21st Annual Conference of the Canadian Nuclear Society
Toronto, Ontario, Canada / June 11-14, 2000

HAZOP: A POWERFUL RISK ANALYSIS TOOL

J. Krasnodebski
Quality Consultant

Purpose

- To acquaint the audience with the origins of the Hazard and Operability Studies HAZOP technique, its basics, and application.
- To propose the use of HAZOP to examine existing designs, evaluate nuclear plant aging issues, refurbishment, and modifications, and evaluate plant operation and maintenance processes.

Introduction

Hazards and attendant risks are present in practically all human and industrial activities. In order to manage risks effectively, it is necessary to identify hazards existing in a project/system, estimate risks and control them throughout system's life. This applies to building new plants and to operating and modifying existing plants. A number of hazard identification and risk estimation techniques have been developed. Various industries choose to apply their own preferred methods, which often have to be acceptable to their regulators. One of the most versatile, powerful and effective and widely used analysis techniques is Hazard and Operability Studies - HAZOP. This technique was developed by Imperial Chemical Industries (ICI) in the UK in the seventies (Ref.1), and was initially used in the chemical and related industries. Its use spread to the chemical industry worldwide, and with time has also extended to a variety of other industries including oil and gas, food, forestry, mining, railways, etc. In recent years it has been applied in the electronic and software engineering fields.

HAZOP Principles

HAZOP is a structured, disciplined and synergistic technique for identification of hazards and operability problems and their potential solutions. The technique is based on the assumption that hazards and operability problems are caused by deviations from design intent. The design intent identifies equipment function, and is the designer's specified or desired behaviour for a system and its elements and parameters. A characteristic feature of HAZOP is the "examination session ", during which a multidisciplinary, experienced study team, under the guidance of a trained study team leader examines all relevant parts of a design of a system using selected "guide words". A guide word is a word or a phrase which expresses and defines a specific type of deviation from the design intent. Seven basic guide words are shown in Table 1. The technique aims to stimulate the imagination of team members in a systematic and creative way to identify hazards and operability problems.

TABLE 1 - HAZOP GUIDE WORDS AND THEIR GENERIC MEANINGS

GUIDE WORD	MEANING
NO or NOT	No part of intended design is achieved and nothing else happens (e.g., no flow)
MORE	Quantitative increase (e.g., higher flow)
LESS	Quantitative decrease (e.g., lower flow)
AS WELL AS	Qualitative increase (e.g., impurities in the flow)
PART OF	Qualitative decrease (e.g., one component of the mixture is missing)
REVERSE	Logical opposite to the intent (e.g., reverse flow)
OTHER THAN	Complete substitution, no part of original intent is achieved (e.g., flow of completely different material)

There are also additional guide words relating to clock time: **EARLY** and **LATE,**
and those relating to order or sequence: **BEFORE** and **AFTER.**

HAZOP Process

HAZOP studies consist of four basic sequential steps: Definition, Preparation, Examination and Documentation and Follow up. These steps and associated tasks are shown in Figure 1.

The manager who initiates the HAZOP study, should at the outset define its Objective and the Scope. The objective will depend to a great extent on the purpose for which the results of the study will be used. The Scope should define the system to be studied, its states and boundaries. The study team leader may if required, assist the manager in the above tasks. The selection of the qualified study leader, recorder and team members with knowledge and experience in the system to be examined, is critical to the success of a study. The team members should be trained in HAZOP studies procedure.

Assembly of a complete and accurate design representation is a prerequisite to success of a HAZOP examination. A design representation is a descriptive model of a system which adequately describes the system under study, its parts and elements and their characteristics/parameters. The design representation of a system being studied should:

- capture the design intent, and fully describe the system and function of each of its parts
- identify all critical elements and their characteristics whose deviations from design intent can cause hazards or operability problems
- facilitate easy understanding of the system function

The design representation may be either of the logical design or the physical design. The usual design representation used in the chemical industry is process piping and instrumentation diagrams (P&ID). They allow process to be followed, and identify implicitly function of each part and element (e.g., pipe - contains and transfers fluid, or heat exchanger - transfers heat, contains fluid). These diagrams can be augmented by other information about equipment design and materials, such as equipment specifications. Layout of the system being studied may also be required.

