KOMB - A new approach to hazard analysis in plant design

Bönig, S.; Heimannsfeld, K.

Im Rahmen des Sonderforschungsbereiches 180 „Konstruktion verfahrenstechnischer Maschinen bei besonderen thermischen, mechanischen oder chemischen Belastungen“ befaßt sich das Teilprojekt A2 „Wissensbasierte Fehler- und Störfallanalyse bei der Entwicklung verfahrenstechnischer Maschinen mit Methoden der präventiven Störfallanalyse“. Im folgenden soll eine neue Methode zur Fehler- und Störfallanalyse vorgestellt.

This paper will develop requirements for a safety analysis and present a new approach for a failure and hazard analysis in early phases of plant design. This work has been carried out in the special research area 180 “Design of process engineering machinery with special reference to exceptional mechanical, thermal or chemical stress“ in the project A2 “Knowledge based failure and hazard analysis in the design of process engineering machinery“.

1 Requirements for safety analysis methods in plant design

When establishing the requirements to carry out a safety analysis method in plant design special features have to be taken into account. The requirements result from a multitude of different substances used in chemical plants which may be aggressive, toxic, corrosive or flamable. Different effects have to be considered: effects among the substances for instance, effects between the substances and adjoining materials in view of operating parameters as well as corrosive influences etc.

Furthermore the human factor is important when looking at chemical plants. The probability of a fault action or a late action is dependent on different influence factors and must be considered when carrying out safety analysis methods: the operator often has to intervene, for instance to repair or to replace abrasive elements, to start-up or shut down the plant or has to transport materials. Each change in operation indicates risks because of unstable operating conditions.

Depending on their origin most safety analysis methods have been defined with their specific requirements. However to select the most appropriate method the user will have to consider a lot of alternatives. In the following we will demonstrate some of the most important requirements for safety analysis which have been divided according to four different classes:

- General aspects
- Integration into the design process
- Application to chemical plant design
- Law requirements

1.1 General aspects

The major aspect of the industrial use is the economic benefit obtained. Therefore costs and time consumed must be acceptable and especially predictable. Kuhlmann /7/ demands that the external safety requirements are fulfilled while minimizing the additional costs for safety measures. To save further costs and time the reusability of past analysis should be considered. Reusability goes along with good precise documentation. Each step taken as well as the results should be documented in a clear, precise and comprehensive fashion understandable also to external experts.

To ensure that no hazard is overseen the approach should guide the analyst systematically while allowing for some creative freedom. The analysis should be extentable to support later changes and extensions of the system in review. The analysis should clearly elicit the event chain that transforms a potential hazard into an accident. Furthermore the method should support new as well as existing systems. It should also allow to reexamine parts of a system when changes occur.

The usability is often defined by the implementation rather than by the method itself. The user interface, implemented through paperwork or a computer program is the key for the acceptance by the user and its success. Finally the analysis should yield a final and definite result.

1.2 Integration into the design process

It is well known that an early integration of hazard analysis will result in a reduction of costs and time. However as input data is fuzzy in early conceptual design phases it is necessary that each stage in the design of a system is accompanied with the appropriate method.

The approach itself has to be adapted to the specific design process of the domain of application. It should be organized in small and manageable parts. Provisions for several iterations in the analysis should be included. The analysis should start as early as possible in the design process and should accompany the design process in parallel /7/. For a concurrent application of safety analysis methods throughout the design process it is necessary to combine different methods.

The analysis should be able to cope with several iterations, since changes may introduce further safety relevant aspects. Optional the documentation should support the possibility of changes /10/. Maintenance, inspections and human operators (and their erroneous behavior) should be taken into account while designing the system. The design should follow the basic principles of safe design for life, failsafe design and protection against sabotage /11/.

1.3 Application to chemical plants

A hazard and safety analysis applied to chemical plants should support the following requirements:

- It should be possible to examine the complete plant or subsystems. Therefore the plant is divided into units of functionality and function elements.
- The following data should be taken into account if the design in review is a new design:

  Plant organisation, production process, working method, all possible states of operation (including health hazards i.e. noise emissions, dust and hazardous substances), substances used and their properties (i.e from DIN 52900 or Dows fire and explosion index and hazards classification guide), process parameters (i.e. pressure,temperature, mass, flows), process equipment materials, plant layout, safety relevant control equipment,...
- The hazard analysis method should be able to cope with continuous and batch processing /8/.
- It should be possible to visualize and to analyse the chain of events resulting from an initial event.

