyze the information in a structured manner. The following experiences with interviewing techniques, document analysis and flowcharting are gained.

Analysis of safety-related documentation

A clear property of document analysis, is that the final results unambiguously indicate which documents to be maintained as required by e.g. IEC 61508 are indeed properly stored, and which documents are still missing. The arguments to maintain a document database, is clearly explained in this thesis. Also the necessity to have this kind of information available as input for the safety-related activities is obvious. During the many SIS classification and validation studies, as carried out by the author, HAZOP reports and risk assessment reports often appeared difficult to trace, or not to be found at all. Surprisingly enough, many companies have a SIS installed without having defined the various SIF's and their required reliability (SIL). In many situations a poor reference list was added to these documents, something that made it difficult to trace missing documents, and to determine the relationship between the involved safety-related documents. Case study 1 was mainly conducted by analysis of the safety-related documentation. (See for more details, Chapter 8.)

Interviews

A very powerful technique to quickly collect valuable information is to make use of interviews. Whereas the analysis of the safety-related documentation normally takes a lot of time, the people who work with these documents can relative quickly indicate deficiencies of these documents. Furthermore, discrepancies between the formal requirements and procedures written in the documents are relatively easily found through interviews.

A disadvantage of interviews is that employees may not always be willing to fully cooperate. Especially in case that the reality deviates from the written procedures, people do not always like to admit it. At the same time, the interviewees may depict a nicer view than the actual situation is. For instance, the Health, Safety and Environment manager who is responsible for the PSM, might illustrate the current safety performance by excellent Lost Time Injury (LTI) and Fatal Accident Rate (FAR) figures, rather than focus on the potentially dangerous situations, which may impact future LTI and FAR figures. Before interviews are held, it is of essential importance that all involved persons are convinced to cooperate by creating awareness and commitment. In certain sensitive situations it may be required to process the interview results anonymously.

Case 2 was mainly based on holding interviews. (See for more details, Chapter 8.) One of the key characteristics of the MIR assessments was the verification of the required information flows.

A first step that was taken was the scope definition of the assessment, for instance the reliability of a particular product. Secondly, the whole process of specification, design and engineering and production and assembly of this product was mapped out. A following step concerned the allocation of people and departments that are involved in the realization of the product.

From that moment on, a number of people were interviewed to reveal the necessary information and thus the required information flows.

A typical characteristic of these interviews concerns cross checking of 'supply and demand' of information on two levels. People of each department were interviewed on two levels. Those persons that are responsible for defining and controlling the objectives, and those persons that are responsible for the actual execution of the required activities. Figure 38 shows 5 different kinds of communications between a superior and other superiors and executors. Obviously, adequate communication is required between these

two groups of people to take care that the people, who are responsible for the execution, indeed know what the requirements are. At the same time, it is important that their superiors know that these requirements are correctly implemented.

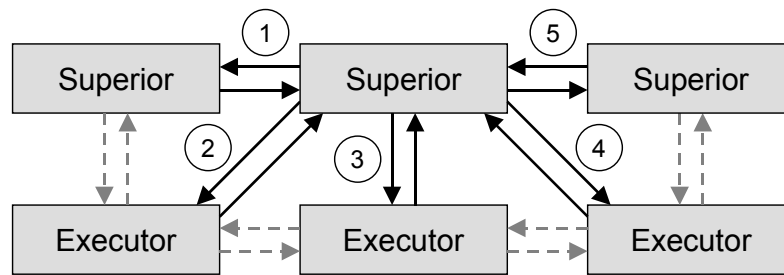


Figure 38 Communications between a superior and other superiors and executors

The final judgment on the achieved MIR level was based on the perception and interpretation of the experts who conducted the assessment. Especially the judgment on the level of detail that is handled during the interviews strongly depends on the interviewers. It depends on their judgment whether the required information is judged appropriate and complete, or whether more information is needed and thus extra questions need to be asked.

It sometimes appeared that more names of involved persons were mentioned during the interviews. This could indicate that the initially used safety lifecycle model was not completely or correctly defined. At the moment that ‘new’ names were revealed, it was determined whether these persons should also be invited for interviews, and whether the safety lifecycle model should be modified. This kind of experiences illustrates the iterative character of MIR and SLM analyses. A second or third analysis round might be necessary to collect *all* required information, and to be able to properly analyze the information.

Development of activity flow charts

Due to the importance of having realized the necessary reliability-related or safety-related information flows, during all MIR assessments and the SLM analyses, activity flowcharts were developed. The strong advantage of such flowcharts is the graphical representation and the resulting ability to indicate missing or poor information flows, allocate barriers, and explain suggestions for solutions. It appeared that the activity flowcharts were highly accepted by the involved people of the analyzed processes. An experienced weakness appeared the lack of predefined flowcharting conventions and definitions. Also the procedure to be followed to set up a flowchart is still not considered as a mature technique. Not surprisingly, the development of how to set up an activity flowchart is a natural process that is evaluated during the successive assessments. As part of the definition of the formalized analysis technique that will be discussed in the next section, also the application of activity flowcharts will be subject to formalization.

7.5 Formalization of the MIR-based SLM analysis technique

7.5.1 Need for a formalized SLM analysis technique

The experiences described in previous sections with MIR and SLM analyses, were gained by the experts who were knowledgeable about the MIR and SLM concepts. The first MIR projects were conducted by the researchers, who developed the MIR concept and were characterized by a relatively limited tool set combined with a high level of expertise. As described in the previous sections, a lot of experiences with a number of analysis techniques were gained during these studies. To become better capable to further develop these analysis techniques in a structured and reproducible way, and to be better able to transfer and disseminate the acquired knowledge and expertise, the need for the development of a formalized SLM analysis technique is obvious.

For over decades, companies within the process industries have managed their process safety in various ways. This brings along that safety policies, procedures, regulations, etc., are implemented into their safety management systems. Since that time, techniques are developed to analyze their SMS [CCPS89]. The objective of the development of formalized SLM analysis techniques is not just to replace the currently applied safety assessment schemes, but to enhance and supplement them with the MIR and SLM concepts.

7.5.2 MIR-based SLM analysis steps

The global steps of a MIR-based SLM analysis consist of the collection and analysis of relevant information and documents, and evaluation of the analysis results. The very first questions that arise are, ‘what information should be collected?’, ‘where can this information be obtained from, e.g. from whom?’. Also concerning the analysis and evaluation, questions of this kind may arise. Therefore, a step-by-step program is developed to conduct a MIR-based SLM analysis. Table 6 describes the analysis steps to be followed.

Table 6 MIR-based SLM analysis steps

MIR-based SLM analysis	
Step 1	SLM analysis scope definition
Step 2	Safety lifecycle definition
Step 3	Identification of involved persons
Step 4	Collection of information on SR activities
Step 5	Development of the activity flowchart
Step 6	Analysis of the SR activity flowchart
Step 7	Evaluation of the analysis results
Step 8	Identification of appropriate modifications
Step 9	Implementation of modifications

The above table clearly illustrates that also the analysis steps themselves represent the consecutive MIR categories of information levels. Step 1, 2, 3 and 4 concern the exploration steps of the SMS, and Steps 5 and 6 concern explanatory steps. Concerning

the control and prevention activities, steps 8 and 9 are defined. These two final steps, however, are not part of the core activities of the SLM analysis technique. The rationale behind this is that it will depend on the specific circumstances, which actions should be taken to best control or prevent observed problems. The following sections will discuss each step in detail.

Step 1, SLM analysis scope definition

The objective of this step is to determine the boundary of the SMS that is considered during the SLM analysis. For instance, the analysis could be restricted to the application of safety-instrumented systems. Another aspect that needs to be determined concerns the scope of the lifecycle, e.g. the safety lifecycle of the SIS. The definition of the scope of the SLM analysis will impact for instance the scope of the hazard and risk analysis, the role of other safety-related sub-systems, etc.

Step 2, safety lifecycle definition

As discussed in Chapter 5 and Chapter 6, the purpose of the utilization of a safety lifecycle model is to structure the safety-related activities and to allocate the applicable safety standard requirements. As SIS related standards do not demand that the particular lifecycle model, as defined in these standards is implemented, the end-user is free to define and implement his own safety lifecycle model. As already noted, official SIS-related standards allow that a specially adapted lifecycle model is used, as long as a clear reference is made to the lifecycle phases of the official SIS standards. For practical reasons it is recommended to consider this particular standard and use the standard lifecycle to define the specially adapted lifecycle model. As part of the MIR-based SLM assessments, it is recommended to verify whether the specially adapted lifecycle model complies with a SIS-related standard and verify the correctness of the adapted lifecycle model concerning its scope, references to the standard lifecycle, objectives, etc. (See the verification activities as described in e.g. IEC 61508.)

Unfortunately, many companies in the process industry still haven't decided that their safety-instrumented systems and the accompanying SMS shall comply with one of the latest SIS related standards as e.g. described in Chapter 4. For that reason, during a number of case studies, as described in Chapter 8 and annex A, a reference model is used to verify the correctness and completeness of the adapted lifecycle model. Therefore, in addition to the SAM and SLAM modeling concepts, based on the experiences with the implementation of the safety lifecycle models of IEC 61508, IEC 61511 and ANSI/ISA S84.01, a generic reference safety lifecycle model is defined. This reference model is used as a means to verify that all the main activities are adequately implemented.

For the reason that compliance with safety standards is not a goal on its own, but much more a means to comply with laws and regulations, the lifecycle models of each particular standard will not be further considered but instead considers their scopes, their similarities and their characteristics. Based on the experiences of the author with implementing these lifecycle models, the safety lifecycle reference model is defined and presented in Figure 39. The structure of this model is based on three main activities namely specification, implementation and utilization.

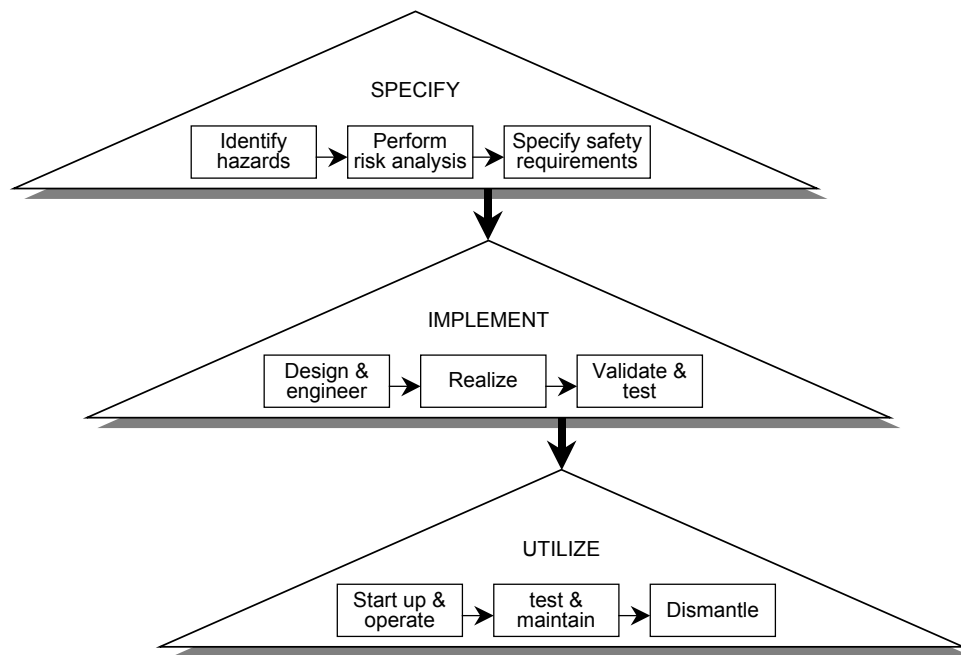


Figure 39 Reference safety lifecycle model

Obviously, the above lifecycle model does not describe all lifecycle phases of e.g. IEC 61508. Especially if besides the Overall lifecycle model, also the ‘hardware’ and ‘software’ lifecycles are considered. Nevertheless, the defined reference model offers a global overview of the structure that a selected lifecycle model should comprise. For instance, modification is not included into the reference model, as this activity could be carried out at any stage of the lifecycle. Procedures for Management Of Change (MOC) are not new in the area of PSM and for more information is referred to e.g. the CCPS [CCPS89].

The case studies described in annex A are based on comparison with this reference model. During the analyses of various safety management systems, the modeling concepts of SAM and SLAM have been included.

The reference model is not further detailed because companies appear to sometimes apply very different methods, tools and technical requirements. For instance, to date many companies have not adopted the terminology of SIL, but often apply an equivalent ranking system. During the case studies, it was therefore only observed whether these companies indeed had adopted an appropriate equivalent ranking, or e.g. no ranking at all.

Step 3, identification of involved persons

Once the safety lifecycle model is defined or selected from a SIS related standard, the safety-related activities that are carried out need to be allocated. In practice, this might result into such a specific degree, that this step is only properly carried out if firstly, the persons who are responsible for the phases of the safety lifecycle model are identified. For instance, the Health, Safety and Environment (HSE) manager is most times considered to be the most appropriate person to identify and allocate the involved responsible persons. To prevent that certain safety-related activities are not considered because the identified persons appear not to be responsible for all of them, it is recommended to apply the overlapping principle where people are selected in a manner that all lifecycle phases are covered by more than one person. Furthermore, one or more persons cover more than one

phase. During the following step, ‘collection of relevant information on SR activities’, it might appear that certain the involved persons are not identified. A first conclusion at this stage could be that the people that are part of the SMS are possibly not well aware of the responsibilities of their colleagues. The creation of an organization chart might solve this problem.

Step 4, Collection of information on SR activities

Once the persons responsible for the safety lifecycle phases are identified, the safety-related activities need to be identified. For each identified activity, the SAM modeling parameters as defined in Chapter 6, shall be described in terms of objectives, input and outputs, enablers and restrictions.

During the course of one project execution (see case study 1 of Chapter 8), it appeared that in reality, at substantial points was deviated from the formal described situation. This discovery led to the conclusion that a SLM analysis should not be restricted to a verification of formal procedures and documentation in order to allocate inadequacies with standards (e.g. IEC 61508 and ANSI/ISA S84.01) and regulations (e.g. Seveso II Directive), but also the actual situation should be revealed. (‘Ist’ situation versus ‘Soll’ situation.) A means to do this is by interviewing the persons involved in the safety-related activities. To cope with the above-described problem, the questions asked during the interviews were therefore oriented on three sub-areas:

- Formal situation : What is officially established?
- Actual situation : What is the actual situation?
- Ideal situation : Could an ideal situation be defined?

This is schematically represented in Figure 40:

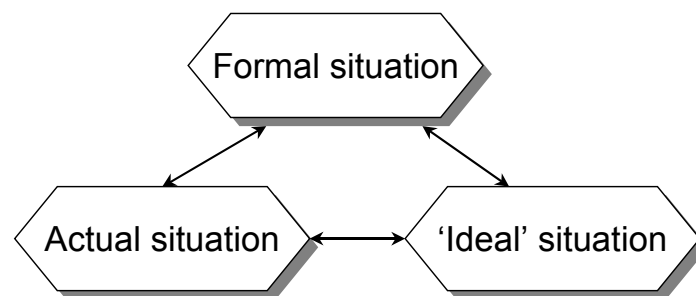


Figure 40 Differences between ‘formal’, ‘actual’ and ‘ideal’ situations

In general, the following sources of information should be consulted:

- Interviewing the identified persons in the previous SLM analysis step. Obviously, it is the intention to collect information on the SAM modeling parameters. Especially concerning these parameters, it is important to focus on the sources, departments, people, etc. of e.g. input information, and the destinations of output information and documentation. Annex C offers an example of an SLM analysis questionnaire.
- Document analysis. Besides the interview, as a kind of verification, the existing safety-related documentation could be analyzed in order to check whether the interview results correspond with the safety-related documentation. Also a

completeness check is done by analysis of the documents. It must be noted that document analysis appears to be very time consuming. (See also the first case described in Chapter 8.)

- A third source of information concerns the technical process installations themselves. It obviously requires dedicated expertise on these technical process installations to be able to judge whether they indeed have implemented the applicable safety requirements. Concerning the safety-instrumented systems, the validation, maintenance and testing registers could be verified, and concluded that the realized safety-instrumented systems are indeed correctly designed and operated. This will result in collection of information on the physical results of the identified safety-related activities.

Step 5, development of the SR activity flowchart

The primary activity of this step is the development of the safety-related activity flowchart. This flowchart should visualize the SAM and SLAM modeling concept as discussed in the previous chapter, including the scope of the SLM analysis, as for instance defined by the safety lifecycle model. The activity flowchart shall be based on gained information during the previous steps, to name the safety lifecycle model, the organization chart and the information of the safety-related activities. (See also annex D for development aspects of flowcharts.)

The application of the SAM models as building blocks for the SLAM model and the safety-related activity flowchart brings with it that once again the involved people will be identified and allocated. This means that a kind of verification will be done of step 3, where at a first stage involved people are allocated.

The definition of a consistent methodology on how to set up a SR activity flowchart will have the benefit that different people can consistently set up and evaluate the flowchart. A restriction is that clear and unambiguous definitions and conventions need to be applied, concerning the used symbols, metrics, chart lay-out, etc. Therefore, to use the flowchart techniques the generic definitions and conventions are adapted for the MIR-based SLM analysis. Annex E gives an overview of the symbol definitions (Table 15) and annex F gives an overview of the stepwise process on how to set up an activity flowchart (Table 16). These definitions and conventions in annexes E and F are in line with the ISO 5807 standard [ISO5807].

Step 6, analysis of the SR activity flowchart

As part of the SLM analysis it must be verified whether the safety-related information flows are identified correctly, and are complete, and whether these information flows are appropriately forwarded or fed back as input to other safety-related activities.

Particularly the MIR analysis focuses on the identification of reliability related information flows. Especially feedback loops are necessary to realize learning cycles, which often are characteristic for MIR level 4. A comparison of the actual versus the ideal flowchart should identify discrepancies and opportunities for improvements. (See also the next steps.)

Step 7, evaluation of the analysis results

Initially, the developed activity flow chart was primarily based on the safety-related documentation (see case 1 of Chapter 8). Analysis of each document and verification of documentation flows resulted in the activity flow chart. Analysis of this flowchart revealed inconsistencies, shortcomings and other inadequacies. One can imagine that in reality at certain points, deviations from the formal described situation occur (Figure 40). (If for instance the procedures, as part of the corporate standard, are not practical.) Through modification of the related standard or through adaptation of the SMS, bottlenecks can be removed. Of crucial importance is to find out *why* at a certain point was chosen to deviate from the formal situation. Only then it will be possible to define and implement adequate improvements.

In order to judge whether a specific information flow complies with the required MIR level, common methodologies and techniques that generate, transfer and process information, can give an indication on this (different tools or methods result in different quality levels of information). Table 7 gives an overview of existing tools and techniques that are used in the area of safety and reliability engineering and management [Bro97]. For certain techniques the realized MIR level depends on, the extension, thoroughness, and moment of the application of the tools.

Table 7 Applicable tools, techniques, methods per MIR level

Level	Tools, techniques, methods
MIR 0	No safety policy
MIR 1	ISO 9001, checklists, testing
MIR 2	FMEA, checklists, FTA, ETA
MIR 3	SPC, FMEA, DOE, Reliability database
MIR 4	Near miss reporting, brainstorming, literature, conferences, FMEA, DOE, Markov

Currently, a trend is going on where Management Information Systems (MIS), such as Oracle, SAP and Baan, are not only used to control financial and administrative information of the organization, but also increasingly for control of materials and spare parts. A probable next step would be to use these information systems for management of safety and reliability information. For instance, a concrete first step could be to process information of failures, test results, and maintenance by a MIS.

Steps 8 and 9, identify and implement modifications

Steps 8 and 9 concern the identification and implementation of modifications. Based on the evaluation of the safety-related activity flowchart analysis results, specific problems concerning information flows are allocated. Based on this knowledge, adaptations and action points shall be defined that solve the allocated problems. A key element in this step concerns the information on the actual achieved MIR level and the required MIR level of a specific information flow. At the moment that this information is available, it will give a clear indication of what needs to be improved.

In practice, it often happens that an unforeseen problem arises. As explained at the beginning of this sub-section, the modifications that should be taken to control or prevent

observed problems depend on the specific circumstances. Therefore, improvements are illustrated by a number of examples.

For instance, during the operation phase it appears that the actual failure rate of an ESD valve is higher than expected. The deviating failure rate may seriously decrease the SIL of the SIF of which the ESD valve is part of. At the moment that inadequate performance is measured, a mechanism shall be in place that takes care that the information is adequately processed and appropriate action is taken.

With regard to e.g. a bad performing ESD valve, it could be decided that a second valve is installed to make the SIF fault tolerant. As an alternative measure, it might be decided that the Test Interval (TI) of the valve needs to be shortened. The installation of an extra valve results in a re-design of the SIF and relevant information shall therefore be fed back to the realization phase. If it is chosen to shorten the TI, the SIF will need to be re-validated (feed back to the validation phase) and test procedures will need to be adapted (operation, maintenance and testing phase).

Another example of a situation that requires an information feedback loop concerns a process or SIS modification. Such a modification might imply an upgrade of the SIS software or design changes to the process installation. How to take care of such a modification with regard to the feedback and/or feed forward of safety-related information, is not covered by e.g. IEC 61508. The only remark given by this standard is that one should go back to the appropriate phase. How the appropriate phase shall be determined and what kind of information shall be fed back is not indicated. The added value of the application of activity flowcharts is its power to allocate required information flows. Furthermore, the required MIR level of each information flow can be established. For instance, the required MIR level might depend on the impact of the modification. A big modification may require a far-reaching feedback in the lifecycle model and the accompanying information flow might therefore be required to comply with a high MIR level. Conversely, small modifications may not require a far-reaching feedback in the lifecycle model and the quality of the accompanying information flow might subsequently be acceptable if it complies with a lower MIR level.

The case studies in Chapter 8 and annex A show many more examples of these steps.

The formalized MIR-based SLM analysis technique does not cover all SMS assessment aspects, but is restricted to the specific aspects of SLM. The application of such a formalized MIR-based SLM analysis technique will make appropriate comparison of analysis results possible and should form the basis to prioritize adequate action points to improve the SMS.

The next section will discuss the benefits of the application of the MIR-based SLM analysis technique.

7.6 Expected benefits of the MIR-based SLM analysis technique

Obviously, the final goal of using the MIR-based SLM analysis technique is to improve the safety performance of the plant, organization, or process installation. As discussed in Chapter 5, difficulty will always be to demonstrate direct relationships between an accident or prevented accident, and the contribution of the SMS to it. Nevertheless, if accidents that occurred in the past are considered [Bel00], the direct cause, e.g. the fact that a piece of equipment had failed was not properly maintained or was operated incorrectly, could in many cases have been prevented from developing into a hazardous event. The reason that the hazardous event scenario continued to develop, was because

appropriate information management lacked. If the involved people knew that a failure occurred, why it occurred, and what would be an adequate action to be taken, many accidents could probably be prevented (awareness and commitment). The MIR-based SLM analysis technique therefore focuses on the adequate control of safety and reliability-related information. The technique helps to determine the actual characteristics and level of information flows, and the required level. If barriers or delay factors disturb proper flow of information, the MIR-based SLM analysis technique is able to reveal and allocate these barriers. The following section discusses these and other benefits in detail.

7.6.1 Allocation of missing activities and information flows

The MIR-based SLM analysis technique is comparable with existing techniques that verify, audit, and assess organizations with regard to safety and reliability related information management. An overview of characteristics that can be observed by an SLM assessment consists of:

- Allocation of missing safety-related activities
- Allocation of required information flows
- Requirements of information flow characteristics
- Identification of responsible and other involved persons
- Allocation of communication channels
- Allocation of information transfer barriers
- Documentation and information sources
- Verification model to analyze near misses and real accidents

As stated before, the relationship and impact on the safety performance, and corrective actions to be taken, depend on the specific organization and circumstances.

7.6.2 Identification of improvement points

Barriers could be the result of many causes. For instance, clear shortage on human resources prevents proper testing and maintenance. Barriers do not necessarily exist due to lack of communication between an operator and an engineer. The MIR-based SLM analysis technique is capable to reveal and identify barriers. Further analysis will in that case be necessary to exactly determine the root cause, and the solution to remove this barrier.