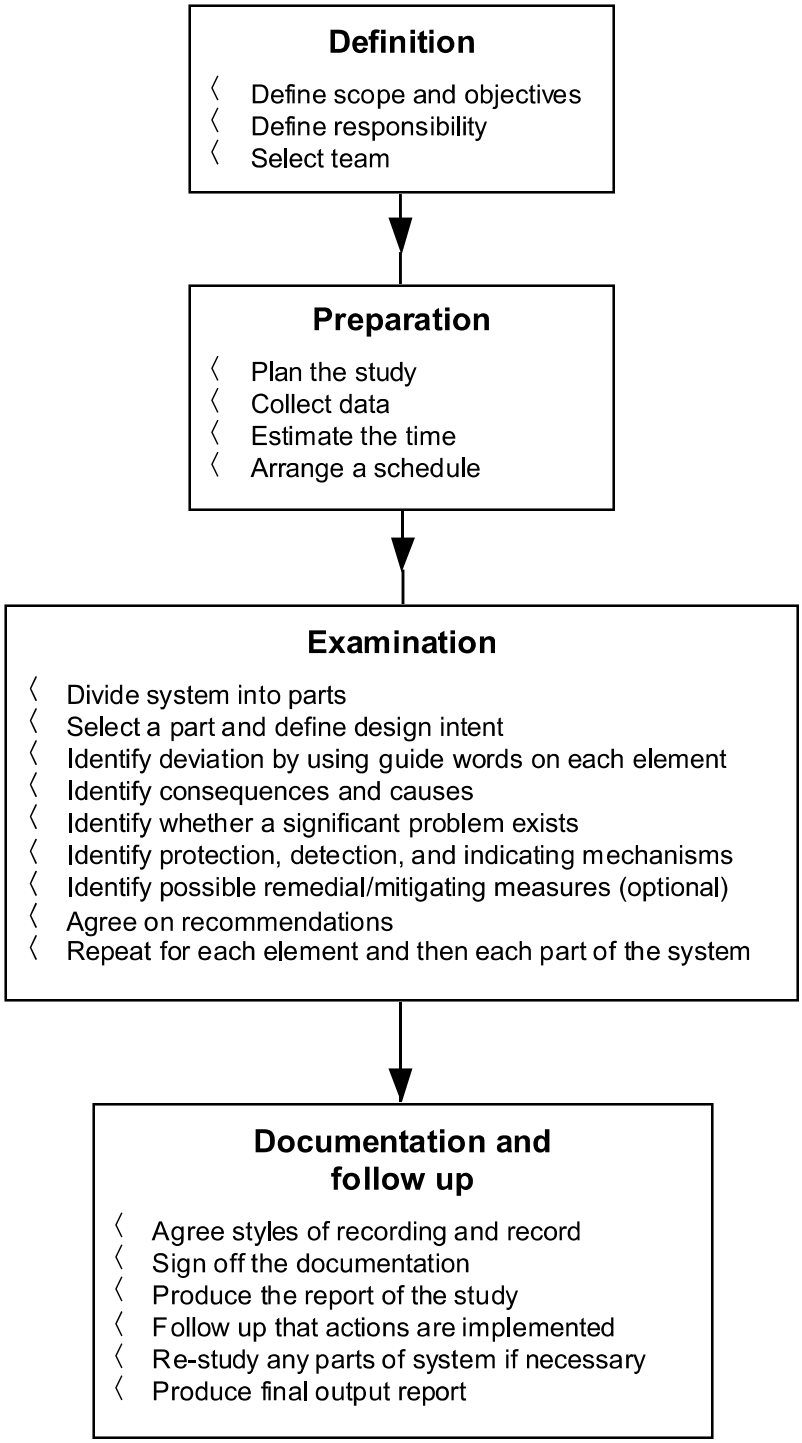
Various other types of design documentation can also be utilized as the design representation. If the design representation of one type does not cover all critical elements /characteristics of the system being studied, the design representation of different type(s) should also be used. It should be noted that if the system elements/characteristics are not included in the design representation(s) used, hazards which they may cause will not be identified. The selected design representation is divided into parts and the design intent for each part and element is defined to facilitate the HAZOP examination.

The examination is carried out, by an experienced, interdisciplinary team representing design, operation, maintenance and other functions which can contribute to the objectives of the study. At the beginning of the examination meeting, a study team leader outlines the objectives and the scope of the study, lists the design representation and reviews its division into parts and elements and their design intents. Applicable guide words and their interpretation are also reviewed. The steps in examination are as follows:

- The team leader guides the team through a structured set of questions using guide words that focus on deviations of each elements/characteristics from the design intent. These guide words stimulate individual thought and focus group discussion.
- The team looks for causes and consequences of each credible and hazardous deviation. When significant consequences – safety or economic are identified, evaluation of adequacy of safeguards is made and if additional safeguards or design changes are needed, the team makes suitable recommendations. Identified hazardous deviations can be categorized according to the severity of their consequences or in terms of relative risk ranking. To estimate risk ranking, a frequency /consequence matrix can be developed. This semi-quantitative method of risk estimation can provide useful input into decision making process.
- The procedure is then repeated for all elements and parts until the representation of the whole system has been examined.