1.4 Law requirements

Safety critical plants may be required to conduct hazard analysis by law (i.e. BImSchG, OSHA standards). The hazard analysis must therefore be comprehensible to the supervising authority. The results of the analysis should document the effort.

The german **BImSchG** for example requires the analysis to include the following information /6,9/ :

- description of the plant or the process under normal conditions, including type, amount and process parameters of the chemicals used,
- description of the safety relevant components (components with hazardous materials, safety devices, ...),
- description of hazards (internal hazards, external hazards, hazards from sabotage),
- investigation of initial or starting events,
- description of accident prevention measures,

description of accident limiting measures, evaluation of the accident effects.

In the next chapter we will look at the procedure for a Hazard and Operability Study (HAZOP) to shown how this specific method fulfills the defined requirements. After the discussion of advantages and disadvantages of HAZOP we will develop a new approach in chapter 3.

2 HAZOP

The Hazard and Operability Study (HAZOP) has been developed in England end of the seventies /5/ to discover and avoid hazards originating from chemical plants. "*HAZOP is a technique which provides opportunities for people to let their imagination go free and think of all possible ways in which hazards or operating problems might arise, but - to reduce the chance that something is missed - it is done in a systematic way*" /4/. The study is carried out by a team from different fields of expertise. In this way the members will stimulate each other and will build upon each other´s ideas. Detailed information as plant layout, flow sheets etc. is needed to carry out the study.

HAZOP starts with the partitioning of the system into subsystems (or main plant items). For each subsystem the system function is defined. A pipeline connecting two items for example should allow only forward flow. The pipeline is then analysed by creating a deviation by combining a guide word with the system function. The seven guidewords are describing changes in quality and quantity such as NO/NONE, MORE OF, LESS OF, AS WELL AS, PART OF, INVERSION and OTHER. The next step evaluates the deviation for the possible causes, the effects and required countermeasures and actions /1/. Due to the strong systematic approach HAZOP is easy to learn. Each step in the study as well as the end is clearly defined.

The costs and the work for a HAZOP study can be tremendous. The reuse of a study for similar arranged components is seldom feasible. Furthermore it is not possible to consider combinations of faults besides individual faults and hazards.

After proposing countermeasures the study has to be repeated. Without repetition the system might be even unsafer. A weak point of HAZOP is that there is no control concerning the definition of the system function. When evaluating the system function the team just checks the intended purpose, its completeness and correctness. The purpose by itself will not be analysed. Furthermore it is not always guaranteed that by the means of the guidewords the allowed increase/decrease of the process parameters can be shown precisely in order to estimate the causes and the effects on the system.

HAZOP cannot fulfill all requirements besides its advantages. The following weak points cannot be accepted here:

- the high amount of time when defining the “system function“ for each subsystem and the doubt of its correctness,
- the documentation of causes and effects without systematic and clear order to work out sensible and sufficient countermeasures without high documentation time.
- Correlations cannot be shown in the HAZOP formular, there is no space for additional informations.

In the following chapter a modified HAZOP analysis will be introduced to overcome some of these problems.

3 The KOMB-Analysis

The KOMB-Analysis has been developed as a qualitative safety analysis to investigate chemical plants in the stage of design phase when P&I-flowsheets are available /3/. KOMB- Analysis means:

Kombinierte **O**perabilitäts-, **M**atrix- und **B**ewertungsanalyse.

The aim of this analysis is to discover faults, to determine causes and effects, to show its correlations as well as to work out and assess necessary countermeasures.

In connection with other analysis methods KOMB can be used in design process of chemical plants as an integrated safety analysis. After “Definition of components structure“ when single machines, devices or rigs have been chosen to carry out the physical operations needed and when the principal measures have been established the modified analysis can be applied. After realizing necessary countermeasures as a result of the KOMB-analysis the design process may continue: the requirements of each element can be established.