7.6.3 Awareness and commitment

The level of awareness that can be measured by the MIR-based SLM analysis technique is probably best explained and illustrated by the following case study:

In spring of 1997 at a Belgian company an introduction on IEC 61508 was given. Approximately one year later, during a presentation of MIR assessment results, the same group of persons was invited. It appeared that during that year, particularly due to a number of reorganizations, 8 out of 10 persons were replaced, meaning that a number of people were new, a number of people changed from their function, and a number of people were not longer active within the organization. Due to the time pressure as a result of bad economic circumstances, there was

hardly any opportunity to transfer knowledge on new trends and standards. During the presentation of the results, it appeared that hardly any attending person, was aware of the scope, objective and concepts of IEC 61508. It was therefore concluded that during the intermediate period of one year, no progress was realized. (See also Case 1 of Chapter 8)

The effect of improvement of commitment by application of MIR-based SLM is illustrated by the following case description:

During an introduction presentation on IEC 61508 and a preparatory study of typical SIF's of a Canadian fertilizer plant, people were invited from the instrumentation department as well as from the HAZOP department. Initially, it appeared that there was a strong resistance to the proposed new concepts of IEC 61508. Later on however, people from both departments came to the conclusion that the new approach would increase the safety performance of their organization and ultimately benefit themselves. As a result of this, commitment was created to further cooperate in future. (See also Case 3 of Annex A)

7.7 Recapitulation

This chapter introduced the formalized MIR-based SLM analysis technique, together with first application experiences of MIR-based analyses and examples of information flow barriers. The following chapter will describe two case studies that were carried out during the development process of the MIR-based SLM analysis technique. The experiences gained during these case studies formed the basis for the described nine analysis steps. Annex A contains descriptions of 9 other case studies, where (potential) safety-related problems were revealed and analyzed.

8 Case studies

Extensive experiences with the application of the MIR concept to analyze the implementation of the safety lifecycle models have led to the development of the formalized MIR-based SLM analysis technique. The majority of these experiences are gained during a total of 11 case study of which two are discussed below. Annex A gives an overview of nine other case studies performed at various companies in the process industry. Typical business process-related safety problems, which were observed during these case studies, are further explored and explained using the MIR-based analysis technique. This chapter will describe two case studies carried out at two different chemical companies in the process industries. At the end of this chapter the case study results of these two cases together with nine cases of annex A are evaluated.

Case studies have proven to be an excellent means to investigate an empirical topic by following a set of pre-specified procedures [Yin94]. Particularly in the area of design research (as discussed in Chapter 2), case studies are a perfect means to demonstrate relationships between specific parameters, but sometimes can not be completely explained by formal rationally derived models. Especially the fact that case studies are directly carried out in practice (in the process industries), contributes to the validation of the developed formalized analysis technique.

Conducting e.g. experiments would have been another means of collecting evidence to test the theory. The disadvantage however of doing experiments is the amount of time and resources that is needed to conduct an experiment.

8.1 Design of the case studies

This section will discuss and describe the objective, scope, level of detail, the determination of the MIR levels, sources of evidence, and structure of the case studies. The 11 case studies, which are described in this thesis, are based on these definitions, restrictions and assumptions.

8.1.1 Objective of the case studies

Probably the best way to acquire clear and unambiguous evidence that application of the SLM concept leads to a significant improvement of the safety performance, would be a comparison study performed on two exactly identical plants. One plant should operate a safety management system that is not based on a lifecycle model, and the other plant should conversely be operated based on the safety lifecycle management concept. To be able to measure differences in safety performance, the observation period should be at least several years of operation. To measure statistical relevant differences would take two large groups of identical plants and many years of operation should be used. Unfortunately, no two plants in the world are fully identical and therefore, this way of demonstrating the relationship between the SLM concept and the safety performance is not practical and realistic, and thus not achievable.

Nevertheless however, typical safety-related business process problems, which are considered to be the result of *not* having the SLM concept implemented, need to be traced and solved. It is for that reason, that the formalized MIR-based SLM analysis technique has been developed.

One of the objectives of the MIR-based SLM analysis technique is to allocate safety-related information flows and determine the required and actually realized MIR level. However, the ultimate objective of organizations is to solve typical safety-related business problems. Obviously, in order to solve a problem, it first needs to be detected and analyzed before appropriate modifications can be taken. These modifications however, will always depend on the specific application, management strategy, and culture of the organization in question. During the case studies, a number of safety-related business problems have been revealed and analyzed. For the reason that qualification of information flows is in that respect considered as being an essential part of the analysis, the MIR level of the information flows, which are part of the concerned safety-related activities, are determined. The degree, to which the problems are successfully identified, analyzed and explained, validates the MIR-based SLM analysis technique.

8.1.2 Case study scope

The cases that are described in this thesis are closely related to the experiences gained by the author during his work as a safety consultant for the process industries. These experiences consist of the investigation of occurred accidents, SIL validation studies, and SMS assessment studies.

These case studies focus on the utilization of safety-instrumented systems and their interaction with the other risk reduction measures. SIL validation studies of safety-instrumented systems were carried out, and in case of significant over- or under protection, also the underlying business processes from which these technical systems were the result, were included in to the study.

Concerning the SIS-related SMS analysis studies, the ability of compliance with standards like IEC 61508 was considered. In other words, if the safety-related business processes were set up adequately, would it from this perspective be reasonably probable that the realized safety-instrumented systems fulfill the required safety functions and achieve the required SIL?

The interaction between the adequacy of the safety-related business processes and the appropriateness of the realized technical safety-instrumented systems was continuously point of special interest.

8.1.3 Level of detail

The question that arises is related to the level of detail for each case study in order to be able to adequately validate the developed analysis technique. Particularly in the area of design researches, the methodology is only then valid if in all likelihood, relationships and interdependencies are demonstrated. The case study results should therefore be reproducible and convincing.

Furthermore, the relatively high number of case studies contributes to prove the applicability and validity of the analysis technique. The validity of the analysis technique is considered to be acceptable, at the moment that the specific safety-related business problems, as described in Chapter 5, are well observed, explored, and explained. In some cases it was therefore required to carry out the study more profound and detailed than in other cases. This explains the fact that some cases are described in less detail than other cases.

8.1.4 Determination of the MIR levels

As will be stated in 8.2.1, important is to understand that, although the fact that the objective of the MIR-based SLM analysis technique is to qualify MIR levels of information flows, it must be noted that the underlying reason to apply this technique is to solve safety-related problems. From this perspective, this analysis technique is much more a means to allocate, analyze, and explain the specific problems. Therefore, as part of the case studies MIR levels are only established for the specific information flows which are related to the safety problem. For each described case study, a specific section in generic terms will discuss the actual achieved MIR levels versus the required MIR levels of safety-related information flows of the observed problems.

8.1.5 Sources of evidence

A case study inquiry usually copes with the technically distinctive situation in which there will be many more variables of interest than data points and, as a result, relies on multiple sources of evidence. To collect the appropriate knowledge of the subject case, Yin distinguishes six sources of evidence, which can serve as basic information to successfully carry out the research [Yin 94].

- Documentation
- Archival records
- Interviews
- Direct observations
- Participant observations
- Physical artifacts

Each source of evidence has its own strengths and weaknesses. This thesis will not discuss the detailed difference between these sources, but will be restricted to the conclusion that no single source is considered to be comprehensive. At the same time, various sources might be complementary and will therefore be considered as additional proof. The analysis steps primarily focus on the analysis of documentation and the collection of information by performing interviews.

8.1.6 Structure of the case descriptions

Sections 8.2 and 8.4 will discuss two detailed cases. The first case study is carried out at a Belgian plant of a Swedish chemical company. This study is mainly based on documentation analysis, a number of interviews and discussions with the local SIS expert. This case study was very much focused on compliance of this organization with the Overall safety lifecycle model of IEC 61508.

Based on these experiences a second case study was carried out at an American chemical plant located in the mid-west of the Netherlands. During the second case study a number of people were interviewed, and a comparison was made between the information obtained from the interviewees and information obtained from the existing documentation.

It should be mentioned that much of the theory as described in the previous chapters is based on the results and experiences of these two cases. These cases should therefore be considered as evidence, which serves as a basis for the development steps, that has resulted in the formalized MIR-based SLM analysis technique. Annex A gives an overview of another nine ‘smaller’ cases. Each case includes a description of a typical

safety-related problem, which is subsequently analyzed, using the MIR-based SLM analysis technique. These cases serve as evidence that confirms the applicability, functioning and added value of the developed technique. The structure of the description of these cases is as follows:

- Introduction; a description of the subject organization, process installation and application circumstances.
- Observation; a description of the current problem area and its specific safety-related problems.
- MIR-based SLM analysis; the analysis of the problem which includes the development of an activity flow chart, including allocated learning circles and barriers.
- Evaluation and conclusions; an evaluation of the root causes of the observed safety-related problems.

Section 8.6 gives conclusions and recommendations of the analysis results of the two case studies of this chapter together with the analysis results of the nine cases as described in annex A.

8.2 Case 1 – IEC 61508 Overall safety lifecycle model analysis of a Belgian plant of a Swedish company

Note:

This case description is a summary of two earlier publications. A more detailed description can be found in the article ‘Safety Lifecycle Management – A flowchart presentation of the IEC 65108 Overall Safety Lifecycle Model’, written by K.A.L. van Heel, B Knegtering, and A.C. Brombacher, published in Quality and Reliability Engineering International 15: 1999 [Hee99], and Heel, K.A.L. van – Safety lifecycle management in the process industries, MSc thesis Eindhoven University of Technology 1999 [Hee99a].

8.2.1 Introduction

For an existing operating process installation a study has been performed to investigate which steps should be taken in order to implement the IEC 61508 standard successfully. This study is based on the Overall safety lifecycle model, and uses a flowchart approach that addresses all relevant items of the Overall safety lifecycle.

The immediate cause to initiate the study, was the fact that the pressure safeguarding instrumentation for a gas storage tank was considered to be old-fashioned and therefore might be obsolete. Before upgrading the old relay-based logic solver and replacing it by a dedicated safety PLC, the instrumentation department thought it would be wise to review old safety studies and create a level of understanding of the current safety requirements.

8.2.2 Development and verification of the safety lifecycle model

As already stated, in order to deal in a systematic way with all activities necessary to ensure the functional safety of the E/E/PE safety-related systems, IEC 61508 describes an

Overall safety lifecycle model. The phases in this model refer to activities that shall be carried out, such as:

- Identification of the EUC boundaries.
- Assessment of the EUC risks.
- Determination of the required risk reduction in terms of safety requirements.
- Realization of the needed safety requirements.
- Planning for installation, commissioning, maintenance, operation, and safety validation concerning the safety-related system(s).
- Installation, commissioning, safety validation, operation, maintenance and repair of the safety-related system(s).
- Ensuring the functional safety of the safety-related system(s) during and after modification, retrofit, decommissioning and disposal.

Activities related to the management of functional safety, verification, and functional safety assessment are also part of the Overall safety lifecycle, but are not included in the Overall safety lifecycle model in order to reduce its complexity.

Shortly after the case study was started, the flowchart approach was used to assess the safety management procedures of the company. A hazard and risk analysis was performed of a gas storage and revealed that the existing and required documentation was not complete and not up to date. Therefore, it was decided to go through the entire company's safety management procedures to identify missing or incomplete procedures. A company-specific flowchart was created, using the following existing information/documentation:

- Procedures for new projects or modifications(draft and official documents),
- hazard and risk analysis of the gas storage,
- P&ID's (Piping and Instrumentation Diagrams) of the involved explosive gas storage installation.
- Descriptive documentation concerning the explosive gas storage.

8.2.3 Case study results

Almost immediately after the study was started it appeared that some of the old P&IDs were missing, as were the original hazard and risk analysis reports. It was questioned whether the hazard and risk reports ever existed, for reason that the storage tanks were constructed almost 30 years ago (in the early seventies of last century). Fortunately, some old documents turned up, which described the original design of the tanks.

Amazingly enough, it was observed that the 'old' drawings were never updated as result of modifications and retrofit during the last 30 years. For example, one of the striking observations was the fact that the gas would be transported to a flare, a few hundred meters farther down. In practice however, on top of the tanks, pressure relief valves were installed. Although the fact that local workers were aware of this, one can imagine that such documents could easily lead to a dangerous situation. A second notable observation was related to the documentation concerning the supply of the gas. Drawings and descriptions still contained information that ships supplied the gas. In reality however, it appeared that in the course of time a gas pipeline was built, which had replaced the supply of gas.

Notwithstanding these observations, it must also be noted that this site was recently taken over by a new company, which had only recently defined a corporate standard on the application of safety instruments. Therefore, the observed shortcomings in the documentation were considered to be an inheritance of the past.

Starting point of the safety study was therefore not just the deficient or obsolete process installation related documentation but also this ‘new’ corporate standard. Surprisingly, this standard contained a lifecycle model, which appeared to be a combined lifecycle model that described the successive stages of the design and construction of a process installation, and the different moments in time that a safety study needed to be performed (see Figure 41). In order to analyze the safety lifecycle model, the safety-related phases and activities were separated from the combined lifecycle and subsequently compared to the IEC 61508 Overall safety lifecycle.

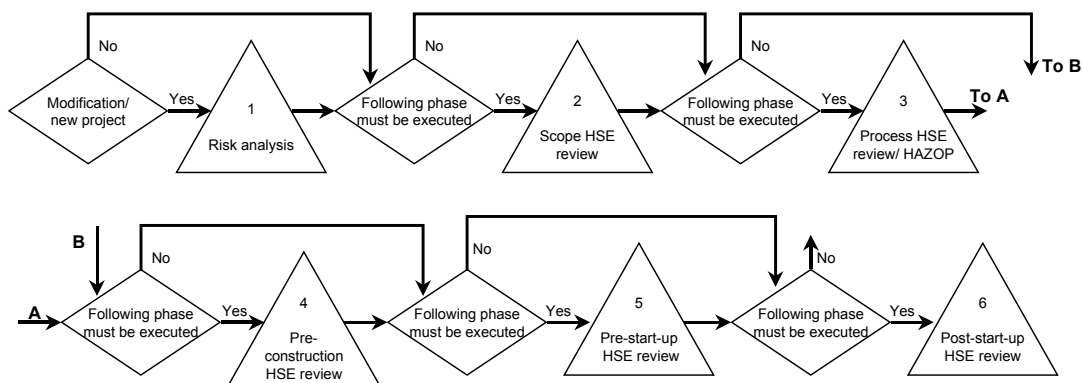


Figure 41 Simplified flowchart of the combined lifecycle phases.

The flowchart created for the safety management procedures has been compared with the flowchart of the IEC 61508 Overall safety lifecycle. As a first step, all missing and incomplete phases were identified. Figure 42 shows the result of this comparison.

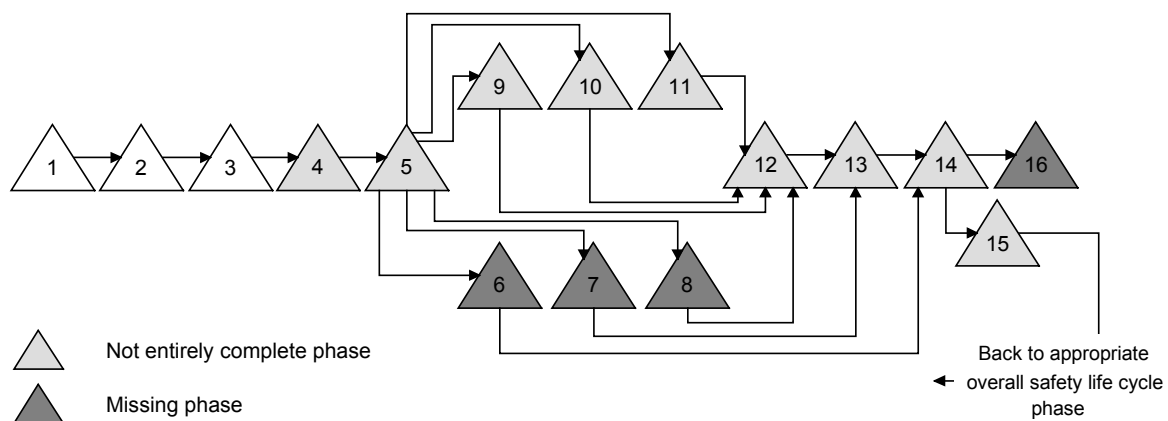


Figure 42 Missing or incomplete phases

The following conclusions were drawn:

- Phases 1 to 5. The risk analysis of the equipment under control and the safety requirements specification procedures, were almost complete. Not included was the description of the procedures with regard to the allocation of safety requirements to safety functions and safety integrity levels.
- No concrete description of planning activities (phases 6 to 8) could be retrieved from the available documentation.
- For phases 9 to 11, realization of the safety measures, it was not indicated which information needed to be documented.
- The objectives of phases 12 to 14 (installation and commissioning, safety validation, maintenance, operation and repair of the safety-instrumented system) could not be realized in line with IEC 61508 because no planning was specified (phases 6, 7 and 8).
- The documentation did not include specific requirements for the decommissioning phase (phase 16).
- Since not all phases were addressed in the company's lifecycle, it was not by every change possible to go back to the appropriate phase after modification or retrofit (phase 15).

8.2.4 Evaluation

The observed problems during the study were related to a twice diagnosed mismatch between existing documentation and the actual realized process installation. The existence of corporate procedures appeared not to have a retroactive effect and did not lead to a systematic update of the documentation set. The motive, given by the local people, was twofold. First of all, the new corporate standard did not require a review of the existing process installations. Secondly, the fact that no accidents were reported during decades of operation, was interpreted as being an indication that the existing situation would not be really unsafe.

Confronting the local people with our observations resulted in the general opinion that the current procedures and guidelines indeed did not lead to a controlled and thus safe situation. The fact that the existing documentation was not properly maintained and kept up to date, was concluded to be the result of inadequate safety-related information about the entailed risks.

Based on the MIR level criteria as described in Section 5.2.2, it was concluded that the current SIS-related SMS was not under control. To explain this problem in order to solve it and prevent similar problems in future, a MIR assessment was carried out with regard to this particular safety-related information. It was concluded that the current information flow only met the requirements of MIR level 1 and 2, i.e. only information about *what* needed to be modified or changed was distributed. The fact that no rationale was given *why* (MIR level 3) this modification needed to be incorporated in the documentation set, was concluded to be the root cause.

8.3 Review case 1, adapted strategy case 2

During case study 1, the developed activity flow chart was primarily based on information obtained from the existing safety-related documentation. Analysis of each document and verification of documentation management resulted in the developed flowchart. Analysis of this flowchart revealed inconsistencies, shortcomings and other inadequacies. However, during the course of the project execution it appeared that in reality at substantial points was deviated from the formal described. This observation led to the conclusion that a SLM analysis should not be restricted to a verification of formal procedures and documentation to allocate inadequacies with official standards (e.g. IEC 61508 and ANSI/ISA S84.01) and regulations (e.g. Seveso II Directive). Also the actual situation should be revealed and compared with the desired situation ('*Ist*' situation versus '*Soll*' situation.). A well-proven method to do this is by interviewing the people involved in the identified safety-related activities. To cope with the above-described problem, the questions asked during the interviews were therefore concentrated on three sub-areas (see also Figure 40):

- Formal situation : What is officially defined? E.g. in corporate standards, procedures or work instructions.
- Actual situation : What is the actual situation? E.g. actual working methods, realized installations, transfer of information.
- Ideal situation : Which situation is desired? E.g. compliance with legislation, official guidelines and national or international standards.

One can imagine that in reality at certain points is deviated from the formal described situation. (If for instance the procedures are experienced to be not practical.) Of crucial importance is to find out *why* at certain point is deviated from the formal situation. Only then it will be possible to define and implement adequate improvements. From that point of view, it is presumed that any information on the discrepancy between these three situations is considered to be very useful to reduce these discrepancies.

8.4 Case 2 – ANSI/ISA S84.01 safety lifecycle model analysis of a Dutch site of an American chemical company

Based on experiences with the first case study, it was decided to start the second case, based on interviewing people, in order to create a picture of the actual situation. This actual situation was subsequently analyzed in order to allocate shortcomings or deficiencies compared to the desired situation (in this situation compliance with ANSI/ISA S84.01 – 1996). As far as the actual situation appeared to meet the requirements of the desired situation, verification was carried out in order to check whether the actual situation corresponded with the formal situation as in standards procedures and work instructions. A questionnaire was developed as a basis for the interviews.

8.4.1 Introduction

This case study was performed in the beginning of 1999, at a chemical plant of an American company, operating in the mid-west of the Netherlands. At this plant, an ANSI/ISA S84.01 compliance study (which is the sector-specific standard for process

industry facilities in the United States) was carried out. Particular attention was paid to the process of exchange and transfer of safety-related information. The motive for this study was the result of earlier experiences gained during a SIL validation study that was carried out the year before. At that time, the actually achieved safety integrity levels of a specific unit were determined. During this study it appeared to be sometimes very difficult to gather the required information, which was essential to adequately validate the safety-instrumented functions, and in some cases it appeared that the required information was not available at all. Based on these experiences it was agreed to start an additional study regarding the SMS with respect to the application of the SIS.

The plant in the Netherlands is one of many sites owned by this company, and on corporate level an engineering standard had been developed with regard to the design of safety-instrumented systems. This standard was developed at the headquarters in the U.S., and subsequently distributed to the various sites.

8.4.2 SLM assessment plan

As a first step, the existing corporate standard was reviewed in order to allocate discrepancies with the ANSI/ISA S84.01. (An essential line in the scope definition of this corporate standard stated that the requirements in this standard were consistent with requirements in ANSI/ISA S84.01.)

A very striking immediate conclusion however, was the fact that no safety lifecycle model was defined in the corporate standard.

A second activity concerned the interviewing of involved employees. People that were interviewed: HAZOP leaders, HSE manager, instrumentation engineers, operation engineers and maintenance engineers. Based on the SAM model, a questionnaire was developed which served as the basis for the interviews of the involved people. (See annex C for an overview of this questionnaire.) The questions concerned the following topics:

- Safety awareness in general
- Position of the interviewee with regard to the ANSI/ISA S84.01 safety lifecycle
- Process safety; objectives, strategy and policy
- Expertise of the employees
- Safety-related activities
- Communication methods and information flows
- Safety-related document control

In order to create awareness and commitment to cooperate with this study an introductory presentation was given. Secondly, each involved person was informed about the content of the interviews by sending out an informative brochure about these interviews. Furthermore, it was explained to all interviewees that information would be treated confidentially.

8.4.3 Assessment scope

The company's policy is to apply the principle that all processes should be designed to be inherently safe when ever possible. This is mainly achieved during the design stage of the process as part of the so-called Front End Loading stages (FEL 1 – 3). Based on P&IDs and other safety-related documents, a Process Hazard Analysis (PHA) will be carried out. During the PHA, the safety-instrumented functions are defined and classified.

Subsequently the safety-instrumented systems need to be realized, after which the process installation can be commissioned. Based on information obtained during the research, a safety lifecycle model was developed by the researchers. This is graphically presented in Figure 43.