The results of the examination are documented identifying responsibilities for follow up. The report is submitted to the project manager (decision maker) who is responsible for the resolution of identified hazards and operability problems.

Figure 1 The HAZOP Study procedure



Discussion of Hazards Analysis Techniques

There are many different techniques available for the identification of potential hazards and operability problems, ranging from Checklists, What-If Analysis, Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), to HAZOP (Ref. 4). Some techniques such as Checklists and What-If Analysis can be used early in the design when little information is available, or in later phases, if a less detailed analysis is adequate. HAZOP requires more details on the system being studied and produces more comprehensive information on both hazards and errors in system design. It can also be used in early design phase, but is most suitable in the later phases of detailed design when adequate design representation is available. It can also be used later in the lifecycle in examining operating facilities including plant modifications and plant decommissioning, etc.

An important feature of HAZOP is that the examination is performed by the designers, operators and maintainers who are thoroughly familiar with the system being examined and any recommendations made are likely to be practical and acceptable to the decision makers. HAZOP is particularly useful for identification of hazards, their causes and consequences in systems involving the flow of materials, people or data, or a number of events or activities in a planned sequence, or the procedures controlling such a sequence. HAZOP provides a method for systematically examining the interaction of people and equipment, and thus identification of human errors. It helps in identification of hidden errors in design, operating or maintenance instructions or those created by changes in existing facilities. HAZOP shortcomings are: it is time consuming and human resources intensive, identifies hazards due to a single deviation only, results are qualitative, or at best semi-quantitative.

Where the impact of multiple deviations or quantitative results are required, HAZOP is best used as a front-end analysis. The majority of the hazards identified by the HAZOP are removed, and the remaining one's can then be subjected to a Fault Free Analysis (FTA), to consider the impact of multiple deviations and allow the detailed review of sequences of failures. Not only can the FTA demonstrate the significance of various controls and safeguards, but it can help point out other ways in which the same undesired outcome can arise. As such, the two techniques are very complementary. Quantifying the fault trees adds yet another level of benefits in identifying whether or not to pursue changes in equipment, procedures, maintenance practices, etc. HAZOP being bottom up approach when used in conjunction with FTA, can also help to identify any missing branches of the trees. As mentioned before, HAZOP is particularly useful in analysis of systems involving flow, and mechanical systems.

Potential Applications for HAZOP in the Nuclear Power Industry

Different industries have their own preferred methods for hazard identification and risk analysis. In the aircraft industry, it is Functional Risk Analysis and FMEA, in the chemical industry it is HAZOP, and in the nuclear industry it is Probabilistic Risk Assessment (PRA). PRA is based on Event Tree Analysis, and Fault Tree Analysis (FTA). Event Trees identify hazardous events and event sequences. FTA uses a top down approach, starting with a undesired event and mapping its causes in a systematic manner. Development and quantification of Fault trees require careful identification of top events, a detailed understanding of plant systems, and reliable data. FTA is very time consuming. Event Trees and Fault Trees are generally performed by the analysts, who are not involved in the design or operation of a system. Application of PRA is limited to assess the magnitude of risks to the public from accidents due to operation of the nuclear generating stations and may also be used for assessment of risks resulting from toxic materials. It is limited to the safety and safety support systems. Risk Analysis does not cover any hazards which may result from operation of the balance of the plant, radioactive materials storage and transportation, or conventional personnel hazards.

The confidence in a system and personnel safety cannot be achieved effectively and efficiently by any single technique. The application of different complimentary techniques may be required. HAZOP is often used as a complementary technique to FTA.. There are several situations where HAZOP has been applied in the chemical and other industries, which would suggest parallel applications in the nuclear industry. These include:

1. Plant Modifications
   The HAZOP assessment method can be applied directly to plant modifications with particular attention being paid to how the modification will impact on the existing overall plant design configuration. The HAZOP study can be structured to examine equipment substitution or equipment improvements to ensure that no new failure mechanisms are introduced. It can also be used to examine any potential cascading effects of the design change which may not be obvious.

2. Plant Refurbishment
   It is possible to adapt HAZOP assessments to the review of the value and impact of various plant refurbishment options, in addition to the detailed review of the designs. Such an application may be useful in pointing out, or verifying, the safety benefit or potential safety issues associated with planned refurbishment work.