Actualized informations of all stages of the design process must be available to the interdisziplinary team. Besides the P&I-flowsheets, variants of solutions inclusive, the team needs all line or process diagrams and the list of properties.

The user has to be aware of safety and economic aspects as well as is obliged to consider ethical factors when planning chemical plants with high risks for mankind, machines and environment. “Inherent safety“ must been given priority.

The process to carry out KOMB is shown in fig. 3.1. The main steps are as follows:

- *Dividing the system into subsystems,*
- *Examination of safety relevant components,*
- *Processing of components K1, ..., Kn,*
- *Detailed function of component K1,*
- *Determination of realistic faults S1,1;...; S1,m,*
- *Determination of causes Cx,*
- *Determination of effects Ex,*
- *Processing of components K2, ..., Kn,*
- *Creation of causes-effects-matrix,*
- *Creation of causes-components-matrix,*
- *Assessment of measures (1),*
- *Actualization of causes-effects-matrix,*
- *Creation of effects-components-matrix,*
- *Assessment of measures (2),*
- *Changes in planing documents,*
- *Assessment of hazards.*

⇒ *Dividing into subsystems*

Similar to HAZOP subsystems of the P&I-flowsheet will be coloured marked. The subsystems have to be checked in succession but the analysis should be carried out in view of the safety of the entire system. Size and amount of subsystems are

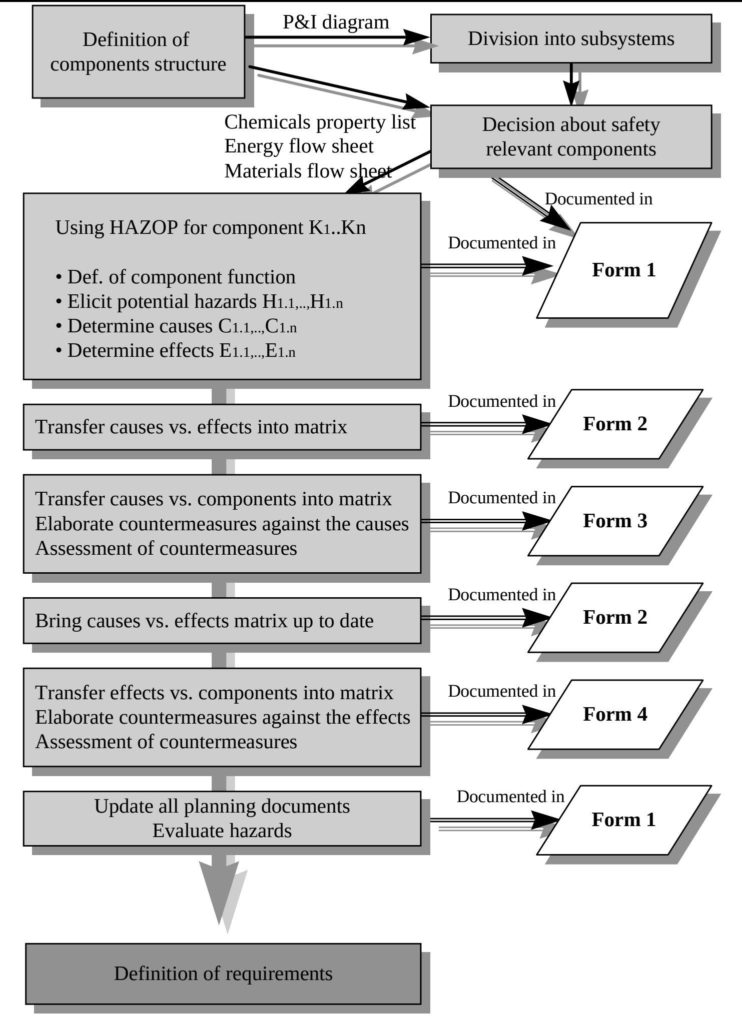

Figure 3.1: General approach of the KOMB analysis

dependent on the kind of plant and the user´s experience. A subsystem may be for instance a system that can run by its own, that is important to the entire system or that is an aid to operate the plant /9/.

An additional description of the plant and process is necessary when this analysis is used to analyse chemical plants for which a liscence is required for, see 12. BImSchV.