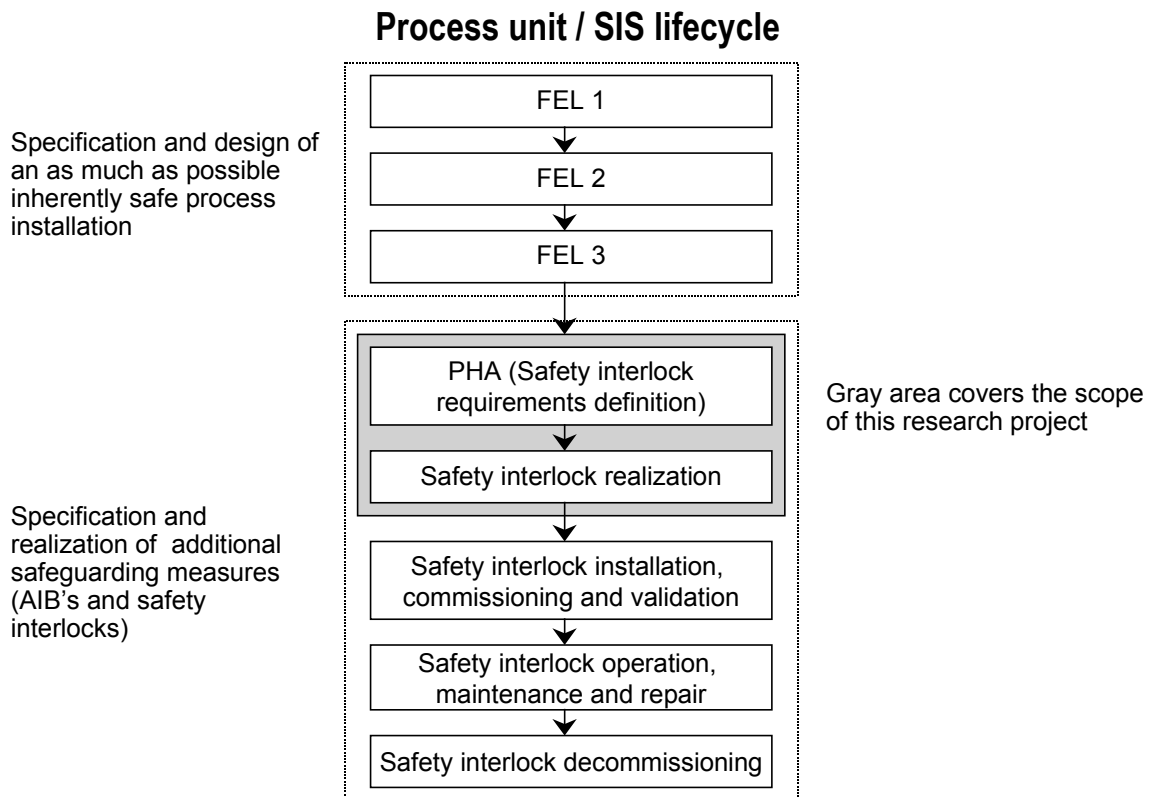


Figure 43 SIS lifecycle model as resulting from the case study

The study concentrated on the stages, Process Hazard Analysis (including interlock requirements definition) and Safety Interlock realization (gray arched stages). Following sections describe the different aspects of these stages.

8.4.4 Assessment results

Classification of risks

Standard ANSI/ISA S84.01 and IEC 61508 describe, as part of the safety lifecycle, a specific phase during which a hazard and risk analysis needs to be performed. Only IEC 61508 has defined requirements concerning this phase (phase 3) how to carry out such an analysis. ANSI/ISA S84.01 does not elaborate on this phase, as this is covered by other U.S. legal requirements. Nevertheless, it might be obvious that it is of essential importance that potential hazardous situations are properly identified and related risks are correctly estimated and classified.

For the reason that the researchers have no particular expertise in the area of hazard identification (HAZOP) techniques, only the risk classification method is investigated. The corporate standard describes two methods on how to carry out a risk analysis. Through the application of a risk matrix, a first estimate of the magnitude of the risk, is obtained. In case the involved risk is estimated to be relatively high, this risk shall be

accurately analyzed, using appropriate techniques like e.g. Fault Tree Analysis (FTA). How to execute an FTA is not further described. In case the risk is estimated to be relatively small, no other risk analysis method has to be applied but instead, the Automated Independent Backup (AIB) method can be applied to classify the safety interlocks.

For the reason that the company standard is defined in the U.S. on corporate level, and because the local Dutch legislation has to be applied as well, this plant uses a self-defined risk matrix. The researchers established that this risk matrix is only used to determine whether a certain hazard is a SHE (Safety Health or Environment) event or not. The researchers could not obtain clarity whether risks are considered to be (just) acceptable.

Interlock classification

In contradiction to IEC 61508, standard ANSI/ISA S84.01 has only defined three safety integrity levels (SIL 1 – SIL 3). Depending on the extend to which a certain risk needs to be reduced, a specific safety integrity level has to be realized. The higher the SIL, the higher the safety availability (reliability) of the SIS should be. Both standards ANSI/ISA S84.01 and IEC 61508 include examples of methods on how to classify safety-instrumented systems. (Risk matrix, risk graph, etc.)

The company has also defined different levels with regard to the classification of its safety-instrumented systems. This classification consists of 5 levels, class A up to class E. It appeared to be rather confusing to the researchers that both the SHE events as well as the interlock classification uses the categories A – E. Therefore, for instance it is possible that a class A event can be protected by 2 safety interlocks of class A, or by means of the application of an other technology based safety-related system in combination with 1 safety interlock class B.

Specification of safety requirements

The requirements concerning the design and reliability of safety-instrumented systems depend on the SIL that needs to be realized. As discussed in the previous section, the company has defined 5 safety interlock levels. Based on the risk analysis, the required interlock class is determined. The corporate standard uses examples of typical architectures on how to realize a specific safety level. However, during the interviews, it appeared that these 'typicals' do not always offer suitable solutions. Therefore, in practice one might deviate from the initial design as part of the corporate standard.

The company's policy is to make these adaptations as much as possible in line with one of the examples. Unfortunately however, this is no guarantee that the final realized safety-instrumented system is as reliable as required.

Safety lifecycle implementation

At this moment in time the corporate standard does not contain a defined safety lifecycle. It is obvious that in a situation where no lifecycle is defined, this doesn't automatically mean that the requirements per phase are not met. All activities, which need to be carried out per phase, can in practice be performed correctly. (For example, if no phase with respect to maintenance and inspection is defined, it does not mean that no maintenance or inspection is carried out at all.)

The perception of the researchers is that the phases, as mentioned in the IEC 61508 Overall safety lifecycle, are to a certain extent covered by the company. In order to allocate the complete set of activities, as mentioned in this lifecycle, proved to be a difficult task.

Communication and information transfer

The safety lifecycle of ANSI/ISA S84.01 contains 12 different phases. The IEC 61508 Overall safety lifecycle contains 16 phases. For each phase specific objectives need to be realized, and activities need to be carried out. It might be obvious that activities can only be carried out properly if also the preceding activities are correctly performed and the outcome is correctly processed in the following phase. To realize this, it is of essential importance that the results of a carried out activity are well documented and an appropriate information transfer is in place to the people responsible and the performers of the following phase. Appropriate communication and mutual adaptation is of essential importance.

It has appeared that the manner the plant is operated, is characterized by frequently working in teams. Due to an extended 'overlap' of the different teams (through people being part of more than one team), it is the perception of the researchers that a proper communication, cooperation and mutual adaptation is achieved.

Application of standards

To realize the required safety performance, application of standards can offer a positive contribution. With regard to process safety, it is the general attitude that companies consider compliance with applicable standards to be the best prove that an acceptable safety level is achieved. The American Occupational Health and Safety Administration (OSHA) recently declared that compliance with ANSI/ISA S84.01 is considered as good engineering practice concerning the Process Safety Management (PSM) aspects of regulation OSHA 1910.119. A similar development is at the moment going on in the European Union. IEC 61508 is in 2001 adopted by the EU and has become a harmonized European Norm, and might subsequently be part of the reference list of safety-related European Directives (e.g. the Low Voltage Directive (LVD)).

This corporate standard mentions that it is in conformance with ANSI/ISA S84.01. The researchers have the opinion that for a number of aspects this is the case, but that clear references to ANSI/ISA S84.01 are lacking. Furthermore, it is established that reading the corporate standard, many references are made to other corporate standards.

Although the corporate standard has a reference list describing relations to other standards, it is the perception of the researchers that an overview of the mutual relations is difficult to make. During the interviews with the involved employees, it appeared that they too find it difficult to put all standards in the correct perspective and obtain an overview.

Knowledge, expertise and safety awareness

Extensive knowledge and experience of those who are responsible for the definition, realization, and operation of safety-instrumented systems, might probably be *the* most important aspect to achieve a reliable, effective and efficient safety system. IEC 61508 part 1, clause 6 'Management of functional safety' and annex B 'Competence of persons', describe a list of competence factors of persons who are involved in the realization or

application of SIS. The standard however, does not in detail describe for each phase which requirements these people should comply with.

To realize an appropriate SIS, proper knowledge is required concerning the involved production process as well as the applied equipment. Unfortunately, the researchers have no specific expertise on the company's chemical processes. The judgment of the researchers is therefore restricted to obtaining an impression of the knowledge and experience concerning the application of safety-instrumented systems.

In the opinion of the researchers, due to a large variety of measures in combination with the complexity of the company and its internal standards, it is the perception that a high safety level is achieved. Nevertheless, it is also the perception of the researchers that only few employees substantially have an idea of 'how' safe the achieved level is. The application of a clear and unambiguous risk analysis method and the subsequent SIL classification method could contribute to this.

8.4.5 Evaluation

Most remarkable observation was the lack of a safety lifecycle model in the corporate standard. As a result of this, it appeared that no appropriate communication channels existed for exchanging information between the department responsible for the definition of the safety-instrumented systems and the departments who were responsible for the operation, testing and maintenance of the SIS.

A closed learning loop between the departments that represented different lifecycle phases was therefore not realized. Figure 44 shows the SIS-related safety lifecycle model as observed during the study.

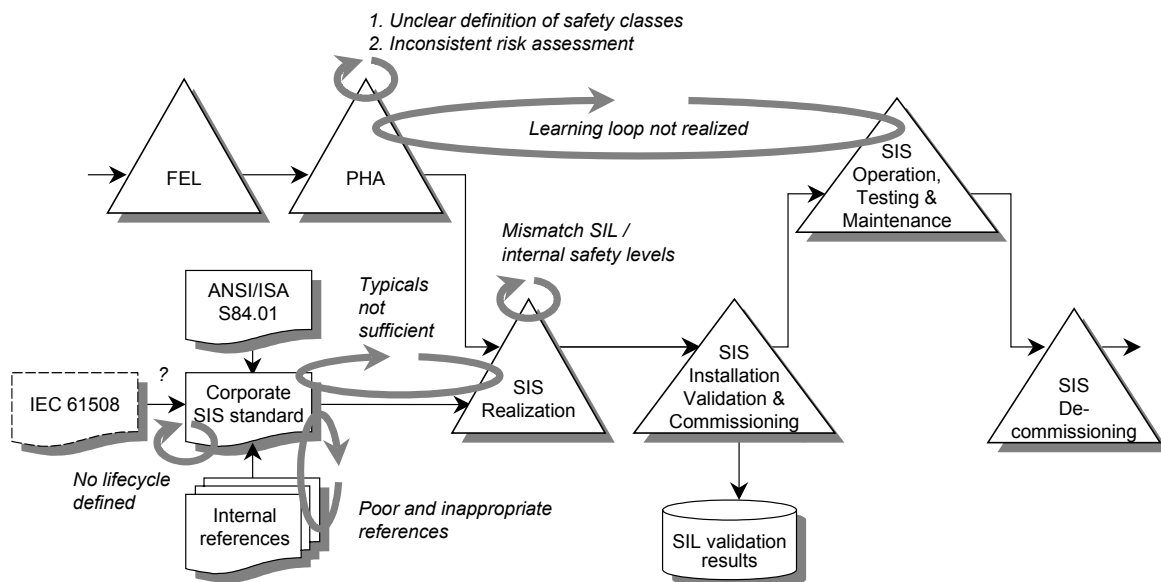


Figure 44 The observed SIS-related safety lifecycle model

Another striking observation, related to the unclear risk assessment method, is the definition of safety classes. Discussions with the interviewees on the safety classes led to significant confusion during the discussions. It appeared that various interviewees had a different interpretation on the application of the risk assessment method and on the consequently required safety class.

Furthermore, the corporate standard did not give enough guidance with regard to the design of the SIS. The list of typicals appeared not to be sufficient and did not offer a solution for every SIS design. At last, it was observed that poor references were made to other corporate standards, without adequate explanation of the scope and objectives of these standards.

In general, it was concluded that the lack of a safety lifecycle model had resulted in a poor structure with regard to mutual linked safety-related activities. The transfer of information from the HAZOP study to the people who were responsible for the operation and maintenance of the SIS only achieved a MIR level 2. However, according to the researchers, at least a MIR level 3 is required to control that the SIS requirements would be adequately implemented. Improvement of the SIS performance during operation is only realized if a feedback loop i.e. a learning loop (MIR level 4) between these lifecycle phases is established.

8.5 Recapitulation of case studies 1 and 2

As indicated in 8.1, the first two case studies were performed while the MIR-based SLM analysis technique was not yet completely developed and formalized. Lessons learned from these two case studies strongly influenced the development of the MIR-based SLM analysis technique. These lessons will be discussed in this section.

Companies that have to comply with certain regulations or standards will have to be able to prove that they indeed do so. This means that also in case of a serious accident, evidence must be available that shows that compliance is achieved. Today, creating a set of documents in general does this. During a safety assessment or during an incident investigation this documentation is considered as the primary source of information that is consulted. Therefore, during case study 1, a strong emphasis was laid on reviewing the existing safety-related documentation. One of the lessons learned from this case was that it was experienced to be difficult to check the completeness and structure of the documentation set. The solution was to develop the activity flowchart based on the safety lifecycle model as defined by their corporate standard and the IEC 61508. This resulted in the definition of the 2nd and 5th step of the MIR-based SLM analysis technique.

Furthermore, it was established that the documentation set was not always consistent with the actual situation (as is described in Section 8.4). In order to establish the actual existing situation, analyzing what is, and has been done in reality, can only lead to this kind of information. This could be done by speaking with people involved and examine the physically implemented safeguarding measures. Therefore, the step 3 '*identification of involved persons*' has been defined.

The first 5 steps of the MIR-based SLM analysis technique are intended to create an overview of the currently performed safety-related activities and business processes. As part of the development of the analysis of this overview of activities, the MIR concept has appeared to be well fitting with regard to analysis of the case study results. Particularly, the classification of information appeared to be effective with regard to the qualification of the observed problem. Therefore the MIR concept has been implemented in the development of step 7 '*evaluation of the analysis results*'. One original design aspect of the MIR concept is to determine the actually achieved MIR level of the business processes and compare this with the required MIR level. However, it appeared to be sometimes difficult to determine the precise MIR level of the business processes. The difficulty concerned the fact that these business processes are sometimes of very complex nature.

The observation is that these business processes show aspects of different MIR levels. This leads to the conclusion that a MIR level could only be allocated to a specific part of the business processes. This resulted in an adaptation of the application of the MIR concept where MIR levels are to be determined for specific information flows. As part of the 7th step, the MIR-based SLM analysis technique, comparison of the actually achieved MIR level of the information flows with the required information flows, is defined.

The following section will discuss 9 other case studies. The value of the application of the SLM concept and the MIR-based SLM analysis technique will be discussed and evaluated.

8.6 Evaluation of all case studies

The previous sections gave an overview of two case studies. Based on the results and experiences of these cases, the MIR-based SLM analysis technique has been further developed. Annex A gives an overview of another nine case studies. These 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 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 8 gives an overview of the comparison results. Subsequently, the description of these aspects and the results of the evaluation are discussed.

Table 8 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

— 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 try 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 standards, but were confronted with certain requirements of a 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 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 a 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 chapter 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 [Nun99]. 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.

8.7 Conclusions on all 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 has 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 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.

8.8 Discussion on 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*

As discussed in Chapter 6, two diverging SLM models, namely line management and process flow management, are identified. However, literature on organizational structures describe many more management models [Vel87], [Jäg91], [Min92]. 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’ (see description in 6.8) 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 following chapter will discuss the overall conclusions of this research and will give recommendations for further research.

9 Conclusions and recommendations

The main purpose of this study is to design a new safety management concept. As described in 2.1.1, the design should, on one hand, focus on implementation concepts and on the other hand, focus on the development of techniques that are able to measure the degree to which these concepts are implemented. This resulted in the definition of four research questions in Chapter 2, which were extended with a fifth research question in Chapter 5.

In Section 9.1, the main conclusions of the study will be summarized and the research questions will be answered. In Section 9.2, a number of proposals for further research will be discussed.

9.1 Conclusions

9.1.1 Observed new kind of problems due to growing complexity of systems and organizations in the process industry

As discussed in Chapter 1, many, sometimes even major, industrial accidents still happen today in the process industries. During the last few decades, the ‘traditional’ approach to control process safety was to take an additional safety measure based on lessons learned from the occurrence of a new accident. Problems with the process installation usually resulted in the development of a new additional technical measure.

Recent investigations on accidents, however, show a complicated relationship between a relatively high number of safety-related problems and the occurrence of the final hazardous event. These problems appear to be the result of the growing complexity of the process installations, where the capacity of the installations are increasingly pushed to their physical limits, and more and more products are produced by a single installation. Furthermore, the development of process control and safeguarding instrumentation has led to an increasing application of microprocessor-based PLC systems, which are highly complex systems compared to previous relay-based systems. Also, in parallel with these developments, the complexity of the plant organization has increased, in which sub-system suppliers and engineering contractors are increasingly responsible for certain parts of the processes [Kne01]. Finally, today the organizations are characterized by reduction of staff, outsourcing of expertise and a relatively large turnover of labor and staff.

Recent studies, such as performed by the British Health and Safety Executive, illustrate that the majority of the root causes of the problems leading to a hazardous event are not just the result of inadequate, unreliable equipment, but much more the result of poor process safety management [HSE97]. Based on these kinds of studies it is concluded that the control of safety-related business processes has become an increasingly important aspect with regard to the control of process safety. During the last decade, this aspect has been recognized and has led to the development of a number of techniques, such as near miss reporting, and bench-marking techniques that focus on the control of process safety by controlling so-called key performance indicators. These techniques, however, apply a kind of ‘black box’ approach, where precise relationships between control parameters are still not considered.

9.1.2 Observed need for implementation rules of safety lifecycle models

This study has shown that recent standards on safety instrumented systems emphasize the use of so-called safety lifecycle models. The intention of these lifecycle models is to structure the safety requirements, also in relation to the business processes, and make it easier to implement and verify them. Through these standards, safety lifecycle models are therefore considered to form a framework to control all of the safety-related activities that are involved [IEC61511]. The observed questions and problems that companies currently struggle with were how to define, validate and analyze lifecycle models in order to utilize them to control safety-related activities and thereby control process safety. It was furthermore observed that the root causes of typical problems with a safety-instrumented system occurred during many stages of its lifetime [HSE95]. This observation stressed the need for a structured approach to control problems at all lifecycle phases.

9.1.3 Solutions designed, based on the research questions

Based on the observation that the complexity of organizations and process installations has significantly increased, and the conclusion that current safety management techniques are still very much restricted to ‘black box’ approaches, the need for a more structured control of the safety-related business processes has been established. It is subsequently proposed that the safety lifecycle models defined in SIS-related standards might serve as a new structure to measure, analyze, control and improve the safety-related business processes. Therefore, the research objective was defined to design a new safety control concept. As described in 2.1.1, the design should, on one hand, focus on implementation concepts and on the other hand, focus on the development of techniques that can measure the degree to which these concepts are implemented. This objective resulted in 4 research questions as described in Chapter 2.

To develop a better understanding of process safety management in relation to the control of safety-related business processes, in Chapter 5, aspects of measurement and control engineering and system theory were discussed. It was concluded that knowledge exchange plays an essential role to control the business processes. Therefore, the quality of communication, documentation and information flows need to be controlled.

Recent studies have shown that the development of the MIR concept proves to be an effective means to analyze reliability-related information flows, and the capability of an organization to control reliability-related business processes [Bro99], [Bro00]. The MIR concept was primarily developed in the consumer products industry with relatively high numbers of product problems and it was questioned whether this concept would be applicable to control safety-related business processes. A 5th research question was therefore further specified in this chapter, concerning the applicability of the MIR concept in the area of process safety management. In particular, it was focused on the added value of qualification of safety-related information flows in order to control safety-related business processes as part of the SIS safety lifecycle.

◆ *Research question 1*

Research question 1 concerned whether and how safety lifecycle models can support the control of safety-related business processes.

The development of the SLM concept together with the SAM and SLAM models, and the development of the formalized MIR-based SLM analysis techniques, illustrate how

lifecycle models serve a structured framework on which the SLM activities are based. The demonstration of the relationship between safety-related activities and safety lifecycle models results in the conclusion that this knowledge improves the ability to control the concerned business processes. With that, it positively confirms that using lifecycle models indeed supports the control of safety-related business processes. Implicitly, this conclusion is supported by the discussion on the answers to the other research questions that illustrate the added value of using lifecycle models.

◆ *Research question 2*

Research question 2 concerned what exactly is phased (what is included in a lifecycle phase) and which other factors determine the quality of what is included in each phase. In Chapter 6, it was established that it would need to be determined which information flows need to be controlled. Key words consistent with the MIR framework, such as 'why', 'where', 'when', 'who', 'what' and 'how', were used to answer that question. Based on the outcome of this, the safety-related activity management (SAM) model has been developed. This model describes the key parameters that determine the performance of the subject safety-related activity. The SAM model represents relevant aspects that determine the quality of a lifecycle phase, and with that answers research question 2.

◆ *Research question 3*

Research question 3 concerned how, specifically, the quality of information exchange between lifecycle phases could be controlled.

As described in the second part of Chapter 6, the inter-relationship between these activities and the role of information flows is captured by the development of the safety lifecycle activities management (SLAM) model. Subsequently, safety lifecycle management is defined, as the application of these two models to manage process safety. The stepwise implementation scheme as developed in Section 6.7, describes the implementation process of the required information flows between the identified and allocated safety-related activities. The quality of information exchange directly depends on the correctness and completeness of the implementation of these steps. This quality can be expressed by determining the achieved MIR level.

◆ *Research question 4*

Research question 4 concerned how relevant aspects and parameters could be measured in order to get to know whether these parameter settings need to be adapted.

Based on the development of the SLM concept, it was concluded that its validity could only be demonstrated if a method, which is based on this concept, would indeed have the ability to analyze the safety-related business processes and detect the new type of safety-related problems (as discussed in Section 1.5). This resulted in the development of the formalized MIR-based SLM analysis technique (see Table 9). This analysis technique consists of 7 steps that led to the detection and explanation of safety-related problems. An additional 8th and 9th step have been added which define control and modifications.

Table 9 *MIR-based SLM analysis steps (copy of Table 6 Chapter 7, Section 5.2)*

MIR-based SLM analysis	
Step 1	SLM analysis scope definition
Step 2	Safety lifecycle definition
Step 3	Identification of involved persons
Step 4	Collection of information on SR activities
Step 5	Development of the activity flowchart
Step 6	Analysis of the SR activity flowchart
Step 7	Evaluation of the analysis results
Step 8	Identification of appropriate modifications
Step 9	Implementation of modifications

One of the main aspects of 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 activity and information flowcharts. First experiences with the use of the analysis technique have shown that indeed a reasonable explanation of safety-related information transfer problems could be given, which otherwise would have likely been difficult or not explainable. Based on a number of case studies, these safety lifecycle model based activity flowcharts have proven to be a valuable means to explain the observed problems. Using these models, a relationship could be demonstrated where observed problems appeared to be primarily the results of inadequate communication and information exchange. This was particularly true for problems that were related to the differences in perception between people who are involved in inter-related activities. Poor quality of information that is exchanged is one of the main reasons. The development of formalized information transfer flowcharts makes it possible to establish prerequisites of information transfer between people who are involved in these inter-related activities.

◆ *Research question 5*

A fifth research question, as discussed in 5.7, concerned the applicability of the MIR concept in the area of process safety management.

The application of MIR levels, as criteria to determine the quality of the subject information flows, has shown to be an effective means to explain possible shortcomings of the quality of information exchange that is actually achieved versus the required quality level. Particularly, the adapted application of the MIR concept as described in 7.3.3 appeared to be a welcome enhancement with regard to the establishment of necessary improvements. The original MIR analysis technique was macro-oriented and tried to arrive at judgment of the achieved MIR level, which is made on the organization as a whole, whereas the MIR-based SLM analysis technique focuses on the quality of specific information flows.

9.1.4 Validation results of the designed solution

Based on a number of case studies performed at different companies in the process industry, it is concluded that by applying the developed SLM concept and the formalized MIR-based SLM analysis technique, safety-related problems are very well detectable and explainable, and can assist in finding a solution. It is concluded that the observed problems are not by definition relatively complex of nature. Common characteristic of the majority of problems with the application of safety instrumented systems appeared to be related to inadequate control of the safety-related business processes (see case studies). The difficulty in modern process industries is that apparently simple problems appear to be hidden and remain unrevealed due to the complexity and obscurity of its organizations. The added value of the MIR-based SLM analysis technique is its power to reveal and solve these problems.

9.1.5 Recapitulation of the conclusions

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

9.2 Discussion and recommendations on further research

This discussion starts with the following proposition: ‘A company that does not know how reliable its safeguarding measures are, also does not know how safe its process installations are.’ The intention of definition of safety integrity levels by safety standards is to express the reliability of a SIS and therefore achieve a level of risk reduction. Obviously, the level of risk reduction is not intended to indicate the reduction at a certain moment in time, but much more for a certain time period. The definition of safety lifecycle models by safety standards can therefore be considered as a first step to realize and control the required level of risk reduction for a specific time period. The predictive aspect of this new approach directly illustrates the role of adequate information control. Safety assessments, however, are today still very much characterized as being a momentaneous impression of the safety level of a company. It is the expectation that the MIR-based SLM analysis technique might become an important basis to do a kind of predictive assessment of the safety level for a specific time period. This leads to the first recommendation:

- 1. At this moment, the MIR-based SLM analysis technique does not make a prediction of the achieved risk reduction or plant safety level. Further research is needed to develop this predictive aspect.*

Despite the fact that during the case studies the companies involved positively cooperated with the researchers, it must nevertheless be noticed that safety-related problems were not always openly discussed. The conclusion that employees might be seriously injured or killed is still not always openly communicated. Obviously, successful application of the

MIR-based SLM analysis technique directly depends on the openness of the organization and its preparedness to disclose all relevant safety-related information. This results in the second recommendation:

2. *Methods need to be developed to support these kind of safety studies and create awareness and commitment with the subject organization in order for them to cooperate.*

Another aspect that was observed during the case studies was that it was difficult to deduce and filter the required information from the large amount of information that was frequently made available. 'Fuzziness' is a term that is often used to describe the level of uncertainty associated with the risks due to imperfect knowledge or information in risk management [Jab95]. This results in the third recommendation:

3. *Techniques need to be developed to analyze and control the fuzziness of information. Obviously, the higher the fuzziness, the less clear and thus less reliable or accurate the information will be [Lu01], [Lu02].*

Further research should be performed in order to obtain a better understanding of the development and evolution of safety-related information. It is assumed that processing this information increases the quality level of information. Therefore, criteria should be developed that determine the quality of measurement of a particular safety-related parameter, the quality of information transfer mediums and the quality of safety-related information implementation techniques. During the case studies, a number of problems were detected and explained by the establishment of the MIR level of the safety-related information. The researchers determined the need for a specific MIR level based on their expert perception and judgment. Techniques need to be developed in order to establish the need of a specific MIR level. Standards do not currently require that quality levels are applied to information flows. Furthermore, criteria should be developed in order to determine the degree to which an organization meets the MIR level requirements of their information flows. Based on these criteria, an overall indication could be given on the maturity level of information control of its business processes. This results in a fourth recommendation:

4. *Techniques should be further developed in order to determine the maximum MIR level that can be achieved if certain existing safety and reliability analysis methods are used.*

10 Bibliography

- [Acu02] Acu Tech Consulting Inc. – AcuSafe Newsletter January 2002.
<http://www.acusafe.com/Newsletter/Stories/0102News-MonthlyIncidents.htm>
- [Ake99] Aken, van Joan E. – Management theory developments on the basis of the design paradigm – The quest for tested and grounded technological rules
Eindhoven University of Technology
Report EUT/BDK/93, Eindhoven 1999
- [And87] Andreasen, H.M. and Hein, L., – Integrated Product Development
IFS Publications Ltd. 1987
- [AT&T90] AT&T – Quality Manager’s Handbook
Published by AT&T Quality Steering Committee
AT&T customer information center.
Indianapolis, U.S. 1990
- [Bel00] Belke, James – Chemical accident risks in U.S. industry – A preliminary analysis of accident risk data from U.S. hazardous chemical facilities
EPA, September 2000
www.denix.osd.mil/denix/public/intl/mapp/dec99/belke/belke.html
- [Bra94] Brassard, M., Ritter, D. – The Memory Jogger II
Goal/QPC Methuen, USA 1994
- [Bra96] Bralla J.G. Bralla – Design For eXcellence
Mc Graw-Hill. 1996
- [Bra99] Bradley, – “The Reliability Challenge” Presentation handouts
Conference London. 1999
- [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
- [Bro01] Brombacher, A.C. et. al – Bedrijfszekerheid van technische systemen bij veranderende bedrijfsprocessen
Bedrijfszekerheid 2nd quarter 2001 issue
- [Bro92] Brombacher, A.C. – Reliability by Design
John Wiley & sons. 1992

- [Bro97] Brombacher, A.C. – “The Reliability Challenge” Presentation handouts
Conference Regent’s Park London. 1999
- [Bro99] Brombacher, A.C. – MIR: Covering non-technical aspects of IEC 61508
reliability certification, Reliability Engineering and System Safety 66.
1999
- [Car92] Carter, D.E. and Stilwell Baker, B. – Concurrent Engineering
Mentor Graphics Corporation. 1992
- [CCPS89] Center for Chemical Process Safety (CCPS) – Guidelines for Technical
Management of Chemical Process Safety
New York: American Institute of Chemical Engineers. 1989
- [CCPS93] Center for Chemical Process Safety (CCPS) – Guidelines for Safe
Automation of Chemical Processes
New York: American Institute of Chemical Engineers. 1993
- [CCPS96] Center for Chemical Process Safety (CCPS) – Inherently Safer Chemical
Processes: A Life Cycle Approach
New York: American Institute of Chemical Engineers. 1996
- [CFT94] Centre of Manufacturing Technology– Concurrent Engineering Handbook
Internal report CTR598-94-0115
Philips Electronics N.V. Eindhoven, Netherlands 1994
- [Cha91] C. Chatfield – Statistics for technology, a course in applied statistics
Chapman & Hall. 3 edition 1991
- [Dap01] Dapena, P. Rodríguez – Software Safety Verification in Critical Software
Intensive Systems
Ph.D. thesis, Eindhoven University of Technology, Beta 2001 (to be
published)
- [Das78] Dassen, B.J. – Program flowcharting for business data processing
Chichester, Wiley 1978
- [Dow97] Dowell, A. M., III – Layer of Protection Analysis: A New PHA Tool,
After HAZOP before Fault Tree Analysis
Presented at Center for Chemical Process Safety International Conference
and Workshop on Risk Analysis in the Process Safety, Atlanta, GA.
October 21, 1997
- [Dow98] Dowell, A. M., III – Layer of Protection Analysis for Determining Safety
Integrity Level.
ISA Transactions 37 155-165. 1998
- [dTR84.02] ISA dTR84.02 version 3 December 1997- 67 Alexander Drive, P.O.
Box 12277, Research Triangle Park, NC 27709

- [EC96] Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances
Official Journal L 010 , 14/01/1997 p. 0013 – 0033
- [Fel01] Felton, Bob – Safety study IDs leading causes of accidents
InTech p.77, March 2001
- [Fis93] Baruch Fischhoff, Sarah Lichtenstein, Paul Slovic [et al.]. – Acceptable risk
Cambridge University Press, Cambridge, 1993
- [Fry96] Fryman, C. – Managing HazOp Recommendations Using an Action Classification Scheme
AIChE Spring National Meeting, New Orleans, LA, February 25-29, 1996
- [Git84] Gits, C. W. – On the maintenance concept for a technical system, a framework for design
Eindhoven University of Technology
Dissertatie Drukkerij Wibro, Helmond, Netherlands 1984
- [Gob92] William M. Goble – Evaluating Control Systems Reliability, Techniques and Applications ISA books 1992
- [Gob98] William M. Goble – The use and development of quantitative reliability and safety analysis in new product design. Ph.D. thesis
University press facilities, Eindhoven University of Technology, the Netherlands 1998
- [Gre95] Green, D. L., and A. M. Dowell, III – How to Design, Verify, and Validate Emergency Shutdown Systems
ISA Transactions 34, 261-72 1995
- [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
- [Hee99a] Heel, K.A.L. van – Safety lifecycle management in the process industries
MSc thesis Eindhoven University of Technology 1999
- [Hon90] Hon Lord Cullen – The public inquiry into the Piper Alpha disaster
Department of energy London, HSMO November 1990
- [Hou01] Houtermans M.J.M. – A method for dynamic process hazard analysis and integrated process safety management
Ph.D. thesis Eindhoven University of Technology, 2001
- [HSE95] Health and Safety Executive – Out of control
HSE books, United Kingdom 1995

- [HSE97] Health and Safety Executive, clause 6.2 of Contract Research Report 139/1997, 'Explosions in gas-fired plant' United Kingdom 1997
- [Hui98] Huijben A.J.M., Sonnemans P.J.M., Geudens W.H.J., Brombacher A.C., Wolbert P.M.M. – Reliability improvement, a generic approach? Proceedings of the ESREL '98 conference, page 359-366, Trondheim, Norway, 16-19 June 1998
- [Hum89] Humphrey, Watts S. – Managing the Software Process Reading, MA: Addison-Wesley, 1989
- [IEC60051] ISO/IEC Guide 60051 second edition (1997 draft)
- [IEC60300] IEC 60300-3-9 (1995-12) – Dependability Management Part 3: Application guide – Section 9: Risk analysis of technological systems
- [IEC61078] IEC 61078 – Analysis techniques for dependability – Reliability block diagram method, 1991
- [IEC61165] IEC 61165 (1995-12) – Application of Markov techniques
- [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)
- [IEC62061] IEC 62061 Safety of machinery – Functional Safety – electrical, electronic and programmable electronic control systems. (Draft version 44/292/CD, 2000-09-29)
- [ISA96] ANSI/ISA S84.01 – 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709 1996
- [ISO14001] ISO 14001 – Environmental management systems – Specification with guidance for use
- [ISO51] ISO/IEC guide 51 second edition 1997 (draft)
- [ISO5807] ISO 5807 – Information processing, Document symbols and conventions for data, program and system flowcharts, program network charts and systems resources. 1985
- [ISO8402] ISO 8402 – Quality management and quality assurance-vocabulary
- [ISO9004] ISO 9004 – Quality Management and quality system elements

- [Jab95] Jablonski, M. – Recognizing knowledge imperfection in the risk management process
3rd international symposium in uncertainty modeling and analysis, and annual conference of the North American fuzzy information processing society. Proceedings of ISUMA – NAFIPS 1995
- [Jäg91] Jägers, H.P.M. Jansen W. – Het ontwerpen van effectieve organisaties. Stenfert Kroese, Leiden 1991
- [Kap92] Kaplan, R.S. and Norton, D.P. – The balanced score card – Measures that drive performance
Harvard Business Review (Jan. – Feb.), 71-79. 1992
- [Kel99] Kelly, T.P. – Arguing Safety - A Systematic Approach to Safety Case Management
Ph.D. Thesis, Department of Computer Science Green Report
The University of York, U.K. 1999
- [Kem98] Kemps, C.M.M. Cost of Safety in the Process Industry
Houston – ISA Show 1998
- [Ker98] Kerklaan, L.A.F.M., Kingma, J., Kleef van, F.P.J.– De cockpit van de organisatie 1^e druk, 6^e oplage. Kluwer Bedrijfsinformatie B.V. 1998
- [Kip96] Kipp, Jonathan D. and Loflin, Murrey E.. – Emergency incident risk management : a safety and health perspective
New York : Van Nostrand Reinhold, 1996
- [Kle99] Kletz, T. – Hazop and hazan
Institute of chemical engineers
Warwickshire, United Kingdom 1999
- [Klu98] Knegtering, B. – Handboek proces-automatisering, 5. Systemen
Kluwer Editorial, Diegem / Ten Hagen & Stam, Den Haag 1999
- [Kne00a] Knegtering, B. Brombacher, A.C. – A method to prevent excessive numbers of Markov states in Markov models for quantitative safety and reliability
ISA-transactions 39, 363-369, 2000
- [Kne00b] Knegtering, B. – The impact of IEC 61508 and IEC 61511 on Dutch industry
Epigram, official journal of Core Interest User Group of Programmable Electronic Systems London Autumn 2000
- [Kne01] Knegtering, B. – Safety Lifecycle Management
Automation in Petro Chemicals Industry Conference
Congress center Delft University of Technology, 21-22 November 2001

- [Kne98a] Knegtering, B. – Conceptual comparison of two commonly used safeguarding principles
17th International Conference SAFECOMP'98 Proceedings
Heidelberg, Germany, October 1998
- [Kne98b] Knegtering, B. – A conceptual comparison of two commonly used safeguarding principles
Petromin Asia, September 1999
- [Kne98c] Knegtering, B. Application of Micro Markov models for quantitative safety assessment to determine safety integrity levels
ISA-Expo, Houston 1998
- [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
- [Kne99b] Knegtering, B. Brombacher, A.C. – Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by IEC 61508 standard for functional safety
Reliability Engineering and System Safety 66, Elsevier 1999
- [Kne99c] Knegtering, B. – Introduction to the IEC 61508
5th symposium prevention of serious accidents
Ministry of employment and labor, Houffalize, Belgium 1999
- [Kne99d] Knegtering, B. – Implementing the new international safety standard IEC 61508: methods and tools
Hydrocarbon Asia, September 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
- [Kne99f] Knegtering, B , Bakel van, F. – Experiences with organizational aspects of implementing the IEC 61508 safety standard into an existing quality management system
Interkama, Düsseldorf, Germany 1999
- [Kno98] Knowles, Jim – Safety Management Systems, Friends or Foes?
Health and Safety Conference Proceedings
Queensland Mining Industry 1998
- [Lee96] Lees F. P. – Loss prevention in the process industries
Butterworth-Heinemann (second edition) 1996

- [Lie98] Lienhard, John H. – Acceptable risk. University of Houston
<http://www.uh.edu/engines/epi1097.htm> 1998
- [Lu01] Lu, Y., Loh, H.T., Den Ouden. E., Yap, C.M., Brombacher, A.C., –
Recognizing fuzziness in managing product quality and reliability in a time
driven derivative product development
Product Development and Management Association (PDMA) International
Research Conference, Santa Clara, USA, Sept 9-13, 2001
- [Lu02] Lu, Y., Brombacher, A. C., Den Ouden, E., Kovers, P., – Analyzing
fuzziness in product quality and reliability information-flow during a time-
driven product-development-process
Accepted for presentation at Annual Reliability and Maintainability
Symposium(RAMS), Seattle, WA USA, 2002
- [Meu95] Meulen van der M. – Definitions for hardware/software reliability
engineers, 1995, ISBN 90 9008437 1
- [MIL217] MIL-HDBK-217F – Military Handbook. Reliability prediction of
Electronic Equipment
Department of Defense USA: December 1990
- [Min92] Mintzberg, H. – Structures in five, designing effective organizations.
Prentice Hall 1992
- [Mol01] Molenaar P.A., Huijben A.J.M., Bouwhuis D., Brombacher A.C. – Why do
quality and reliability feedback loops not always work in practice?
Reliability Engineering and System Safety 2001
- [Moo83] Moore, N - How to do research
The library association - London 1983
- [Nag79] Nagel, E. – The structure of science
Hackett, Indianapolis - USA 1979
- [Nun99] Nunns, S., Hamers, A., Kneegtering, B. – The European Core User Interest
Group (CUIG) & its activities in the Conformity Assessment Arena
International Conference – European Process Safety Center
Paris, November 1999
- [ORE92] OREDA-92 – Offshore Reliability Data Handbook, 2nd Edition
Høvik, Norway: DNV Technica ISBN 82 515 0188 1 1999
- [OSHA1910] OSHA Regulations (Standards – 29 CFR) – Process safety management of
highly hazardous chemicals. – 1910.119
- [Pap99] Papadopoulos, Y., McDermid, J.A. – The potential for a generic approach
to certification of safety critical systems in the transportation sector
Reliability Engineering and Systems Safety 63 (1999) 47-66
Elsevier Science Ltd.

- [Par00] Parchomchuk, L. – Keys to successful PHA studies
AcuSafe Newsletter August 2000
- [Per84] Perrow, Charles – Normal accidents: living with high-risk technologies
New York : Basic Books 1984
- [Phi87] Phillips, E. M., Pugh, D. S. – How to get a Ph.D. Managing the peaks and troughs of research
Open university press
Milton Keynes, Philadelphia USA 1987
- [EN50126] EN 50126 – Railway applications: The specification and demonstration of reliability, availability, maintainability and safety (RAMS) for railway applications Part 0: dependability 1999.
- [RAC91] Failure Mode/Mechanism Distributions – RAC – Reliability Analysis
Center Department of Defence (DoD) 1991
Rome Laboratory, NY No. FMD-91
- [Ren90] Renshaw, F. M. – A Major Accident Prevention Program
Plant/Operations Progress 9,3 July 1990, 194-7
- [Rob90] Robbins S.P. – Organization theory, structure, design and application.
Prentice-Hall International Inc. 1990
- [Rou01] Rouvroye, J.L., – Enhanced Markov analysis as a method to assess safety in the process industry
Eindhoven University of Technology 2001
- [Rou95] Rouvroye, J.L., Brombacher A.C., et al – Uncertainty in safety, New techniques for the assessment and optimization of safety in process industry
SERA-Vol. 4, Safety Engineering and Risk Analysis, ASME, San Francisco, 1995
- [Rou99] Rouvroye, J.L., Brombacher, A.C. – New quantitative safety standards: different techniques, different results?
Reliability Engineering & System Safety, Vol. 66, No. 2, November 1999
- [San00] Sander, P.C., Brombacher, A.C. – Analysis of quality information flows in the product creation process of high-volume consumer products
Production Economics No. 67, Elsevier Science 2001
- [Sch92] Schaaf, T. van der. – Near miss reporting in the chemical process industry
Eindhoven University of Technology, 1992.
- [She98] Shell Global Solutions – Instrument Protective Function Classification
Brochure The Hague Netherlands 1998

- [Smi93] Smith, David J.– Reliability, Maintainability and Risk
Butterworth Heinemann, 4th edition 1993
- [Sol99] Solingen, R. van – Product focused Software Process Improvement. SPI in
the embedded software domain
BETA. Ph.D. thesis. Eindhoven University of Technology, 1999
- [Sou93] Suokas, Jouko and Rouhiainen, Veikko – Quality management of safety
and risk analysis
Amsterdam : Elsevier, 1993
- [STT01] Stichting Toekomst der Techniek – Betrouwbaarheid van technische
systemen, anticiperen op trends
Netherlands : STT publication No. 64, 2001
- [Sul86] Sullivan, L.P. – Quality Function Deployment. A system to assure that
customer needs drive the product design and production process.
Quality Progress, June 1986
- [Tha99] Thai Oil Refinery – Laem Chabang Thailand, Gasoline storage tank
explosion.
US Chemical Incident Reports Centre Databases. December 17, 1999
- [Tho67] Thompson J. – Organizations in action
New York: McGraw-Hill 1967
- [Vee88] Veerman, C. P., Essers, J. P. J. M - Wetenschap en wetenschapsleer, een
inleiding
Eburon - Delft, the Netherlands 1988
- [Vel87] Prof.Ir. J. in 't Veld – Analyse van organisatieproblemen, een toepassing
van denken in systemen en processen
Stenfert Kroese, Leiden - Antwerpen 1987 4th edition
- [Xin96] Leiming Xing, Karl N. Fleming, Wee Tee Loh – Comparison of Markov
model and fault tree approach in determining initiating event frequency for
systems with two train configurations. Reliability Engineering and System
Safety 53 (1996) 17-29, Elsevier Science Limited
- [Yin93] Yin, Robert K – Applications of case study research
Newbury Park SAGE, 1993. - XVI
- [Yin94] Yin, Robert K – Case study research : design and methods - 2nd ed. –
London : Sage, 1994. - XVII

Annex A Case studies

Case 3 – Fertilizer plant in Canada

A.3.1 Introduction

In spring of 1999, a SIL classification and validation case study was carried out at a fertilizer plant in Canada. This plant used to be part of a large oil company. Therefore, many of the applied standards and practices were still based on the former situation when the plant was still owned by the oil company. Because of the publication of standards ANSI/ISA S84.01 and the first parts of IEC 61508, the instrumentation department of this plant organized a workshop to gain experience with these new standards. Because of the scope of these standards, the HAZOP leaders and people from instrumentation were invited. During the workshop an introduction on the standards was given and subsequently a number of industrial cases were discussed whereby typical SIF's were analyzed.

A.3.2 Observations

During the introduction on the new safety standards, a level of awareness and commitment was created among the attendants that the concepts of these standards really needed to be implemented. The following discussion on the industrial cases however, revealed some serious implementation problems. It appeared that HAZOP leaders were not able to determine the SIL requirements for the SIF's to be applied. On the other hand, the people from the instrumentation department seriously needed this information to meet the requirements of IEC 61508. It was decided to look at the current HAZOP procedures and find out how the risk assessment was prescribed. These procedures were found in an 'old' standard developed during the period the plant was owned by the oil company. In this standard a risk matrix was described with different categories for severity of the consequences and categories for the probability that a hazardous event would take place (see Table 10 and Table 11). An amazing observation was the fact that the risk matrix appeared to be completely empty and no criteria were defined concerning the acceptable risk level. Thereupon, a discussion followed on how SIL's could be filled into the empty risk matrix. Unfortunately, the people from the HAZOP team were at that moment not motivated to fill out the matrix, for the reason that in their opinion it would restrict their freedom to define SIS requirements.

Table 10 Consequence categories

Consequence Category	Consideration			
	Health/Safety	Public Disruption	Environmental Impact	Financial Impact
I	Fatalities/serious impact on public	Large portion of a community or a large community	Major/extended duration/ full scale response	Corporate
II	Serious injury to personnel/limited impact on public	Small portion of a community or a large community	Serious/significant resource commitment	Business Unit
III	Medical treatment for personnel/no impact on public	Minor	Moderate/limited response of short duration	Production Plant
IV	Minor impact on public	Minimal to none	Minor/little or no response needed	Other (portion of unit)

Table 11 Probability categories

Probability Category	Description	Definition
A	Frequent	Likely to occur repeatedly during lifecycle of system
B	Probable	Likely to occur several times in lifecycle of system
C	Occasional	Likely to occur sometime in lifecycle of system
D	Remote	Not likely to occur in lifecycle of system
E	Improbable	Probability of occurrence cannot be distinguished from zero

To determine the risks, a risk matrix had been constructed of the four consequence classes and the five probability classes (see Figure 45). As can be seen, no SIL requirements are indicated into this matrix (as it is for instance illustrated by an example in IEC 61508 part 5). During the workshop a discussion took place in order to fill out this matrix with the needed SIL requirements.

		Probability				
		A	B	C	D	E
Consequence	I					
	II					
	III					
	IV					

Figure 45 Risk matrix of the fertilizer plant

A.3.3 MIR-based SLM analysis

The activity flowchart of Figure 46 shows part of the overall SIS safety lifecycle. The problems that were observed are located between the lifecycle phase ‘hazard and risk assessment’ and phase ‘SIS realization’.