⇒ *Examination of safety relevant components*

In order to reduce the time needed only safety relevant components will be considered (as demanded in 12. BImSchV).

1. Parts of plant with special substances:

bins, silos, bunkers, reactors, filters, separators, washers, towers, pumps, compressors, ventilators, coolers, heat exchanger, pipelines, ...

2. Protective devices:

relief and safety valves, fire fighting installations, catch basins, ...

3. Other parts of plant important to operation reliability:

machines to ensure addition and output of energy, machines to ensure mass flux, parts of plant to discharge, eliminate or to detain substances (according to appendix 2 of 12.BImSchV),...

To carry out this analysis the following criteria will be added:

4. Substances used in the operation:

correct description, material data, compounds, additives, properties, flash point,...

5. Process parameters:

pressure, temperature, mass, mass flow, concentration, properties,...

⇒ *Processing of components K1,..., Kn:*

The components as mentioned above will be numbered and will be worked on separately.

⇒ *Detailed function of component K1:*

The function of component K1 of the subsystem has to be described shortly.

⇒ *Determination of realistic faults S1,1; ...; S1,m:*

Realistic deviations from normal operation, further on called hazards, will be analysed first concerning component K1 by the means of the function and the guidewords of HAZOP, see table 3.1. **Table 3.1:** Guidewords used in HAZOP and KOMB /1,4/

Guidewords	**Meaning**
NO/NONE	negation of the function
MORE OF/LESS OF	quantitative increase or decrease
AS WELL AS	qualitative increase
PART OF	qualitative decrease
INVERSION	the logic opposite of the function
OTHER	total replacement (exchange)

The guidewords are applied to the component´s function, for example its way of working or the substance`s properties.

⇒ *Determination of causes Cx:*

The causes of each hazard S1,x will be analysed. The detailed informations about the causes of hazard shall be helpful when eliminating the hazard in the analysis later on. Different cases can be taken into account:

- One certain cause results in more than one hazard: the number X of the cause will be the same for each hazard.
- One hazard will be caused by more than one cause, which is called common-mode-failure. The single causes have to be listed under one number X. Causes of hazards may be failure or reduction of the component, failure in design, operation or material.

⇒ *Determination of effects Ex:*

In the following step the effects Ex for each hazard S1 has to be determined. Different effects get different numbers, identical effects must get the same number. As before the analyst has to differ the following cases when numbering the effects:

- One hazard may cause different effects,
- One effect may be caused by different hazards.

⇒ *Processing of components K2, ...Kn:*

After considering component K1, the analysis has to be carried out in the same way for the remaining components K2 ... Kn. In the case of repeating causes/effects the analyst is free to use just the corresponding number to reduce the time of documentation. The results of KOMB will be recorded in four different formulars. All final results of the analysis will be recorded in the Table of Results, form 1 (see Table 3.2) which includes the following informations:

Col 1: the component.

Col 2: function of the component

Col 3: possible deviations from normal operation.

Col 4: causes of potential deviations.

Col 5: effects of potential deviations,

Col 6: countermeasures implemented,

Col 7: results from countermeasures

⇒ *Creation of causes-effects -matrix (Form 2):*

- The determined causes Cx and effects Ex will be recorded into the "causes-effects-matrix" underneath the other and side by side respectively, see table 3.3. Logic correlations between single causes of hazards and its possible effects will be symbolized through an X in the corresponding area.
- In each row an X indicates the effects Ex that will be caused by a certain cause Cx.
- In a column an X shows the different causes Cx of one special effect Ex.

The number of X indicates whether or not it is sensible to eliminate the causes directly or if this is impossible to reduce or to prevent the effects. The amount shown should be only a help to choose

Table 3.2: Table of Results (Form1)

1	2	3	4	5	6	7	
components	function	hazards/ risks/faults	causes	effects	measures	hazard eliminated	
						Yes	No
K1		S1,1	C1	E1			
				E2			
			C2	E3			
			C3	E4			
		S1,2	C3	E5			
K2		S2,1...	...	...			
...		...	...	...			
Kn		Sn,1...	...	...			

priory measures. In case of doubt the elimination of causes should be always preferred.