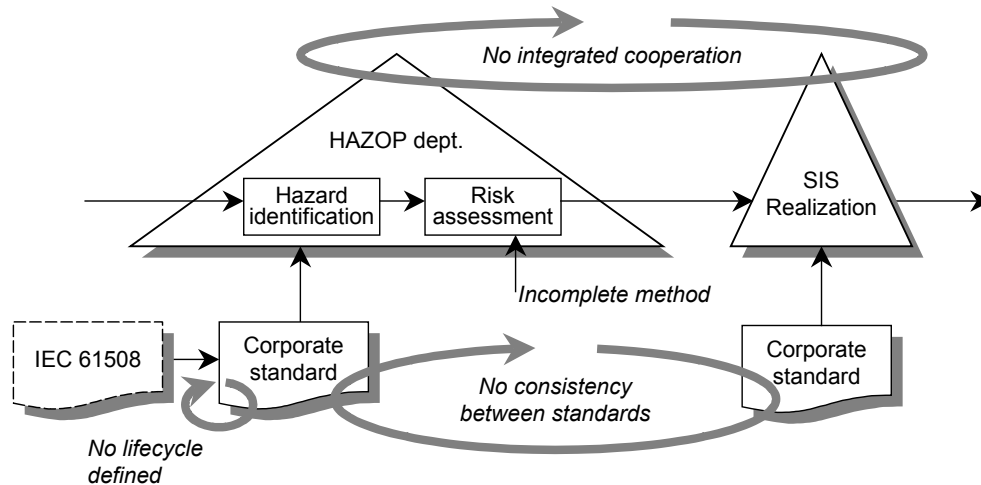


Figure 46 Activity flowchart of the HAZOP and SIS realization phases

The allocated problem concerned the lacking of consistent procedures for the various safety-related activities. No SIS safety lifecycle was defined and no SIL requirement determination technique was applied. During the workshop it was observed that only little cooperation existed between the HAZOP department and instrumentation department.

A.3.4 Evaluation and conclusions

The existence of barriers, missing information loops and learning cycles, is primarily the result of an inadequate corporate standard, which has not adopted a SIS safety lifecycle model. Therefore, the standard was characterized by inconsistent procedures for the various safety-related activities. For the reason that, during the workshop, no responsible person for managing the objectives of the activities of both the HAZOP and Instrumentation departments attended the workshop, barriers between these departments were not solved at that time. Awareness and commitment was not created by management that the objectives all serve the same goal. This barrier was probably not solved because it was experienced to be a difficult exercise to determine and name the risk levels and specify requirements in order to reduce the risks to an acceptable level.

Based on the MIR model criteria it was concluded that only a MIR level 1 was achieved. Only restricted information was transferred from the HAZOP department to the instrumentation department, concerning the need to apply a SIS. No information was transferred with regard to the required integrity level the SIS should realize. Furthermore, no control loop was observed that verified whether the complete set of safeguarding measures indeed realized the required risk reduction and achieved an acceptable residual risk level (as required by MIR level 3).

Case 4 – An American oil company

A.4.1 Introduction

This case describes the SIL validation study, which was performed in autumn of 1998. An American oil company ordered the SIL validation study, where a total of 15 SIF's were analyzed.

The reason to do this study was the result of the replacement of an existing relay-based safety system, by a dedicated safety PLC. The publication (at that time) of the ANSI/ISA S84.01 standard in 1996 led to the decision to determine the safety integrity levels.

A.4.2 Observations

A first remarkable observation was the fact that the only information that was made available consisted of the descriptions of the SIF's, Functional Logic Diagrams (FLD) and a list of failure rates of field devices.

Before the SIL validation of each SIF could be carried out an overview of additional required information was set up. This overview contained aspects such as the off-line proof Test Interval (TI), and the MTTR in case a repair done. In order to be able to make recommendations, also the required SIL of each SIF was asked for. Surprisingly, when these questions were submitted to the people of the oil company, they were not able to answer these questions. After an internal inquiry, information about the TI and MTTR was obtained, but concerning the required SIL for each SIF no requirements existed.

The reasoning that no SIL requirements existed was the fact that the ANSI/ISA S84.01 standard had not defined methods or techniques on how to determine the necessary SIL requirements.

Referred was to the following two sections of ANSI/ISA S84.01:

Part 1:

1.2.6 Defining the need for a Safety-instrumented Systems is not included in this standard.

1.4 ... Note that this standard does not address the method for performing initial Safety Life Cycle activities, such as:

- a) Performing conceptual process design*
- b) Performing process hazards analysis & risk assessment*
- c) Defining non-SIS protection layers*
- d) Defining the need for an SIS*
- e) Determining required Safety Integrity Level*

These activities are outside the scope of this standard.

Nevertheless, the section concerning the Safety Requirements Specification clearly has stated:

SRS Input requirements:

A list of the safety function(s) required and the SIL of each safety function...

The opinion of the people of the oil company was to first have an overview of the achieved SIL of each SIF and subsequently adapt the SIL classification criteria to these achieved SIL's.

A.4.3 MIR-based SLM analysis

The MIR-based SLM analysis was not carried out on a detailed level for the reason that the problem was immediately observable and explainable at a global level. Figure 47 shows the safety-related activity flowchart of the SIS-related SMS of the oil company. The flowchart shows that no integrated cooperation existed between the various departments that were responsible for the different safety-related activities. No information flows were observed between the people who were responsible for the hazard and risk analyses, the people from the instrumentation department and the people from the operation, maintenance and testing department.

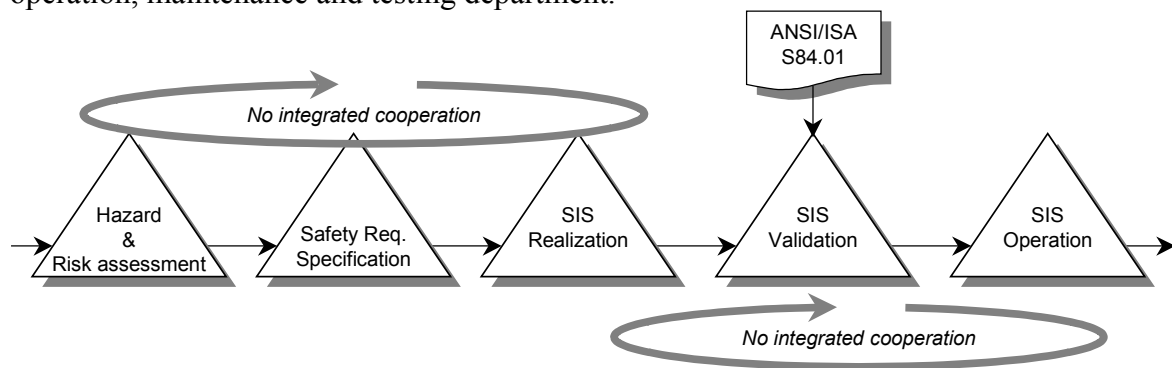


Figure 47 Safety-related activity flowchart of the American oil company

A.4.4 Evaluation and conclusions

It was concluded that the people of this oil company did not understand the objective of the defined safety lifecycle of ANSI/ISA S84.01. The fact that the first 5 stages of the safety lifecycle were out of the scope of the standard and the fact that no requirements were defined on the transfer of information that is generated during these 5 stages, did not make the people from the instrumentation department aware that the added value of each SIF significantly depends on the quality of the safety-related activities of all stages and the quality of transfer of information between these activities.

With regard to the MIR level criteria, it was concluded that not even MIR level 1 was realized.

Case 5 – Chemical company located in Belgium

A.5.1 Introduction

In spring of 1999, a chemical company located in Belgium needed to comply with the Seveso II Directive (Council Directive 96/82/EEC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, see also Chapter 4). Concerning the safeguarding instrumentation, it was decided to comply with the requirements of IEC 61508. The risk assessment and SIL classification was already carried out by the local engineering contractor. Assistance was asked to do the SIL validation of the safeguarding instrumentation of the chloring unit.

A.5.2 Observations

During the SIL validation study a number of problems were revealed. A first problem that was observed concerned the fact that no distinction was made between functions performed by the Basic Process Control System (BPCS) and those performed by the SIS. It appeared that both control and safety functions were performed by a single BPCS. Furthermore, it appeared that a number of safety functions that were SIL classified, only represented an alarm that needed to be followed by required specific operator action.

A.5.3 MIR-based SLM analysis

Figure 48 shows the first three phases of the Overall safety lifecycle model of IEC 61508. The chemical company had not yet specified and implemented a safety lifecycle model into the SMS.

Quality requirements on safety-related information to be created and transferred and inputted to the hazard and risk assessment did not exist.

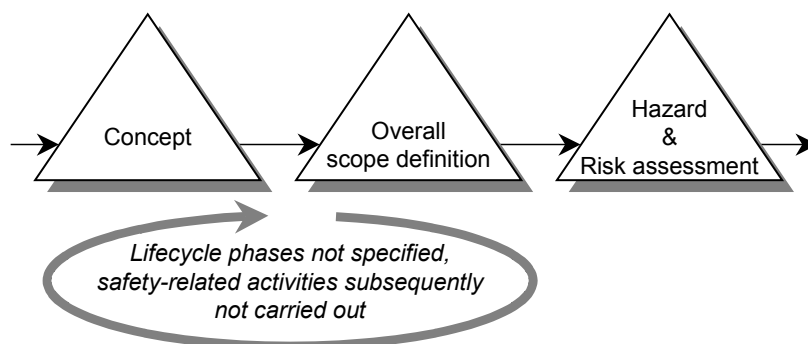


Figure 48 The first three phases of the Overall safety lifecycle model of IEC 61508

A.5.4 Evaluation and conclusions

The main cause resulting in the various problems during the different safety-related activities was the result of the lack of an adequate safety lifecycle model. The lack of lifecycle phases and their activities, automatically meant that the required information from these phases is not created and thus not made available to the subsequent lifecycle phases. It was concluded that a MIR level 1 was therefore not even achieved.

Case 6 – Dutch chemical company in southern Netherlands

A.6.1 Introduction

In June of 1998, an evaluation study was carried out on a modified SIL classification method. The study was carried out at a site of a Dutch chemical company in southern Netherlands. The SIL classification method was based on the risk graph method as described in the German standard DIN V VDE 19250 and in part 5 of IEC 61508. A naphtha cracker process unit was used to test the new developed classification method. The people of the safety, instrumentation and operation department asked for assistance for the evaluation.

A.6.2 Observations

The risk graph method consists of four risk determining parameters. Table 12 shows these four parameters whereby C the consequence represents for the safety of the people, F the frequency and exposure of these people in the hazardous zone, P the probability that the people can avoid the hazardous event and W the probability of the unwanted occurrence. Based on the determined parameter settings of the risk graph, as presented in Figure 49, determines the SIL to be realized by the SIS. In case the risk is determined to be very small, the risk graph does not require special safety requirements (a). In case the risk is determined to be negligible no safety requirements are needed (-). Very high risks are not acceptable (na).

Table 12 Risk graph parameters

Code	Consequence
C0	Slight damage to equipment
C1	One injury
C2	One death
C3	Several deaths
C4	Catastrophic, many deaths

Code	Frequency and exposure
F1	Small probability of persons present in the dangerous zone
F2	High probability of persons present in the dangerous zone

Code	Probability to avoid the hazard
P1	Good chance to avoid the hazard
P2	Hardly impossible to avoid the hazard

Code	Probability of the unwanted occurrence
W1	Probability of hazardous event very small
W2	Probability of hazardous event small
W3	Probability of hazardous event relative high

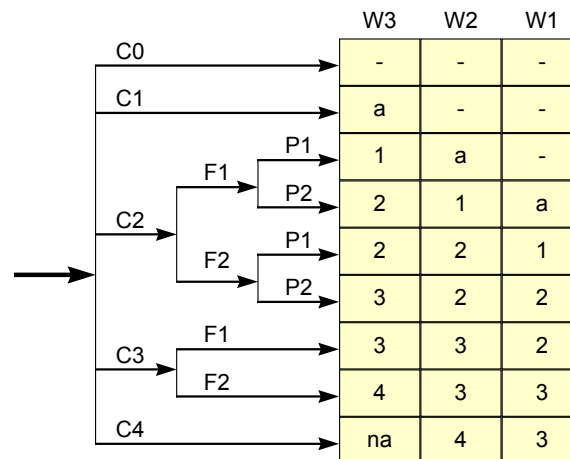


Figure 49 Risk graph

During the evaluation study, a number of accident scenarios were analyzed. The impression of the local people was that the risk graph appeared to be an excellent tool to determine the required SIL. Unfortunately however, it appeared during an analysis of two accident scenarios that the outcomes of the risk graph resulted in different residual risk levels. Accident scenario A and B describe these two scenarios. For each scenario an estimation of the consequences was made, but at the same time, a quantitative estimation was made as well. For instance, in a situation where the frequency and exposure was estimated to be relatively high, this estimation was quantified to be 90% (scenario A). In case the estimation was relatively low, it was quantified to be 10% (scenario B).

Table 13 Accident scenario A

Estimated category	Accident scenario A
C2	Hazard with probably a casualty
F2	Large probability of persons present, assume 90%
P2	No possibility to avoid the hazard, assume 0%
W2	Frequency of occurrence, assume once per 10 years
Calculate risk	$1 * 0,90 * 1 * 0,1 = 0.09$ or 9 casualties per 100 year
Risk graph	Required protection: SIL 2

Table 14 Accident scenario B

Estimated category	Accident scenario B
C3	Hazard with probably several casualties, assume 5 casualties
F1	Small probability of persons present, assume 10%
W2	Frequency of occurrence, assume once per 10 years
Calculate risk	$5 * 0,10 * 0,1 = 0.05$ or 5 casualties per 100 year
Risk graph	Required protection: SIL 3

Table 13 and Table 14 show the accident scenarios and estimated risk parameters. Based on the application of the risk graph, for both scenarios the required SIL was determined.

Subsequently, for both scenarios the risk were calculated, based on the quantitative values estimated for the four parameters. It appeared that the calculated risk of scenario A (9 casualties per 100 year) was almost two times higher than the calculated risk of scenario B (5 casualties per 100 year). Remarkably however, the application of the risk graph indicated that scenario A required a SIS of SIL 2, whereas a SIL 3 appeared to be required to reduce the risk of accident scenario B. This would mean that the application of the risk graph leads to different residual risks for different accident scenarios. Confronting the involved people with this apparent contradiction made them aware of the fact that the application of the risk graph is only then acceptable if afterwards for each risk is verified whether it is reduced to an acceptable level. This can only be done if clear and unambiguous criteria are defined of acceptable risk levels. Undeniable, it must be mentioned that the accidents A and B can not only be compared based on the number of casualties per year. A relatively big accident is most times characterized by large damage to the installation, production loss, etc. In case an accident happens were only one person is injured, a lesson might be learnt and this might prevent future similar accidents. Obviously, another weak point that is subject to inconsistent interpretation, concerns the estimation of the input parameters. Descriptions such as a 'relatively low' probability that an accident might occur are susceptible to subjective interpretation.

A.6.3 MIR-based SLM analysis

Figure 50 shows the phases 3, 4 and 5 of the IEC 61508 Overall safety lifecycle model. During phase 3 the hazards are allocated and risks are determined. During phase 4 the overall safety requirements are specified. This specification is expressed in general terms, e.g. reducing the risk for people from an explosion as a consequence of an over-pressure with a factor 10. Subsequently, these general safety requirements are allocated during phase 5 to one or more safeguarding or risk reduction measures. Together, these measures shall take care that the overall risk reduction requirements are met. Therefore, it should be verified whether this is indeed achieved by the defined safeguarding measures. If methods like the risk graph are used to determine the required SIL for the SIS, also this method should lead to the required risk reduction. Verification of the risk graph method is therefore necessary. It appeared that in this case, the involved people had not realized a verification (or control) loop to check the correct implementation of phase 5 based on the input of phase 4.

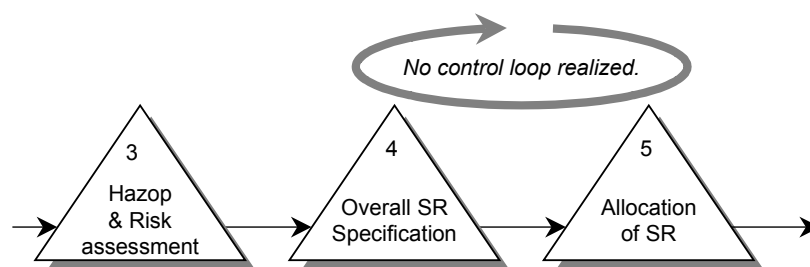


Figure 50 Phases 3, 4 and 5 of the IEC 61508 Overall safety lifecycle model

A.6.4 Evaluation and conclusions

Probably the main reason that such a problem had slipped into the organization was due to the fact that no safety lifecycle model was defined and implemented. This organization

was very hard working on developing all the IEC 61508 safety-related activities without considering the basic framework that establishes the relationships between these activities. The particular problem that no verification was done after phase 5, resulted in the conclusion that only a MIR level 2 was achieved where a MIR level 3 would be required.

Case 7 – A Hungarian refinery

A.7.1 Introduction

In April 2000, a SIL validation pilot project was performed at a Hungarian refinery on a delayed cooker installation. An American engineering contractor owned the license of the process installation design.

A.7.2 Observation

During the start of the study, information was gathered on the process installation and instrumentation. Remarkably, it appeared that the American engineering contractor already added the SIL requirements (based on ANSI/ISA S84.01) of the safeguarding instrumentation to the P&ID's. On the other hand, no detailed narratives on the hazard and risk assessment and no explanations on the prescribed SIL requirements existed.

In order to be able to validate the SIF's, it was started to collect information was collected, among others, about the off-line periodic test procedures, the maintenance procedures and application circumstances of the safeguarding instruments. This information was needed to do the quantitative reliability analysis. During the discussions that followed, it appeared that the people from the engineering department and the operation department had serious doubts concerning the correctness of the prescribed SIL requirements. Obviously, the SIL requirements directly depend on the risks to be reduced. First of all, these risks consider the safety of the people who are present in the dangerous zone. The probability that people are present in the dangerous zone importantly depends on the maintenance and testing procedures, which subsequently depend on the type of instruments that is chosen to be applied. Furthermore, local legislation and circumstances determine e.g. the financial consequences in case somebody gets injured.

Finally, it was decided to contact the engineering contractor and ask for the narratives and rational behind the specification of each SIF. Strangely enough, the engineering contractor responded that no further information could be given. Therefore, it was concluded that the end user should define its own risk assessment method and should verify each SIL requirement by himself.

A.7.3 MIR-based SLM analysis

Figure 51 shows the safety-related activity flowchart that is considered during the study. A serious barrier appeared to exist between user and licensor. The activity flowchart shows the separation of responsibilities of the different activities. The licensor had carried out the hazard and risk assessment and had defined the safety requirements. The end user is responsible for the realization and operation of the SIS and asked an external consultant to assist with the SIL validations.

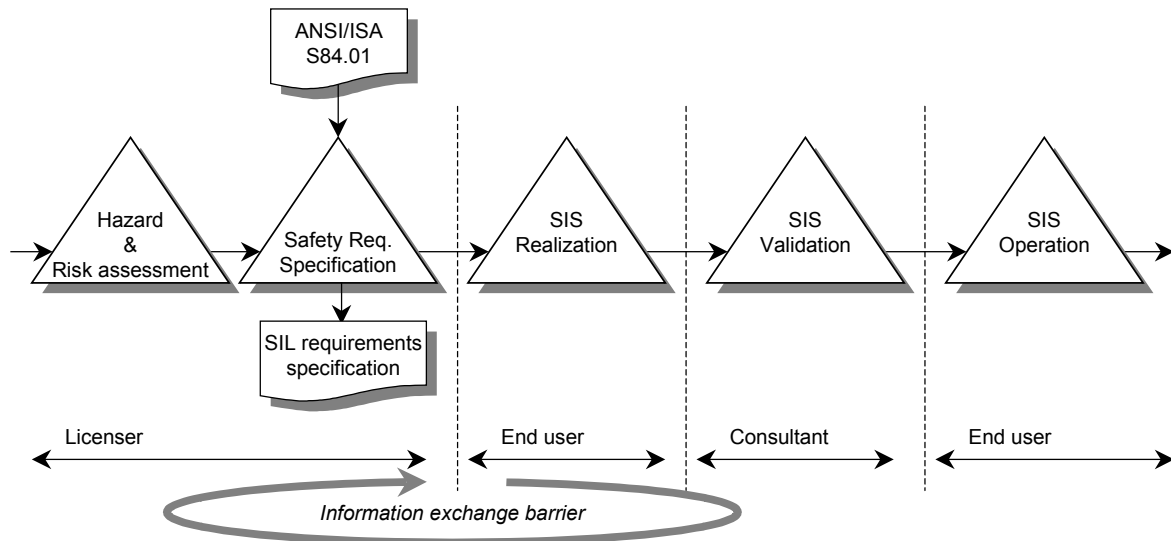


Figure 51 Safety-related activity flowchart of the Hungarian oil refinery

A.7.4 Evaluation and conclusions

The communication between the engineering contractor and the end user was not characterized by a bi-directional exchange of information, knowledge and information. Therefore, it was concluded that no learning cycle between end user and licensor was realized. On a MIR scale, it was concluded that not more than MIR level 1 was achieved. Typical information about ‘*why*’ certain requirements were specified was not passed on, nor documented.

One explanation for the fact that adequate information exchange was not yet structured, was the fact that the oil refinery at that moment just started with the implementation of ANSI/ISA S84.01. No safety lifecycle was defined and implemented in their SMS.

Case 8 – A Belgian oil refinery

A.8.1 Introduction

This case describes the safety-related problems observed during a safety study at a Belgian oil refinery, in the autumn of 2000. During this study, a SIL classification was carried out and a handbook on the application of safety-instrumented systems was developed.

A.8.2 Observations

In spring of 1999 an engineering contractor carried out an IPF (Instrumented Protective Function) classification study at the Belgian refinery. (IPF equal to SIF as is defined by Shell in their Design and Engineering Practice (DEP) 32.80.10.10.) Based on the results of this classification, it was decided to do also a validation study based on IEC 61511. During the SIL validation it appeared that a considerable part of the safety functions was over or under engineered. In fact, a significant number of SIF's was only realized by an alarm function. Thus in case of a alarm, the operator was expected to take the appropriate action in time and e.g. activate valves or stop generators. These alarm functions appeared to be classified as SIL 3. However, the probability that an operator would act appropriately was not further considered. It was therefore concluded that it was not considered to be acceptable to make use of an operator to serve as 'logic solver'. It appeared that HAZOP studies were not combined with the SIL classification, which resulted in problems concerning the verification whether the SIF's indeed reduced the residual risks to acceptable levels.

During the SIL validation it further appeared that information about failure rates of safety-related devices was very difficult to obtain. The people from maintenance were the ones that had the best access to this kind of information but unfortunately these people were employees of a completely different department, which had set its work priorities to other business interests.

Another remarkable observation was the fact that the classified safety functions were not tagged. Based on the concepts of the latest safety standards, safety should be controlled from a functional point of view. Logically, safety-instrumented functions are defined and thus tagged based on the risk analysis. (To date however, almost every company, including this Belgian refinery, only applies tagging to the applied equipment.) To illustrate the potential safety problems, an example is used. In case of a high-high level, a particular valve will have to close. In case of a high-high pressure however, once again the same valve may be required to close. Therefore, tagging the valve needs to be done twice, one time for each safety function, something which might be confusing.

A.8.3 MIR-based SLM analysis

Figure 52 shows the activity flowchart of the safety lifecycle phases from HAZOP studies up to SIS operation and maintenance. The flowchart shows the inconsistency as the result of applying different safety standards for the classification and validation study, and as a consequence of letting different companies do these different activities. Furthermore, the activity flowchart shows the poor storage of the HAZOP results which did not contain information on the required level of risk reduction to be achieved and the allocation of this risk reduction to the different safeguarding measures. At last, the poor cooperation between the instrumentation department and the maintenance department is indicated.

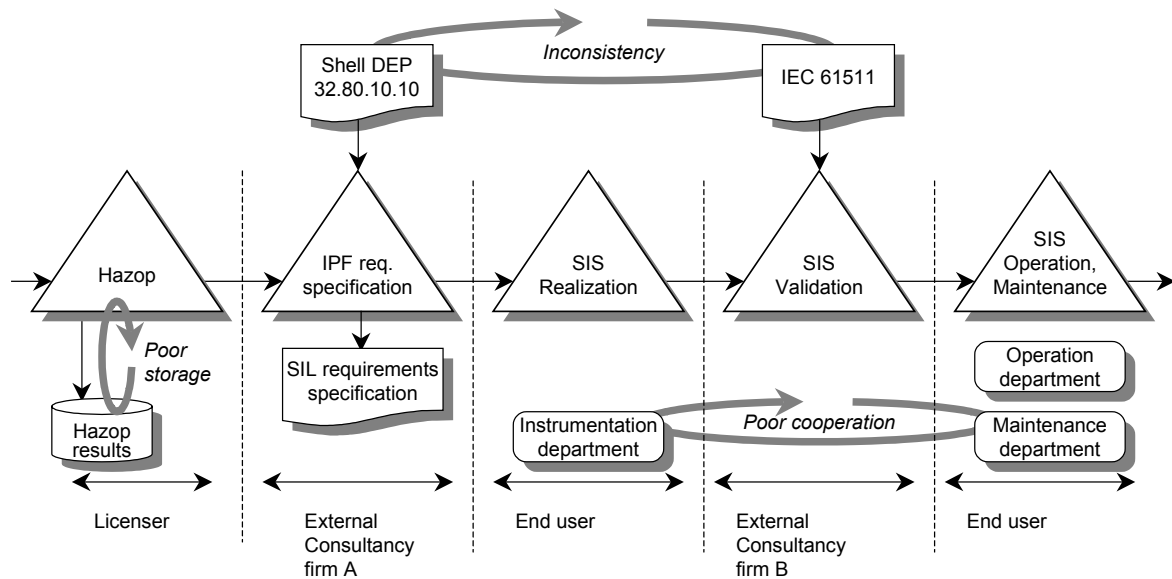


Figure 52 Safety-related activity flowchart of the Belgian oil refinery

A.8.4 Evaluation and conclusions

Also for this Belgian oil refinery it was observed that no safety lifecycle model was defined. In some situations this led to very poor exchange of information. For the three observed problem areas it was generally concluded that the subject safety-related activities were therefore not under control. The lean supply of information on what needed to be done only met the criteria of MIR level 1 or 2. Obviously a MIR level 3 would be required to control these safety-related activities. Therefore, a handbook on the application of safety-instrumented systems was developed which was based on the safety lifecycle model of IEC 61511. In addition to the requirements of this standard, the handbook was extended with clauses that described the rational behind each lifecycle phase and the rational behind the objectives to be achieved for that lifecycle phase. The expectation is that, in the long-term, this approach will lead to improvement of the safety-related activities and improvement of the quality of the information flows.

Case 9 – A chemical plant in the harbors of Antwerp, Belgium

A.9.1 Introduction

In April 2001, a safety problem was analyzed at a chemical plant in the area of the harbors of Antwerp, Belgium. The problem concerned the application of pure nitrogen. Nitrogen is characterized as being inodorous. At the moment that the nitrogen replaces the oxygen in the air, people will suffocate. This plant had a system of nitrogen pipelines and leakage would seriously lead to a dangerous situation. Therefore, at each level a number of fans were installed which continuously refreshed the area with open air. Furthermore, at each floor a number of gas detectors were installed, which would alarm people in that area in case a specific concentration of the nitrogen gas was detected. Procedures were in place to take care that the people, who had to operate in the building, were equipped with oxygen masks. The problem was that in case of a serious leakage the capacity of the fans would be too small. Therefore, highly reliable operation of the gas detectors and the alarms should lead to in time evacuation of the building.

A.9.2 Observations

Initially, the local people who were responsible for the safety instrumentation, performed a SIL classification analysis for the alarm function and came to the conclusion that a SIL 3 would be needed. Subsequently, they asked themselves how SIL 3 should be realized. Furthermore, it was established that in case of a serious leakage an alarm would not be effective for the reason that it would be impossible to evacuate the building in time. As an alternative the number of fans should roughly be duplicated to increase their capacity to an acceptable level to handle such a situation. Another alternative would mean that all the people in the building would permanently have to wear an oxygen mask. These alternatives however, would be very expensive and very impractical.

During the discussions with the people from the instrumentation department, it appeared that they followed their corporate engineering and design guideline in order to determine the required SIL. Nevertheless, they did not feel comfortable with the resulting solution. Therefore, it was decided to further analyze this corporate guideline. Although the latest version of their corporate engineering and design guideline for safety-instrumented systems was based on IEC 61508, it appeared that no clear and unambiguous safety lifecycle model was defined. Instead, a flow diagram was given, describing six main activities that approximately covered the same scope as the IEC 61508 Overall safety lifecycle. Unfortunately however, no cross-references were made to the lifecycle phases of IEC 61508, and not all lifecycle phases of the Overall safety lifecycle model were included in the flow diagram. Furthermore, only the SIL classification, SIS design and testing activities were described in detail. It was therefore concluded that the SIL classification of the SIF's was considered to be the sole responsibility of the instrumentation engineers. Therefore, these people were not aware of the fact that in order to solve this problem, close cooperation would be required with other departments such as HAZOP leaders and the people from mechanical engineering department. The solution that was looked for by the people from the instrumentation department was purely focused on increasing the performance of the alarm functions.

A.9.3 MIR-based SLM analysis

Figure 53 shows the safety-related activity flowchart of this Belgian chemical plant. As described in the previous section, it was observed that a barrier existed between the instrumentation department, HAZOP teams and mechanical engineering department. The nitrogen problem could only be solved if this barrier would be eliminated. This would at the same time led to a more adequate specification and application of the various safety-related systems. This would mean a significant step towards controlled safety-related business processes.

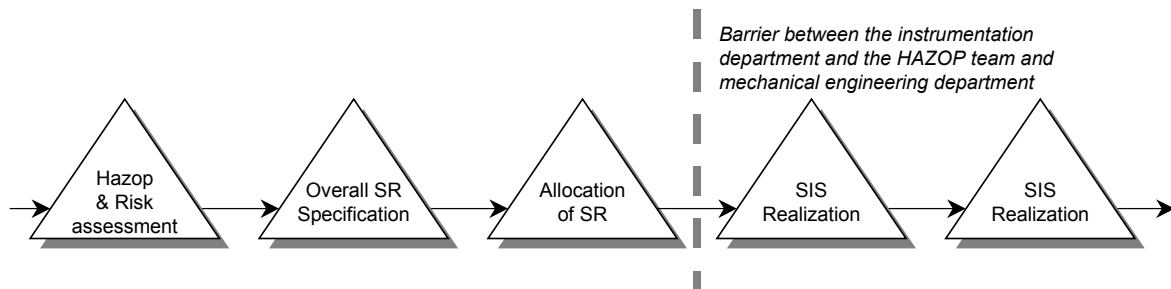


Figure 53 Safety-related activity flowchart of this Belgian chemical site

A.9.4 Evaluation and conclusions

A structured framework of safety-related activities and its related business processes did not characterize the corporate engineering and design manual for the safety-instrumented systems. Instead, it was concluded that the corporate manual only represented a collection of good engineering practices. Relationships and dependencies between consecutive practices were not considered. The kind and quality of information that needed to be created, stored and made accessible to the involved people, was not specified by the corporate manual. Based on the MIR model criteria, it was concluded that only up to MIR level 1 was achieved, if purely the manual was followed. The objective of the corporate manual is to control adequate application of SIS's. Therefore, it was concluded that at least a MIR level 3 should be achieved to comply with these standards. Modification of the corporate procedures and guidelines was therefore required to meet the MIR level 3, resulting in controlled acceptable residual risk levels.

Case 10 – Chief-instrumentation engineers network meeting in Vienna

A.10.1 Introduction

During a chief-instrumentation engineers network meeting in Vienna of a Scandinavian chemical company, typical problems with the implementation of IEC 61508 were discussed. In order to come to a consistent and unambiguous interpretation and application of this standard, it was decided to discuss an industrial case. The objective of this case was to come to a common understanding of the definition and implementation of safety-instrumented functions. A functional logic diagram was used as the basis for this industrial case.

A.10.2 Observations

The functional logic diagram that was considered during the discussion showed the applied sensing elements, the logic as implemented in a safety-related PLC and the applied actuators. In fact, the logic diagram shows a number of sensing devices. For instance, a level sensor, a temperature sensor, a flow sensor, another level sensor and two flame sensors were drawn in the logic diagram. It was explained that in case the process would get out of control, all actuating devices should be activated to bring the process to a safe state by tripping the installation (up to 7 valves had to close). This action could therefore be the result of an out of control limits of each measured process parameter. The question to be discussed and answered was to determine the number of safety-instrumented functions that could be observed in the logic diagram. The general opinion turned out that totally one or maybe two safety-instrumented functions could be distinguished. The final establishment was that the attending instrumentation experts had a line of thought, which was focusing on the technical solution, namely bringing the process to a safe state. After this establishment, it was explained that each process parameter that would get out of control might result in a different hazardous event (e.g. fire, explosion, and toxic gas release). Each hazardous event would result in different consequences (e.g. injuries, damage to the equipment, environmental pollution). This implicated that each out of control process parameter would entail a different risk. Therefore, different SIF's separately safeguarded these process parameters. Thus, a SIF to safeguard the pressure, temperature, flame, etc. Therefore, it was concluded that a total of 5 SIF's could be allocated in the logic diagram. Although the fact that during that meeting a number of examples were presented that explained the functional aspects of IEC 61508 and the concept of risk reduction, the instrumentation engineers were not acquainted with this new approach.

A.10.3 MIR-based SLM analysis

Figure 54 shows part of the IEC 61508 Overall safety lifecycle model (phase 3,4,5 and 9), and one lifecycle phase of the E/E/PES lifecycle model. Apparently, the instrumentation engineers were not aware of the fact that their daily work only concerned a restricted number of lifecycle phases of these lifecycle models. Because IEC 61508 is titled as being a functional safety standard, the instrumentation engineers were not aware of the objective of this functionality. Their interpretation appeared to be restricted to the implementation of the safety requirements as specified in the logic diagrams. This kind of specification however, concerns the *technical* safety requirements specification of E/E/PES lifecycle

phase 9.1. The fact that during lifecycle phase 4, the overall *functional* safety requirements are specified, appeared to be out of the scope of their way of thinking. Therefore, it was concluded that for the reason that this company did not yet specify a safety lifecycle model, was the root cause of a restricted information flow between lifecycle phases 5 and 9.

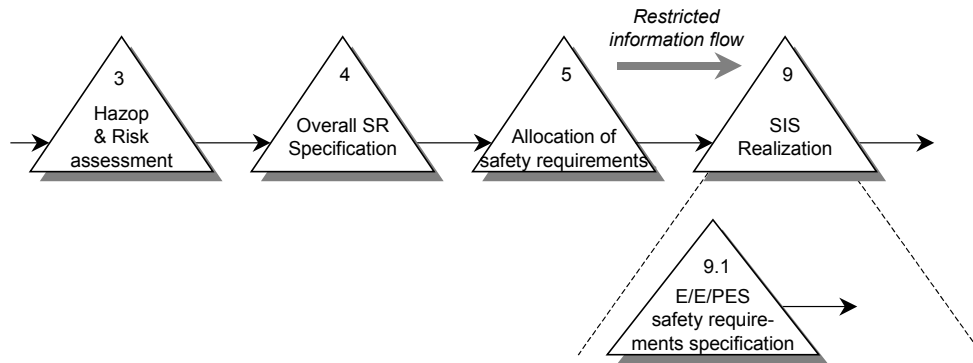


Figure 54 IEC 61508 Overall safety lifecycle model (phase 3,4,5 and 9), and lifecycle phase 9.1 of the E/E/PES lifecycle model

A.10.4 Evaluation and conclusions

The fact that the instrumentation engineers were not accustomed to use a safety lifecycle model restricted them to analyze the logic diagrams from a functional point of view. The only kind of information they were used to work with, was the technical safety requirements specification. This kind of information however, only answers questions such as ‘what’ and ‘where’ instruments should be applied. No information was available ‘why’ these instruments were needed from a functional point of view (e.g. protection the pressure, to prevent an explosion that might lead to injuries of local workers).

Based on the MIR model criteria, it was concluded that only up to MIR level 2 was achieved. It was consequently established that at least a MIR level 3 was required for the input information flow, for the instrumentation engineers to be able to correctly implement the SIS.

Case 11 – A Manufacturer of safety PLCs

Note:

*This case description is a summary of an earlier publication. A more detailed description can be found in the paper *Experiences with organizational aspects of implementing the IEC 61508 safety standard into an existing quality management system* by B. Knechting and F. van Bakel*

ISA-Tech – Philadelphia, USA 1999 [Kne99a] and Interkama – Düsseldorf, Germany 1999 [Kne99f]

A.11.1 Introduction

The analyzed company is a manufacturer of dedicated safety PLCs that are primarily used in the process industries. For the reason that the subject PLC is applied as part of the safety-instrumented function and for the reason that it concerns an electric/electronic/programmable device, it was decided that the PLC would subsequently need to comply with standards like IEC 61508. For the reason that the current product was designed and developed many years before IEC 61508 was published, it was concluded that it was not practical to re-develop the PLC in accordance with the requirements of this standard. Nevertheless, the entire product realization process, from order quotation, order intake, project engineering, assembly and Factory Acceptance Test (FAT), and shipment should be brought in line with IEC 61508.

A.11.2 Observation

In the first half of 1997, the company decided to start with the implementation of IEC 61508 into its organization. The implementation route was divided into three phases:

- Awareness and commitment from the organization towards the implementation.
- Implementation of requirements into the quality management system.
- Third-party assessment.

The approach, results, experiences and conclusions of the implementation are discussed below.

Phase 1: Awareness and commitment from the organization

Experiences, gained during the implementation of the ISO 9001 based quality system, taught that commitment of employees is crucial. The awareness within the organization of the emerging new international safety standard had already been present for several years before 1997. The current Development Engineering (DE) manager was heavily involved in the creation and evolution of IEC 61508, due to his membership in several technical committees that deal with safety standards.

An important step in creating awareness within the organization was to introduce the IEC 6508 standard to the company's management, and provide some background information on the safety lifecycle. As this standard very much affects the type of products that the company offers, it was fairly easy to underline the importance of compliance. Non-compliance would eventually result in losing business in the future and missing a great opportunity to focus on the company's own safety lifecycle improvement and the customers.

The process of creating awareness within the organization was an ongoing activity. Introductory sessions and updates of the status of the standard are still being held periodically. Promoting the standard within other parts of the organization has proven to be very important,, because of the significant impact the standard will have, not only to the company's (safety) business, but also to the entire industry.

A study performed by the British Health and Safety Executive (HSE) proved to be very important and convincing. One of the reasons behind the formulation of the standard is given in Figure 55 (see also Figure 6), which identifies the primary causes of control systems failures (based on investigated incidents in the UK [HSE 95]).

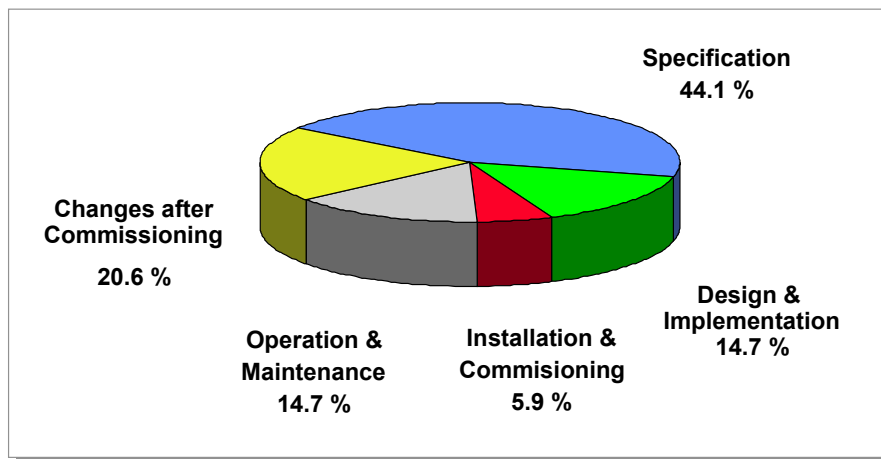


Figure 55 Primary causes of control system failures [HSE95] (see also Figure 6)

The above percentages show that specification and design & implementation affect the safety of the EUC more than 50%. Therefore, it is very important and challenging to implement IEC 61508 to diminish the contribution of specification and design errors.

Phase 2: Implementation of requirements into the quality management system

The ISO quality standards 9001, 9002, 9003 and 9004 were published about ten years ago. Many companies have achieved conformance with these standards since then. The development of quality-related concepts, methods and tools has increased tremendously. This company too, has adopted ISO 9001, and has obtained a compliance certification. In order to realize compliance, a quality management system was established.

The concept of reliability has become more important in recent years. Unreliable products led to increasing cost. The warranty period for products has grown from months or one year to several years. Within the process industry new developments of reliability analysis techniques are applied in order to realize safe operation of process installations. An important aspect of realizing reliable products is that it is closely related with the reliability of the accompanying business processes [Bro99].

Both quality and reliability analysis methods and techniques can be utilized for realizing safe products, installations and organizations. Both groups of techniques are therefore

applied as a starting point for the implementation of IEC 61508. It was subsequently decided to extend the current Quality Management System (QMS) and include the specific requirements of IEC 61508.

Due to the size and complexity of the IEC 61508 standard, it is expected that implementation of the technical requirements is not possible without a proper organizational approach. The standard itself has therefore identified a number of organizational requirements that should be met, e.g. appointment of persons who are responsible for the implementation and maintenance of the implementation of the standard. A clear set of documentation needs to be constructed and maintained. The strategy of implementing the requirements of IEC 61508 into the business processes was three-tiered (see Figure 56).

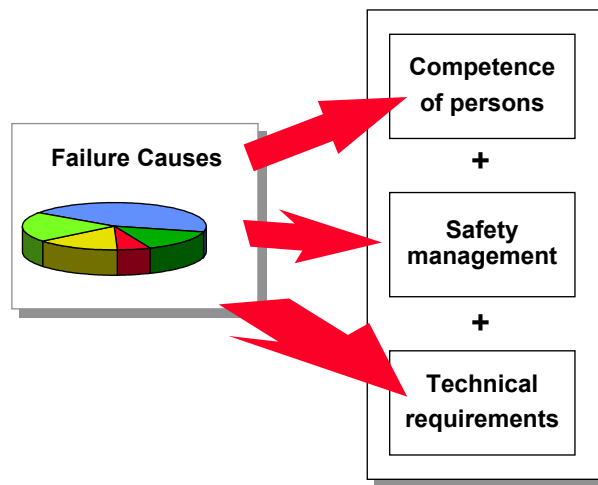


Figure 56 Three-tiered approach of covering aspects of the IEC 61508 safety standard

In order to make sure that operation that is compliant with IEC 61508 would not be restricted to a one-time snapshot but becomes part of the working culture, it was decided to implement safety management by expanding the existing QMS to include the standard requirements.

The quality management system needed to evolve to a level where cooperation between the various phases of the lifecycle is realized (i.e. between departments responsible for the implementation of the requirements for the various phases). Therefore it was needed to improve the management of the product development and introduction process (Product Creation Process as shown in Figure 57, which shows the quality evolution model from the AT&T quality manager's handbook [AT&T90]).

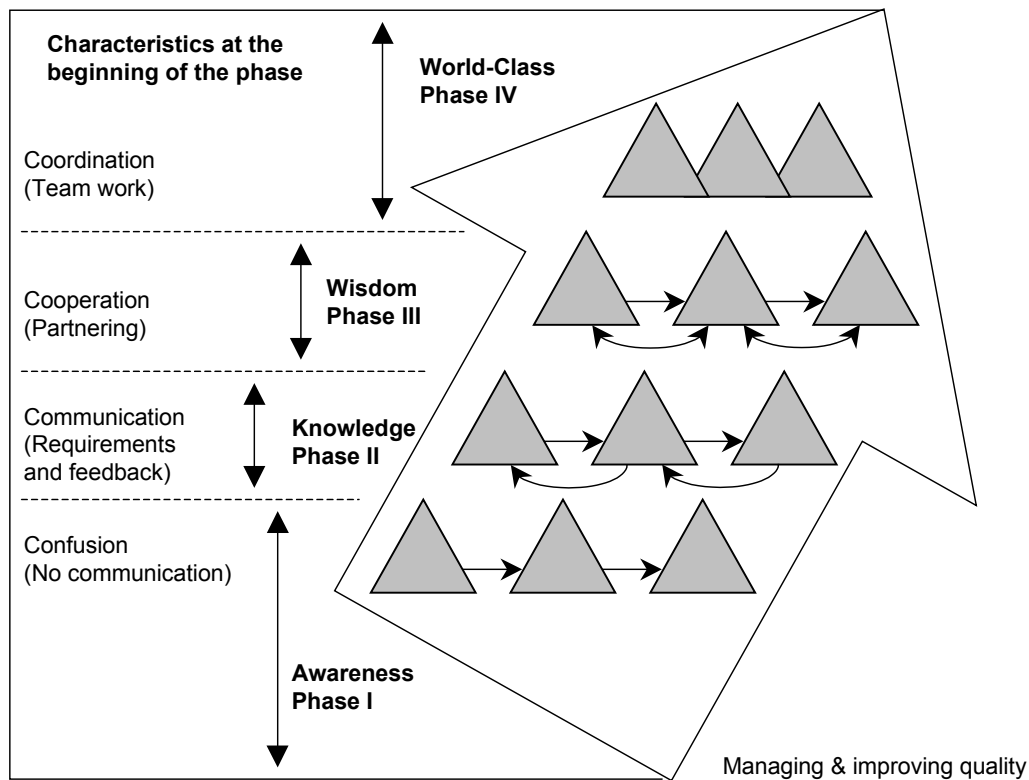


Figure 57 The Quality Evolution model [AT&T90]

The quality evolution model of Figure 57 represents an organization beginning with its quality level development. The large inclined arrow represents the overall process of managing and improving quality. The triangles represent internal as well as external customer-supplier relationships, as they move from one-way communication to sincere integrated teamwork.

Conformance to ISO 9001 [ISO9001] can be recognized as the knowledge phase II in this model. Communication and forward oriented processes are established in a documented quality management system.

The existing quality management system was indeed a highly documented quality system with written procedures and work instructions, mainly focusing on the feed-forward process. Analysis revealed that at several points a clear overview of the interdependencies between the procedures and the possibility to establish an iterative process was missing. This analysis led to the definition of the processes into flowcharts, which focused on the relationships between the various process steps and clear definition of the responsibilities and authorities for each step in the process. The identification of these flows can be considered as a transition phase between the knowledge phase and the wisdom phase III.

Firstly, the organization was split up into three sub-areas (see also Figure 58):

- The product creation process (PCP), covering Management, Development Engineering, Materials Management and the Product Marketing.
- The product realization process (PRP), covering Sales, Project Engineering, Assembly and Support.
- Supporting departments like Human Resources and Quality Assurance.

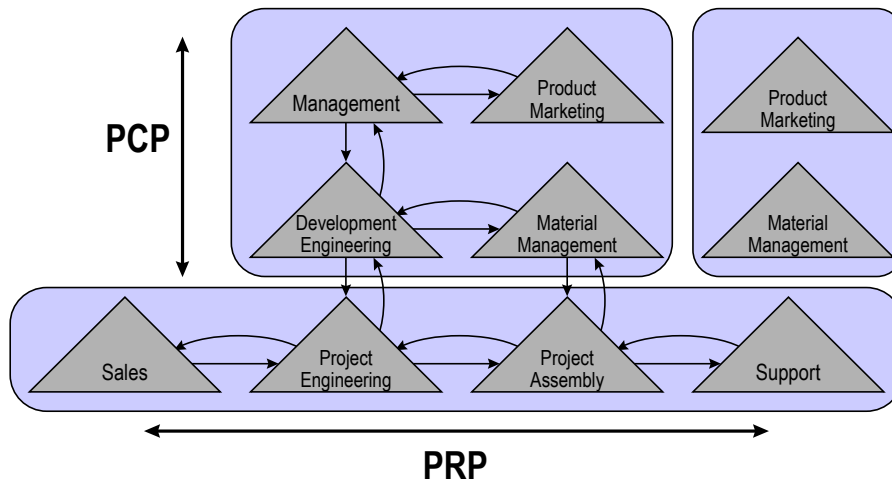


Figure 58 The organization with its product creation process (PCP), product realization process (PRP) and parallel processes

A thorough analysis of the business processes revealed that the knowledge phase was achieved, in which requirements are communicated, forwarded and feedback, as coming from next phase regarding the output from earlier phases.