Table 3.3 : Causes-Effects -Matrix (Form 2)

	effects						
causes	E1	E2	E3	E4	...	Em	sum
C1	X	X					
C2			X				
C3				X			
...							
Cm							
sum							
testsum							

⇒ *Creation of causes-components-matrix (form 3)*

All determined causes will be recorded against the numbered safety relevant components in the causes-components-matrix, see table 3.4. The components now indicate the place of hazard. If necessary the analyst or the team has to suggest measures.

- Amount and place of X per column show how many and what kind of causes of a certain component lead to one or more hazards. A large amount of X indicates that this component is very temperamental for faults/hazards and has to be improved or even exchanged.
- The amount of X in a row makes clear how and what kind of components are affected by a certain cause of fault. A large amount of X here indicates for example that it is necessary to eliminate this cause to avoid failures of several component .

⇒ *Assessment of measures:*

The measures worked out have to be assessed by the means of three criteria:

1. The measure gets to <u>eliminate</u> the cause Cx <u>totally</u> (TE):
2. The measure gets to <u>eliminate</u> the cause Cx <u>partly</u> (PE):
3. A measure will <u>not</u> be suggested to <u>eliminate</u> the cause Cx (NE).

⇒ *Actualization of causes-effects-matrix:*

Afterwards the causes-effects-matrix has to be checked and if necessary changes have to be added. The columns of causes that could be totally eliminated through measures (TE) will be marked in colours or the actualized matrix will be drawn up without them for further investigation. After adding the X in a row the analyst has to determine the effects which primary need to be reduced or even eliminated.

⇒ *Creation of effects-components-matrix (form 4):*

The effects-components-matrix, shown in table 3.5 has to be drawn up similar to the cause-components-matrix. The aim of this matrix is to show clearly the connection between the effects and the single components as well as the urgency of necessary measures.

- A high amount of X in a column shows how many and which effects will be caused by the component looked at when hazards occur.
- A high amount of X in a row shows that many components cause one specific effect on the basis of hazards/failures.

By the means of the actualized causes-effects-matrix the analyst knows which ones of the causes could partly or even totally be eliminated by

Table 3.4: Causes-Components-Matrix (Form 3)

	component (place of hazard)								necessary measures	assessment of measures		
causes	K1	K2	K3	K4	K5	...	Km	Σ		TE	PE	NE
C1		**X**										
C2						**X**						
C3		**X**	**X**	**X**								
...												
Cm												
sum												

measures and the effects that need to be limited by measures.

⇒ *Assessment of measures:*

The measures to eliminate the effects will be carried out similar to the assessment above.

⇒ *Changes in planning documents:*

The suggested measures will be realized in the current planning documents using an iteration procedure. If necessary components added to the system have to be numbered and analysed as before in the forms (1)-(4).

⇒ *Assessment of hazards:*

On the basis of the assessed causes the hazard has to be assessed in the table of results (form 1), see table 3.2. The classification in eliminated hazard/not eliminated hazard is of use to actualize the results of the analysis: eliminated hazards will not be considered later on, when changes at the base of applied measures have already been carried out in all planning documents.

- One hazard does not occur, if all causes of one hazard can be eliminated totally by effective measures.

If it is necessary to consider time dependent events after finishing KOMB an Event Tree Analysis (ETA) can be applied.

3.1 Assessment of KOMB

KOMB is a safety analysis method that provides many positive characteristics to analyse P&I-flowsheets. After applying KOMB on different examples the following advantages will be emphasized now:

1. Systematic approach with definite and traceable results.
2. Clear, comprehensive documentation.
3. Concurrent analysis in parallel to design.
4. Analysis of layout of existing plants as well as new designed plants.
5. Iterative processing, use of EDP possible and recommended,
6. Usability for plants and subsystems,
7. Restriction to the examination of safety relevant components including process parameters and substances used to reduce time and costs.
8. Guarantee of availability and high quality of input data.
9. Definition of the component´s function to show the required conditions as well as to show the hazard preventing precautions.
10. Definition of hazards/risks/faults as undesired events of a component.
11. Consideration of common-mode-failures, human and material behaviour, maintenance and inspection,... .
12. Determination of the causes and the effects of hazards.
13. Establishing the correlations between causes and effects.
14. Drawing up of correlations between causes and place of hazards. (The analysis shows critical components which can be changed or replaced to eliminate the causes of hazards.)
15. Establishing the correlations between effects and place of hazards.
16. Establishing the measures to eliminate the causes of hazards and to reduce the effects of hazards.
17. Qualitative assessment of measures by the