IEC 61508 specifically mentions that Safety Planning should facilitate cooperation between the various lifecycle phases (Phase III). Safety Planning can be realized by referring to the quality management system, as being the standard Safety Plan or by implementing what is called Program Management. Program Management is responsible for the process of product development and introduction for a specific Development and Introduction Program. Besides Program Management, the areas of requirements management, configuration management, competence of people and establishing a Functional Safety Assessment process needed to be emphasized in the QMS. This resulted in specific supporting procedures in those areas, defining the relationships with the core process as well as the infrastructure and methods that were implemented.

The earlier mentioned three-tiered structure was the basis for establishing three dedicated teams in those areas. Their strategy for taking further action was:

1. Take the current Quality Management System as the starting point.
2. Define and review the existing process lifecycle model.
3. Add and/or modify lifecycle activities to incorporate the safety requirements.
4. Include verification steps in each safety lifecycle activity.
5. Define and review the quality documents (procedures, work instructions, etc.), and incorporate the safety requirements in them.

With respect to the Overall safety lifecycle, the realization process of safety-related systems (phase 9 of the Overall Safety Lifecycle of IEC 61508) is defined as a core activity. It was realized that the implementation was influenced by steps 5 (safety requirements allocation), 6&14 (operation & maintenance planning and execution), 7&13 (validation planning and execution), 8&12 (installation and commissioning planning, and execution). This interpretation resulted in a redefinition of three key processes in line with this IEC 61508 approach. An example of such a key process structure is given in Figure 59, showing the Product Creation Process (PCP):

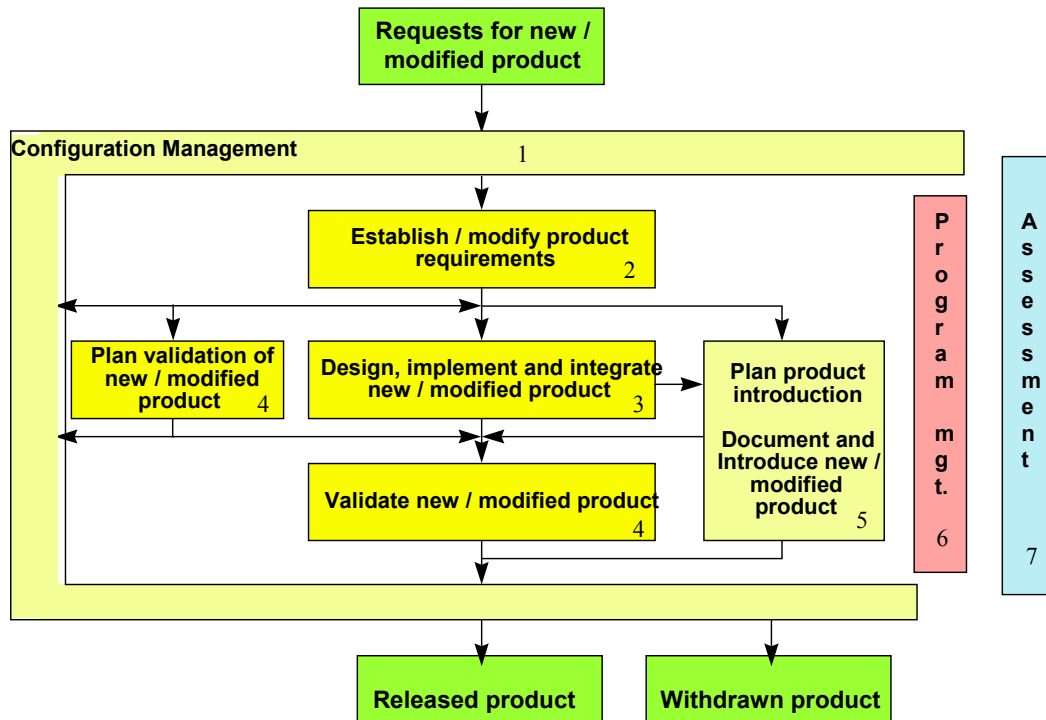


Figure 59 The Product Creation Process (PCP)

The process model reflects the Overall safety lifecycle as defined in IEC 61508 and is the basis for further implementation of the IEC 61508 at the procedural levels.

As an example, activity 3 in the above process (design, implement and integrate new/modified product) shows the model that is being used for Development Engineering activities, which is called the V-model (see Figure 60). In this model, the architecture (based on the product requirements) is split up into modules and components for implementation activities and integrated for testing purposes according to the component, modules and system requirements. This resulted in a complete redesign of the Quality Management System, which had the most impact on the quality manual and procedural levels.

The conclusion is that the implementation process itself consists of three steps:

1. Redesign of the key processes at the quality manual level reflecting the correlation between the key processes and their phases.
2. Redesign of the key process procedures reflecting the required cooperation between each phase.
3. Making changes in the existing work instructions reflecting the more detailed requirements of the safety standard.

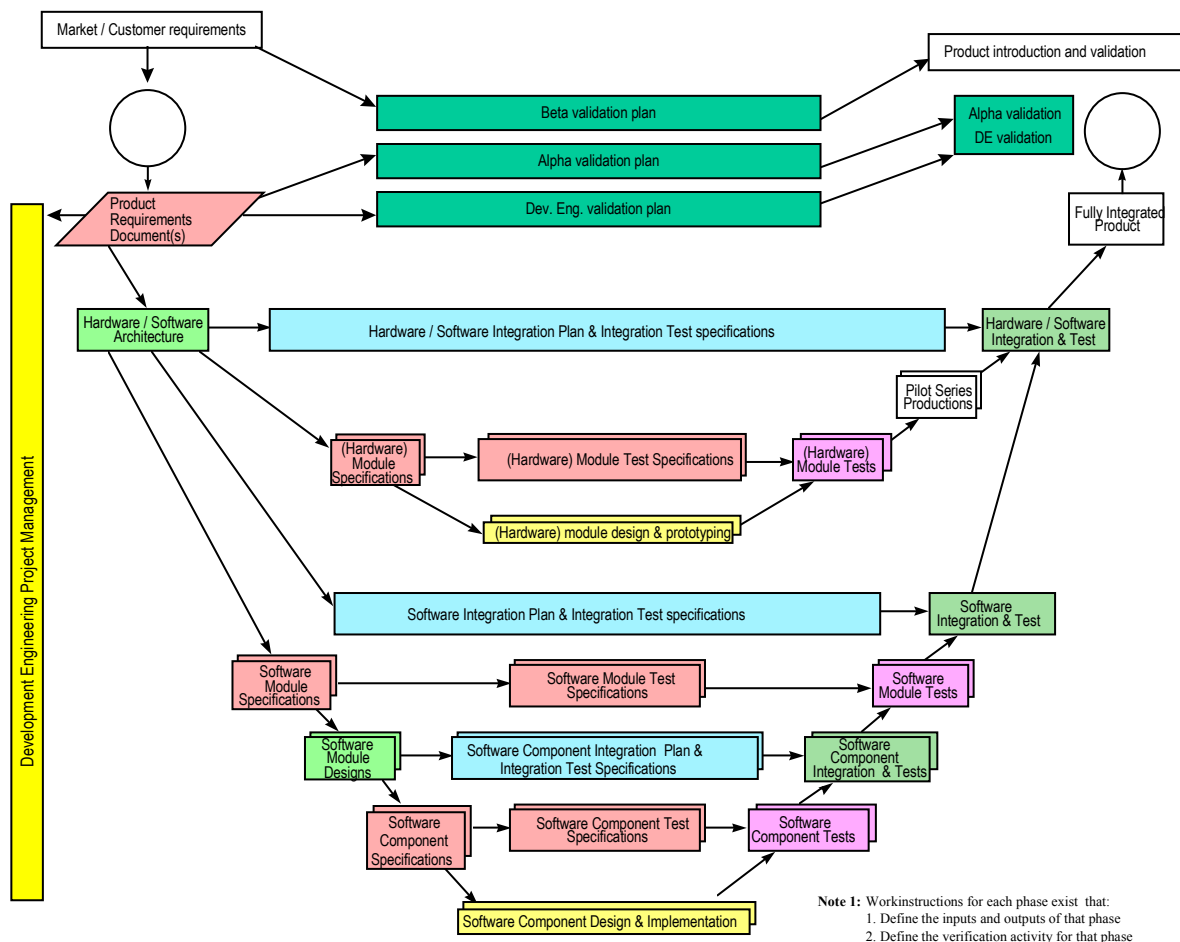


Figure 60 Model of development engineering activities

Phase 3: Third-party assessment

The company has requested an independent body, namely the German Technischer ÜberwachungsVerein (TÜV), to perform an official IEC 61508 certification assessment. This assessment process has been split up into two phases:

1. A pre-assessment.
2. A certification assessment.

The pre-assessment was carried out after the redesign of the QMS was completed at the quality manual level and partly at the procedural level. Such an assessment is a valuable tool to evaluate whether the approach taken is the correct one. Its outcome can identify possible re-directions of the approach. In this situation, the chosen approach appeared to be the right one. A detailed list of the observations and recommendations provided by the TÜV assessors served as input for the remaining part of the implementation process, especially at the work instruction level.

For the final certification assessment, a decision had to be made concerning the scope of the assessment. Both the PCP and PRP were defined as being core activities and therefore part of the Overall safety lifecycle (see IEC 61508). This implies that the company is actually a provider of safety solutions rather than just putting a safety product on the

marketplace. Managing a knowledge network for applying safety solutions will therefore become an aspect to be covered in the certification assessment. More of such aspects (e.g. a proactive approach on gathering feedback from customers concerning the performance of our product in the field) would be dealt with during the official certification assessment.

A.11.3 MIR-based SLM analysis

The previous section described the entire implementation process of IEC 61508 into the existing quality system. Especially the application of the V-model is an excellent example of how to control that the initially defined safety and product requirements are correctly implemented. Two important elements of the validation phase are testing and the reliability analysis. Testing procedures will indicate whether the product indeed meets the required functional specifications. The reliability analysis is required to determine the probability of failure on demand, i.e. the SIL of the logic solver. This reliability analysis is currently based on general reliability data handbooks like for instance MIL 217 [MIL217]. Figure 61 shows the activity flowchart of the main phases of the Logic Solver lifecycle model.

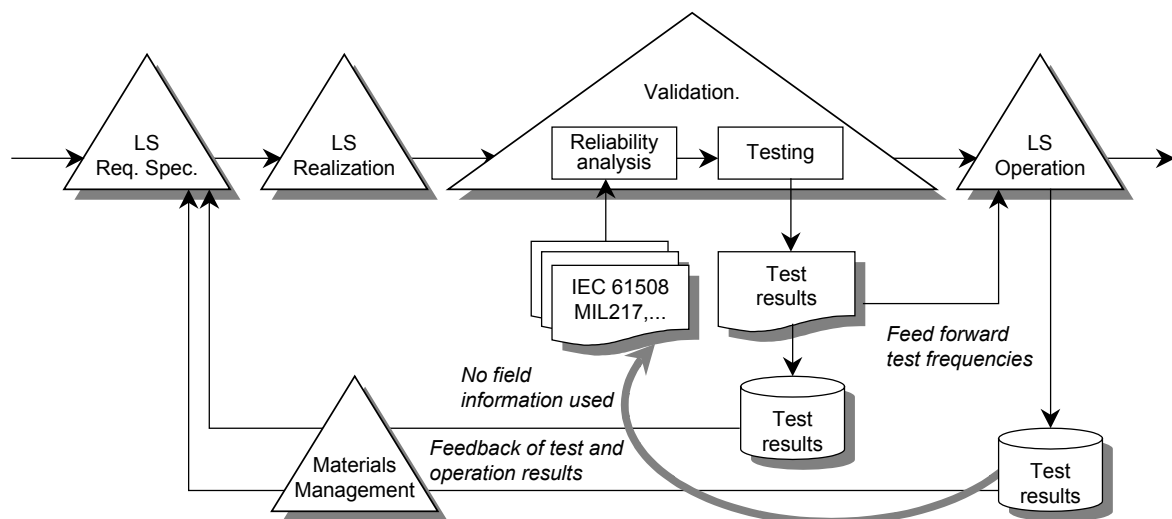


Figure 61 Flowchart of the main phases of the Logic Solver lifecycle

A.11.4 Evaluation and conclusions

The utilization of the V-model is observed as being an excellent means to control the safety-related business processes. Based on the MIR level criteria, it is concluded that a MIR level 3 has been achieved. Certification of compliance with IEC 61508 was subsequently obtained from the independent assessor. Improvement of the performance (MIR level 4) of the logic solver is only achieved if learning cycles are applied. The company has procedures in place which take care that customer complaints (or desires) are considered and included in the product requirements specification. This learning cycle concerns functional requirements of the logic solver. Unfortunately, with regard to the integrity requirements, many times no information is available on the specific application of the PLC's safety function(s). This hampers the evaluation of consequences of a registered and fed back failure or complaints. It was nevertheless concluded that a potential learning cycle was herewith revealed.

Annex B Standards and documents comprising lifecycle models

B.1 ANSI/ISA S84.01-96

ANSI/ISA S84.01 (application of safety-instrumented systems for the process industries) [ISA96] is a process industry specific safety standard with respect to safety-instrumented systems. The clauses in this standard are organized based on the Safety Lifecycle (see Figure 62). The safety lifecycle covers the safety-instrumented system (SIS) activities from initial conception up to and including decommissioning. Please note that this standard does not address the method for carrying out initial safety lifecycle activities, such as:

- performing conceptual process design,
- performing Process Hazards Analysis (PHA) & risk assessment,
- defining non-SIS protection layers,
- defining the need for an SIS, and
- determining the required safety integrity level.

In order to clarify the position that safety requirements take in the safety process, as specified in ANSI/ISA S84.01, Figure 62 below illustrates the phases of the safety lifecycle as described in ANSI/ISA S84.01 and has indicated the phases that comprehend the safety requirements (see legend at the right site). With regard to the phases ‘Development of safety requirements specification’ and ‘Perform SIS conceptual design and verify it meets the SRS,’ is referred to the technical report TR84.0.02. [dTR84.02].

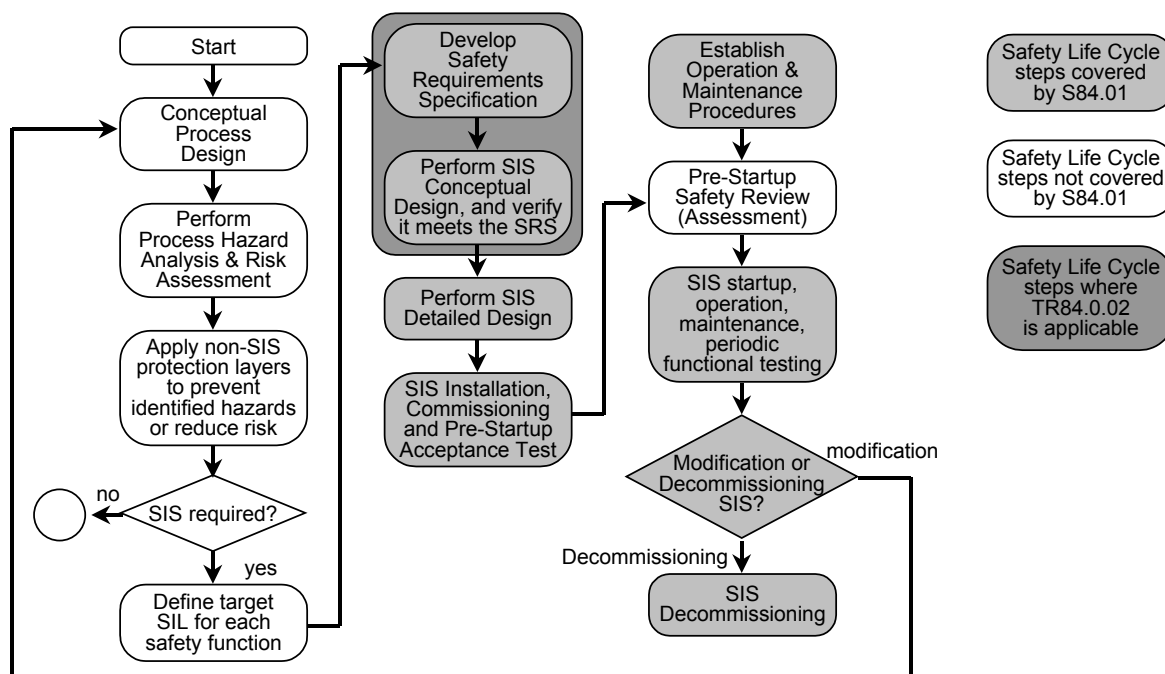


Figure 62 ANSI/ISA S84.01 : Safety lifecycle

B.2 IEC 61511

IEC 61511 is the process industry specific standard on safety-instrumented system and has defined clear requirements concerning the management of functional safety (IEC 61511-1, clause 5.2). The general objectives are to identify the policies and strategies for achieving safety together with the means for evaluating its achievement, which are communicated within the organization. A safety management system is intended to ensure that safety-instrumented systems are able to maintain and/or put the process in a safe state. An important aspect of complying with these objectives is to implement a safety lifecycle structure and planning. Safety planning is necessary to define the activities required, along with the individuals, departments, organization, or other groups responsible for carrying out these activities. This planning is to be updated as necessary throughout the entire safety lifecycle. The safety planning may be incorporated in a section in the quality plan entitled “safety plan” or a separate document entitled “safety plan”, or several documents which may include company procedures or working practices.

The target of application of the safety lifecycle is described in IEC 61511-1, clause 6. The objectives of the requirements in this clause are to organize the technical activities into a safety lifecycle, and to ensure that there is adequate planning for making sure the safety-instrumented system meets the safety requirements or that this planning will be developed. A safety lifecycle incorporating the requirements of this standard is to be defined during safety planning. Each phase of the safety lifecycle will be defined in terms of its inputs, outputs, and verification activities.

Requirements (IEC 61511-1, clause 5.2):

- General
 - The policy and strategy for achieving safety shall be identified together with the means for evaluating its achievement and shall be communicated within the organization.
 - A safety management system shall be in place so as to ensure that safety-instrumented systems have the ability to place and/or maintain the process in a safe state.
- Organization and resources
- Risk evaluation
- Planning
- Implementation and monitoring
- Assessment, auditing and revisions

Planning requirements:

Safety planning shall take place to define the activities that are required to be carried out along with the persons, department, organization or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire safety lifecycle.

NOTE The safety planning may be incorporated in:

- a section in the quality plan entitled “safety plan” or;
- a separate document entitled “safety plan” or;
- several documents which may include company procedures or working practices.

Safety lifecycle structure and planning (IEC 61511-1, clause 6)

Objectives

The objectives of the requirements of this clause are to:

- organize the technical activities into a safety lifecycle;
- ensure that adequate planning exists or is developed that makes certain the safety-instrumented system shall meet the safety requirements.

Requirements

- A safety lifecycle incorporating the requirements of this standard shall be defined during safety planning.

Each phase of the safety lifecycle shall be defined in terms of its inputs, outputs and verification activities.

Not surprisingly, this lifecycle (see Figure 63) shows clear similarities with the IEC 61508 (see Figure 7) and ANSI/ISA S84.01 lifecycles (see Figure 62).

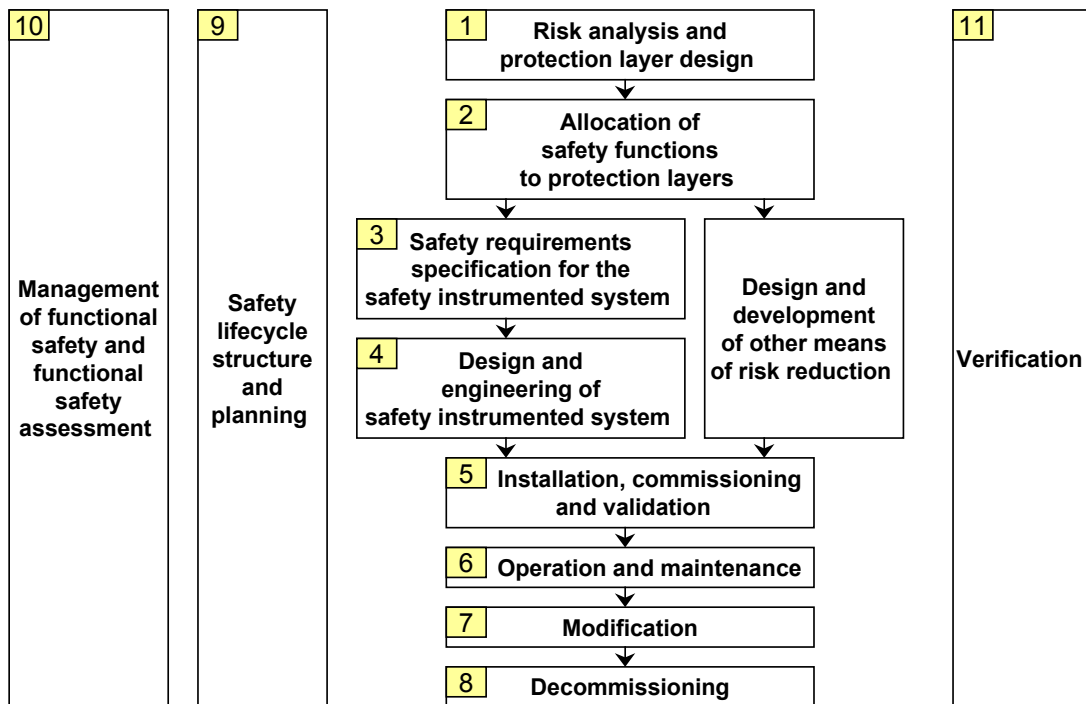


Figure 63 IEC 61511 Part 1, Safety lifecycle

B.3 EN 50126

EN 50126 [EN 50126] – The specification and demonstration of reliability, availability, maintainability, and safety (RAMS) for railway applications - Part 0, Dependability.

The purpose of this EN standard draft is to provide railway authorities and the railway support industries throughout Europe with a common process to specify the dependability requirements and to demonstrate that these requirements have been achieved. The concept of the system lifecycle is fundamental to the process. The process requires that the railway authorities adopt a top-level policy for quality, safety, and performance. The system lifecycle shown in Figure 64 describes the various phases of the system, from concept to its final removal from service and is fundamental to the understanding and implementation of this European standard.

Furthermore, EN 50126 has defined a specific safety lifecycle for railway applications and gives an overview of the relationship of the system lifecycle to the safety lifecycle. Allocation of the specified safety lifecycle phases is applied in the system lifecycle.

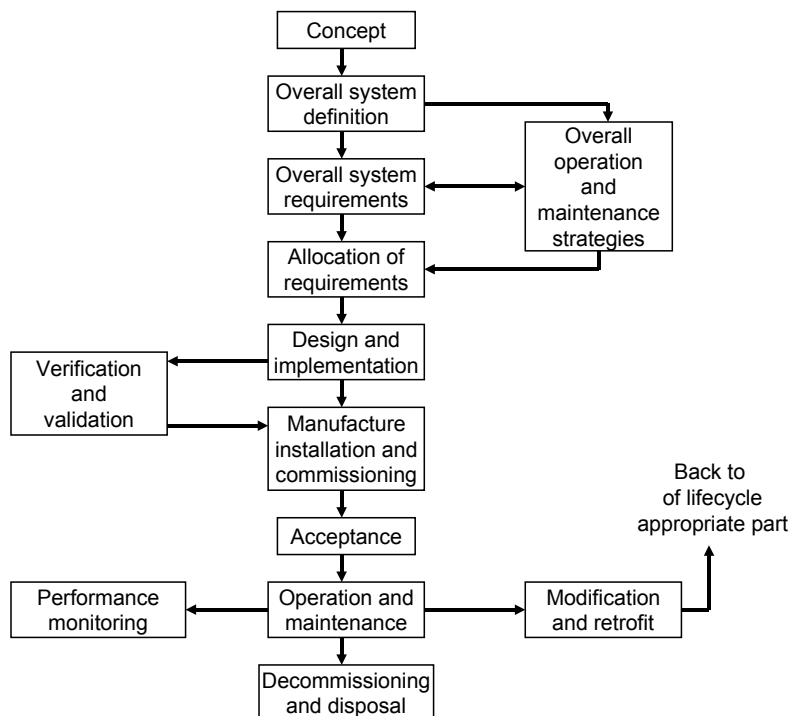


Figure 64 EN 50126-0 : System lifecycle

Annex C SLM interview procedure and questionnaire

C.1 Introduction

C.1.1 Interview goal

Unfortunately, many industrial processes are characterized by the potential occurrence of hazardous events and the related risks for people, environment and asset loss. In order to reduce these risks to an acceptable level, all kinds of safeguarding measures are taken. Obviously, it is of essential importance to optimize their effectiveness and efficiency, and take care that the working effect is maintained. Therefore, it is of the utmost importance to control functional safety of the equipment during its entire lifetime.