Table 3.5: Effects-Components-Matrix (Form 4)

	component (place of hazard)								necessary measures	assessment of measures		
effects	C1	C2	C3	C4	C5	...	Cm	Σ		TE	PE	NE
E1		X										
E2						X						
E3		X	X	X								
...												
Em												
sum												

means of three different criteria.

18. Optimal conditions for safety and economy through assessment of measures to eliminate causes and/or effects of hazards.

19. Assessment of hazards with the aim to actualize the planning documents.

20. With some extensions (i.e. description of plant,...) the results are usable to document the effort for safety as required by some national laws.

21. Possibility to extend the analysis for later investigation. Changes can be added in the forms without requiring a lot of further documentation time.

4 Conclusion

To minimize risks starting out from chemical plants as well as to design economically it is necessary to analyse the system already in parallel to the design process. Dependent on the phase of design the requirements to carry out the safety analysis vary because of the differences of informations available. Even though HAZOP is the most appropriate method to analyse P&I-flowsheets after finishing the phase of "Definition of components structure" the severity of the disadvantages of HAZOP led us to create a modified method to analyse these kinds of system with the best possible results. The KOMB analysis is based on the essential features of HAZOP adding the following new criteria:

– showing clearly the correlations among causes, effects and places of hazards even when analysing multi-component systems;
– assessing of the proposed countermeasures in order to update the planning documents;
– easy integration of the countermeasures into the complete analysis with a minimum of effort;
– extentions can easiliy be added later on by the means of four adequate forms.

5 Literature

/1/ **Bartels, K.; Hoffmann, H.; Rossinelli, L.** 1990: Risikobegrenzung in der Chemie, PAAG-Verfahren (HAZOP), Internationale Sektion der IVSS für die Verhütung von Arbeitsunfällen und Berufskrankheiten in der chemischen Industrie, Heidelberg 1990

/2/ **BImSchG, BImSchV:** Bundesimmissionsschutzgesetz, Verordnung zum BImSchG, 1974/1990, Germany

/3/ **Bönig, S.** 1994: Konzeption einer Methode zur sicherheitsgerechten Planung und Konstruktion verfahrenstechnischer Anlagen, Diplomarbeit, TU Clausthal 1994

/4/ **Kletz, T.A.** 1992: HAZOP and HAZAN, Identifying and Assessing Process Industry Hazards, Institution of chemical engineers, Hemisphere Publishing Coporation, USA 1992

/5/ **Knowlton R.E.** 1981: An introduction to hazard and operabilities studies, The Guide Word Approach, Chemetics International, Vancouver, Canada 1981

/6/ **Kühne, G.** 1984: Anwendung von Methoden zur Erstellung von Sicherheitsanalysen- sind systematische Methoden notwendig? Sicherheitsanalyse nach der Störfall-Verordnung, Kolloquium des Instituts für Umweltschutz im TÜV Rheinland e.V., Verlag TÜV Rheinland GmbH, Köln 1984

/7/ **Kuhlmann, A.** 1981: Einführung in die Sicherheitswissenschaft,Verlag TÜV Rheinland GmbH, Köln 1984

/8/ **Merdian, J.** 1989: Methoden zum Identifizieren komplexer Risiken an Maschinen bzw. neuen Technologien, Arbeitssicherheit, April 1989

/9/ **N.N.** 1985: Beispielsammlung für Sicherheitsanalysen nach §7 Störfallverordnung, Band 1, Hrsg. Umweltbundesamt, Berlin 1985

/10/ **Ruppert, K.A.** 1990: Sicherheitsanalytische Vorgehensweise für Alt- und Neuanlagen, Chem.-Ing.-Techn. 62 (1990) Nr. 11, S.916-927

/11/ **VDI 2244**: Konstruieren sicherheitsgerechter Erzeugnisse, Beuth Verlag GmbH, Berlin 1988