Most recent standards in this area (IEC 61508 and ANSI/ISA S84.01) are therefore based on the application of a safety lifecycle. The whole path that needs to be gone through with regard to, identification of potential hazardous situations, definition and realization of safeguarding measures, operation and maintenance of the safeguarding equipment and the finally decommissioning of this equipment, needs to be done in a safe manner (all safety lifecycle activities).

The final purpose of the researchers is to establish the necessary measures in order to implement the Overall safety lifecycle of IEC 61508. Potential bottlenecks with regard to the implementation need to be revealed and solved.

C.1.2 Investigation organization

By means of performing interviews with people involved, the researchers try to create an overview of the way the company manages the safety of its industrial processes by investigating all safety-related activities. With that, the structure described below is used.

The safety-related activities that are carried out by the interviewee are central. In order to ‘safely’ take care of such an activity, a number of aspects need to be carefully considered. These aspects are the following:

- Objective(s) : The precise objective of this activity.
- Competence of persons Requirements concerning the involved people.
 :
- Tools & Methods : Means methods, tools and techniques to be applied.
- Input information : Required information needed for the activity.
- Requirements : Preconditions like procedures and work instructions.
- Output information : The results and information to be produced
- Documentation : Required documentation to be created and maintained.

This is schematically presented in Figure 65. The questions to be asked during the interviews are based on this scheme.

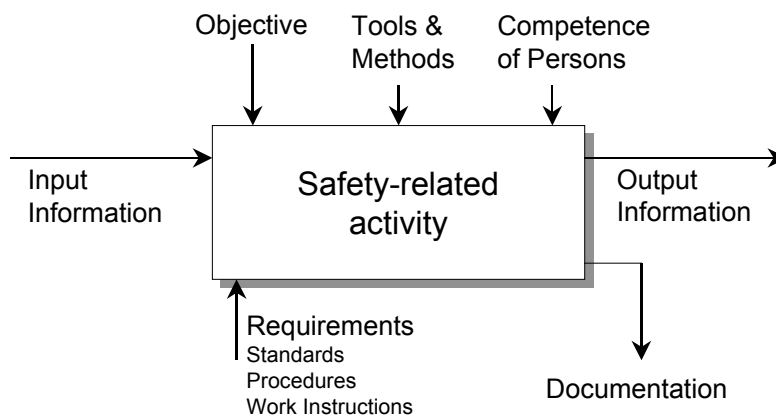


Figure 65 Safety-related activity model

With the use of the scheme of Figure 65, the specific lifecycle model of the company or organization can be created. This model will subsequently be compared with the reference models as defined in official standards such as IEC 61508 and ANSI/ISA S84.01. On the basis of this comparison it can be concluded whether the actually applied model deviates from the reference models.

It is of essential importance to find out *why* deviations are observed. It could e.g. be the case that the reference models do not fit on the specific actual situation. It will have to be analyzed whether the actual model need to be improved and how it could be implemented into the SMS. In order to realize this latter step, each aspect of the above model is further dealt with by detailed questions concerning the following situations.

- Formal situation : What is officially documented and required? What should be done according to procedures / work instructions?
- Actual situation : What is the actual situation and why are deviations from the formal situation present?
- Ideal situation : How could an ideal situation be defined?

This is schematically represented in Figure 66:

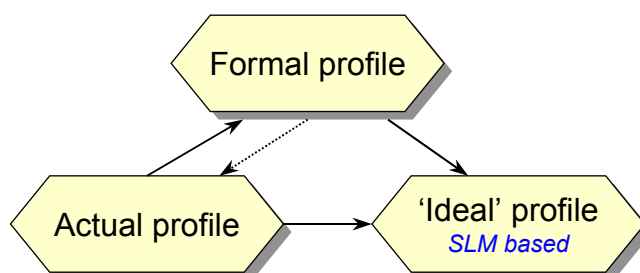


Figure 66 Different situations that can be distinguished

One can imagine that in reality (the actual situation) at certain points is deviated from the formal situation for certain practical reasons. By means of adapting the formal requirements and the SMS, the actual situation could be brought back in agreement with the formal and ideal situation.

C.1.3 Research results

The results of the research will be included into a report and be made available to the company.

The report will contain recommendations concerning measures to be taken.

C.1.4 Confidentiality of the interviews

The information obtained from the interviewees will be treated confidentially. Also the final results will be treated confidential and only be made available to the investigated company or organization.

C.1.5 Interview topics

- Safety awareness in general
- Involvement and responsibility of the interviewee in the IEC 61508 Overall Lifecycle model
- Process safety goals, strategy and policy
- Expertise and experiences of the interviewee
- Safety-related activities
- Communication methods and information flows
- Safety-related document control

C.2 Safety-related activities

This section shows the questions as used in the SLM interviews.

C.2.1 Safety in general

- Could you give a short description of your job (tasks, responsibilities)?
- Are you, in your opinion, sufficiently informed concerning the existence of potential hazardous situations, which may occur and are related to the existing processes, installation and materials?
- Are you informed on the safeguarding measures that are taken to prevent the occurrence of such situations?
- Are you aware of the official legislation and standards concerning process safety?

C.2.2 Position related to the IEC 61508 Overall lifecycle model

- Can you indicate in the IEC 61508 Overall Safety Lifecycle model or company lifecycle for which phase(s) or activities you are responsible or involved?
- To which persons do you report and give account with regard to the safety-related activities as carried out by you?

- Which persons are reporting to you and give account to you concerning the safety-related activities as carried out by them?
- Could you indicate which colleagues are responsible for the activities of the adjoining lifecycle phases and the other phases in general?
- Do you have a structured and organized contact and communication with these people?

Example of process-oriented information flows (horizontal) and task oriented information flows (vertical):

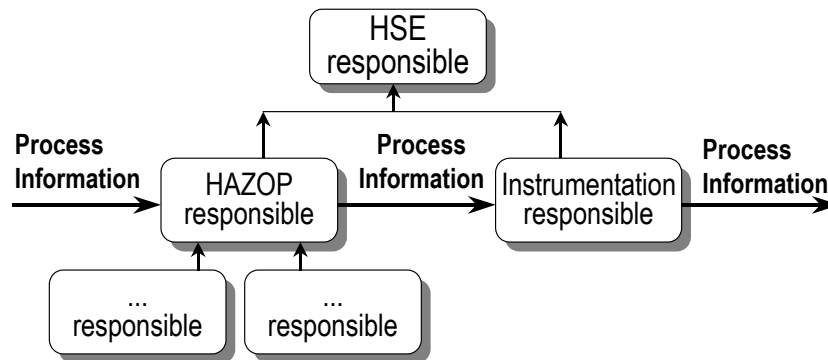


Figure 67 Example of process-oriented information and task oriented information flows

C.3 Objectives

This section discusses the goals, strategy and policy of process safety management.

C.3.1 Goals

- Are clear goals defined for each mentioned activity with regard to the safety-relevant aspects? Are these goals documented?
- What are these goals?
- Are these goals part of a safety plan?
- Is there a document describing this safety plan?

C.3.2 Strategy – Policy – Organization

- Are the mentioned goals implemented in a safety policy?
- How is this safety policy organized? (Structure of the SMS?)
- By which means is awareness and commitment created with regard to the safety policy?

C.3.3 Responsibilities and accountabilities

- Who is responsible for the execution of the safety policy?
- Is an organization chart developed (as part of the SMS), which indicates the distribution of the responsibilities?

C.4 Regulations, information and documentation control

This section evaluates the aspects, output information, input information, regulations and documentation control. The scheme of Figure 68 shows an overview of the various types of information and documentation flows.

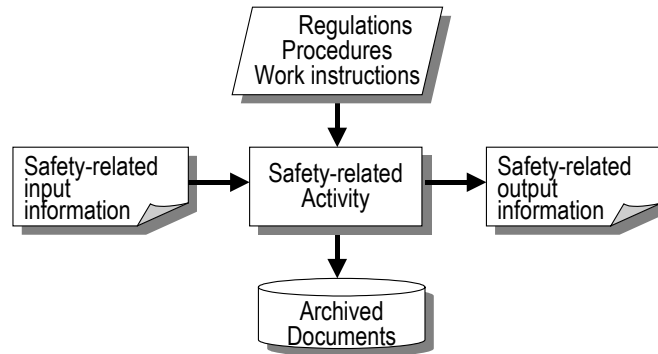


Figure 68 Various types of information flows

C.4.1 Input information

- What (kind of) information is needed to be able to correctly carry out the mentioned safety-related activities?
- From who can this information be obtained, or where can this information be found?
- Are there formal or informal guidelines that indicate how to obtain this information?
- What are the used attributes concerning the safety-related input information? (Title, name, scope of contents, index, revision number, version number, approval, distribution list, maintained by..., allocated/archived at, accessible to...)
- Do the existing communication means function adequately in your opinion, and why (or why not)?

C.4.2 Output information

- Could you give an overview of the (required) output information of the safety-related activities concerning which you are responsible or involved? (E.g. HAZOP results serve as input to do a risk analysis.)
- Which attributes are the used concerning the safety-related output information? (Title, name, scope of contents, index, revision number, version number, approval, distribution list, maintained by..., allocated/archived at, accessible to...)
- How is the distribution of this output information controlled?
- Is a control mechanism present to check whether the right persons received this information and whether these persons have understood the information?

C.4.3 Requirements

Regulations, standards and instructions

- Which standards and corporate guidelines are applicable to the earlier mentioned safety-related activities?
- How and by who is established which standards need to be complied with?
- Are on a regular point in time verified whether these standards cover the defined goals?
- Is this done in a structured manner?
- Which attributes are the used concerning the safety-related standards? (Title, name, scope of contents, index, revision number, version number, approval, distribution list, maintained by..., allocated/archived at, accessible to...)
- Where and how can these regulations, safety standards, and instructions be found?

Work-instructions and procedures

- What are the applicable work instructions and procedures with regard to the mentioned safety-related activities?
- Which attributes are the applied concerning these work instructions and procedures? (Title, name, scope of contents, index, revision number, version number, approval, distribution list, maintained by..., allocated/archived at, accessible to...)
- Where and how can these work instructions and procedures be found?

C.4.4 Documentation

- What kind of documentation needs to be developed (as evidence) concerning certification, insurance, etc.?
- What are the applied attributes concerning documentation? (Title, name, scope of contents, index, revision number, version number, approval, distribution list, maintained by..., allocated/archived at, accessible to...)
- Where and how can these documents be found?

C.5 Competence of persons

This section evaluates the requirements on competence of people.

C.5.1 Education

- Are particular qualifications (education) required for the involved people concerning the mentioned safety-related activities? Is the technical required knowledge specified?
- Does a specification exist concerning the required knowledge of the dangerous processes, installations and material?

C.5.2 Experience

- Is the required experience, concerning the participation and execution of the safety-related activities, specified?
- Is the experience, concerning the required permit to work with processes, installations and material, specified?

C.5.3 Training

- Are employees who are involved in the safety-related activities trained?
- What kind of training needs to be followed?
- Does this training need to be followed on a periodical base?
- Is the training closed with an exam?

C.5.4 Documentation of competence of persons

According to IEC 61508, the required training, qualifications and experiences need to be documented. How is taken care of this?

C.6 Communication of safety-related aspects

Successful application of the safety lifecycle model requires a mutual adaptation and cooperation of involved people. This means that the contacts and communication needs to be structured and maintained.

- Is there a structural contact between the people involved?
- How is this contact organized?
- Who are responsible for maintaining and controlling these contacts?
- Are the results of these structural contacts documented and distributed?

C.7 Tools & Methods

In order to carry out the safety-related activities, it might be necessary to make use of specific aids (tools, methods, instruments). Through correct application of these aids a constant and controlled quality can be achieved.

- Are tools, methods or other aids required and made available to carry out the mentioned safety-related activities?
- If that is the case, what are precisely these aids?
- What (kind of) output needs to be generated by these aids?
- Which persons need to receive these outputs?
- Is it possible to precisely reproduce the output using these aids? (And thus control the quality of the output.)
- Who is responsible for the ‘maintenance’ of these aids?

- Are tools that are used certified/compliant to certain safety standards?

C.8 Continuous improvement

IEC 61508 is a standard and therefore does not contain requirements that demand continuous improvement. Nevertheless however, continuous improvement might be needed to achieve certain goals.

- How is currently dealt with deviations e.g. with IEC 61508?
- How are these deviations observed and measured?
- How are these deviations processed?
- Is a ‘near miss’ reporting system implemented?

C.9 Assessment

Standard IEC 61508 requires the execution of a safety assessment on a periodical base. In order to correctly carry an assessment out, the standard contains requirements with regard to this.

- Are safety assessments currently carried out?
- At which moments of the overall safety lifecycle are they carried out?
- Who is responsible for this assessment?
- Is this person, department or organization independent?
- Is this person, department or organization accredited to do safety assessments?
- Is an assessment scheme used?
- How are results documented?

Annex D Development aspects of activity flowcharts

– *Benefits of developing activity flowcharts*

Flowcharts can be used to identify the actual flow or sequence of events in a process that any product or service follows. Flowcharts can be applied to anything from the travel of an invoice or the flow of materials, to the steps in making a sale or servicing a product [ISO5807], [Das78] and [Bra94].

Two key elements are the conventions of symbols and the step-wise flowchart design. An adapted definition of the symbols, conventions etc. is made, whereas as far as possible the generic standard conventions are followed.

According to Brassard [Bra94], in general, a flowchart has the following benefits. It;

- shows unexpected complexity, problem areas, redundancy, unnecessary loops, and where simplification and standardization may be possible.
- compares and contrasts the actual versus the ideal flow of a process to identify improvement opportunities.
- allows a team to come to agreement on the steps of the process and to examine which activities may impact the process performance.
- identifies locations where additional data can be collected and investigated.
- serves as a training aid to understand the complete process.

– *Composition and construction of the SR activity model*

Brassard [Bra94] has defined the following steps to set up a flowchart:

1. Determine the frame and boundaries of the process.
The analyzers will have to agree on the level of detail that must be shown on the flowchart to clearly understand the process and identify problem areas. The flowchart can be a simple macro-flowchart showing only sufficient information to understand the general process flow or it might be detailed to show every finite action and decision point. The analyzers might start out with a macro-flowchart and then add in detail later or only where it is needed.
2. Determine the steps in the process.
Normally, this step is characterized as purely a brainstorm activity. As part of the SLM assessment however, it is guided by the defined safety lifecycle and of course the scope definition of the SIS-related SMS.
3. Sequence the steps.
Especially in a situation of indistinctness flowcharts show their added value.
4. Draw the flowchart using the appropriate symbols.
With regard to the drawing of the flowchart using the appropriate symbols, also standard ISO 5807 ('Information processing, Document symbols and conventions for data, program and system flowcharts, program network charts and systems resources') offers clear definitions.
5. Test the flowchart for completeness.
See next analysis step.

6. Finalize the flowchart.
See next analysis step.

– *Testing and verification of the flowchart*

According to Brassard [Bra94] as a first verification the flowchart should be tested for completeness. These tests consists of:

- Correctness of the used symbols.
- Identification of process steps (inputs, outputs, actions, decisions, etc.).
- Verification that each feedback loop is closed, i.e. every path goes back to or ahead to another step.
- Continuation-check that every point has a corresponding point elsewhere in the flowchart.
- The application of decision diamonds especially in case more than one output arrow per activity is identified.
- Validation of the flowchart by people, who are not involved in the flowchart definition, but who carry out the process actions.

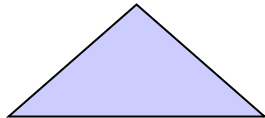
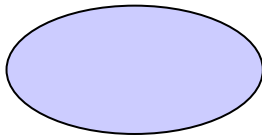
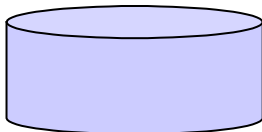
Once the flowchart is correctly and completely set up, it can be further analyzed with regard to the ‘ideal’ situation. Brassard [Bra94] has defined the following questions:

- Is the process being run the way it should be?
- Are people following the process as charted?
- Are there obvious complexities or redundancies that can be reduced or eliminated?
- How different is the current process from an ideal one?

Annex E SLM activity flow chart symbol conventions

The symbols are based on the flow chart conventions that are developed for the information technology. To make them useful for SLM assessments, they are redefined as presented in Table 15 (See also [ISO5807], [Meu95]).

Table 15 Activity flow chart symbol conventions

Lifecycle phase	
	<p>A lifecycle phase can comprise more than one SR-activity. The common characteristic of these activities is that together they achieve the overall objective of this lifecycle phase.</p> <p>According to the American Heritage Dictionary:</p> <ul style="list-style-type: none">– ‘A distinct stage of development’– ‘A temporary manner, attitude, or pattern of behavior’– ‘An aspect; a part’– ‘A particular stage in a periodic process or phenomenon’ <p>Example of a lifecycle phase according IEC 61508 part 1 clause 7.8: Overall safety validation planning</p>
Objective	
	<p>Based on the mission statement, safety strategy and subsequent safety policy, the objectives of each lifecycle phase shall be defined. The objective is therefore, among other things, characterized by a clear scope definition. Also the required output of the concerned phase is typically part of the definition of the objective. To achieve the defined objective, a number of safety-related activities may need to be carried out. Therefore, a lifecycle phase objective can be split into a number of sub-objectives, where for each safety-related activity, a dedicated objective is defined.</p> <p>A very important aspect that determines the successful achievement of the objective is not restricted to a clear and unambiguous description, but also the explanation ‘<i>why</i>’ it is important that the objective is adequately achieved.</p> <p>Example of an objective according IEC 61508 part 1 clause 7.8.1: The objective of the requirements of this sub-clause is to develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.</p>
Information source	
	<p>Information sources could be documents, databases etc. An information source only exists if information is stored into this source. Therefore, an information storage database could also be considered as an information source.</p>

SR-activity



As already described under objective, to achieve the defined objective, a number of safety-related activities may need to be carried out.

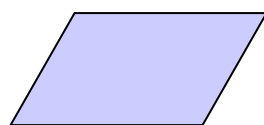
Example of a safety-related activity according IEC 61508 part 1 clause 7.8.2.1:

A plan shall be developed which shall include the following:

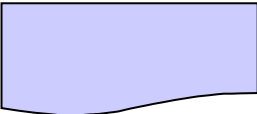
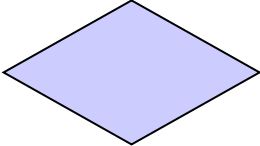
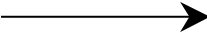
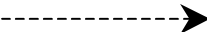

- a) Details of when the validation shall take place;
- b) details of those who shall carry out the validation;
- c) specification of the relevant modes of the EUC operation with their relationship to the E/E/PE safety-related system, including where applicable:
 - preparation for use including setting and adjustment,
 - start up,
 - teach,
 - automatic,
 - manual,
 - semi-automatic,
 - steady state of operation,
 - re-setting,
 - shut down,
 - maintenance,
 - reasonably foreseeable abnormal conditions;
- d) specification of the E/E/PE safety-related systems which need to be validated for each mode of EUC operation before commissioning commences;
- e) the technical strategy for the validation (for example analytical methods, statistical tests, etc);
- f) the measures, techniques and procedures that shall be used for confirmation that the allocation of safety functions has been carried out correctly; this shall include confirmation that each safety function conforms:
 - with the specification for the overall safety functions requirements, and
 - to the specification for the overall safety integrity requirements;
- g) specific reference to each element contained in the outputs from 7.5 and 7.6;
- h) the required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment);
- i) the pass and fail criteria;
- j) the policies and procedures for evaluating the results of the validation, particularly failures.

NOTE In 'planning the overall validation', account should be taken of the work planned for E/E/PES safety validation and software validation as required by parts 2 and 3. It is important to ensure that the interactions between all risk reduction measures are considered and all safety functions (as specified in the outputs of 7.5) have been achieved.

Data


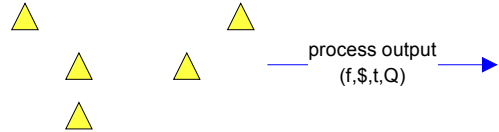
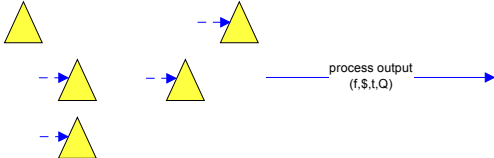
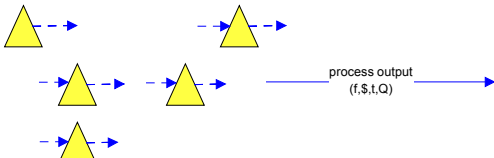
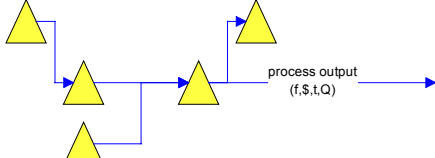
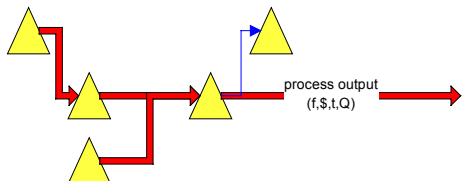
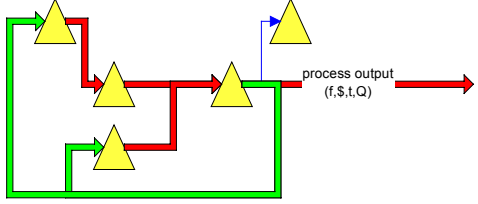


Any kind of information, in any form, that is transferred from one activity to another activity.

Document	
	A document is a kind of information carrier. It could e.g. be a paper document or an electronic file.
Decision	
	E.g. during the Process Hazard Analysis (PHA), the PHA team shall determine whether a hazardous event is classified as being a high, medium or low risk.
Symbol	Description
	<p>Required information flows according e.g. IEC 61508</p> <p>Example according IEC 61508 part 1 clause 7.8.2: The information from 7.8.2.1 shall be documented and shall constitute the plan for the overall safety validation of the E/E/PE safety-related systems.</p> <p>Example according IEC 61508 part 1 table 1, safety lifecycle phase 1: Required inputs: Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements. Required outputs: A plan to facilitate the validation of the E/E/PE safety-related systems.</p>
	Missing information flows
	Realized and required information flows

Annex F Steps used in activity model development

Table 16 Steps used in activity model development

Step	Activity
1	Identify process output 
2	Identify related activities ⇒ identify methods/tools Note: a triangle represents a collection of SR activities. 
3	Identify input ⇒ Identify suppliers 
4	Identify output ⇒ Identify customers 
5	Confirm input as supplier output 
6	Confirm output as customer input
Step	Activity
7	Form linked activities into reliability information flow 
8	Identify off-process outputs
9	Identify feedback loops/ learning cycles 

Curriculum Vitae

Bert Knegtering was born in Eindhoven, the Netherlands on 11 October 1967. He obtained his MSc in mechanical engineering at the Technische Universiteit Eindhoven, where he performed his masters project within the chair Reliability of Mechanical Equipment.

Since 1996, he has been working for Honeywell Safety Management Systems in the area of safety and reliability engineering. As a senior consultant in industrial process safety, he is closely associated with the application of safety-related systems in the most effective and efficient way that make process plants safe in accordance with applicable standards and regulations. Implementation of standards like IEC 61508, IEC 61511, and ANSI/ISA S84.01 form a major part of these activities. Furthermore, Bert is a member of the IEC 61511 standard technical committee, which is the process sector specific standard of IEC 61508. Almost on a daily base, he is involved in helping end-users in the process industry to implement safety lifecycle management activities.