3. Plant Aging Issues
   HAZOP studies are suited to the identification of plant aging mechanisms and a review of their consequences.

4. Radioactive and Hazardous Materials Management
   The HAZOP method has been employed extensively in Hazardous Material management, and is one of the hazard identification and evaluation techniques listed in the U.S. Occupational Safety and Health Administration (OSHA), 29 CFR 1910.119 "Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents". It is particularly suited to review of the design of systems and processes for managing the handling, storage and transportation of radioactive and hazardous materials.

In the Canadian nuclear industry, HAZOP has been used in Chalk River Laboratories, where a number of studies have been successfully performed. Some examples of these studies are as follows (Ref. 5):

- Recycle Fuel Fabrication Facility (RFFL): A HAZOP study was conducted in support of a number of issues that resulted in modifications to the design to bring it closer to modern standards, and fuel fabrication facility refurbishment and Licensing. The study was instrumental in identifying a changes to work control philosophy and operating procedures. The study report formed an input to the safety analysis document for the facility. The report was also used as a stand alone document to demonstrate to the internal Safety Review Committee (SRC) and the external regulator (AECB) that all major hazards, had been identified and that the design was acceptable.

- Combined Electrolysis and Catalytic Exchange Upgrading and Detritiation (CECEUD) Facility: A HAZOP study was conducted on the preliminary design of this demonstration facility which was designed to upgrade and detritiate heavy water. Again the output from this study provided an input to the safety analysis report for the facility which was used to obtain construction and operating approvals and licences.

- High Active Liquid Storage Facility: A HAZOP study was conducted on an operating facility for the storage of fissile liquid waste to identify potential criticality initiating events to support a safety case to increase the concentration of fissile material in the storage tank. The study demonstrated to our internal Criticality Panel and the external regulator (AECB) that the design and operational controls were adequate to prevent a criticality event at the higher concentrations. The study also provide support that the facility was operable at the higher concentration.

- Chemical Pit Remediation Process: A HAZOP study was conducted on a process to treat ground water to remove radioactive contamination. The study resulted in a number of design and operational changes to improve the safety and operability of the system.

- New Isotope Processing Facility

HAZOP Studies have also been successfully conducted on Glace Bay and Port Hawkesbury Heavy Water Plants, and Cameco Port Hope Fuel Fabrication Facility.

In the Canadian nuclear power industry, the only known application has been to CANDU 9 Distributed Control System (DCS) at AECL Power Projects. The use of this technique at the early stage of the design was found effective in discovering potential hazard and operability problems. Results of the assessment provided valuable feedback to the system designers to improve and enhance the DCS design

Standards and References on HAZOP

The purpose of this section is to review briefly some references which provide detailed information on HAZOP and its application. This information should be particularly useful to persons who want to learn more about this technique with a view to applying it in their work.

Reference 1 is the first formal HAZOP publication (1977), describing the HAZOP technique which was developed by Knowlton and Shipley of ICI.

Reference 7 is a draft of a guide on HAZOP which is being prepared by the International Electrotechnical Commission IEC. IEC is responsible for standardization in the electrical and electronic fields, including reliability, maintainability and risk. These latter subjects are within the scope of the Technical Committee TC56 Dependability. IEC/TC56 recognized the need for general guidance in the area of risk analysis and published in 1995 an Application Guide - Risk analysis of technological systems, IEC 60300-3-9 (Ref. 6), which has since been adopted as the Canadian CSA standard. The purpose of this document is to provide guidance and ensure quality and consistency in the planning, execution and documentation of risk analyses. The guide contains risk analysis definitions, concepts, process and methods. It provides guidance to the writers of risk analysis standards in specific fields. IEC/TC56 previously produced a number of standards on reliability methods such as FMEA and FTA which are equally applicable in analyzing risk. A working group of this international committee charged with reviewing various risk analysis methods, noted that Hazard and Operability Studies(HAZOP) was the preferred risk analysis method in the chemical industry. It was also observed that HAZOP, since its inception in the early seventies, had developed in various forms, and that no recent, authoritative, generally applicable guide on this technique existed. It was therefore decided to develop a generic guide on HAZOP technique and its application, which would cover all industries. The publication IEC 61882: Guide for Hazard and Operability Studies (Ref. 7) was initiated and work is nearing completion. The guide covers; definitions, principles of HAZOP, the HAZOP study procedure, documentation and follow up. The appendix provides a number of examples on application of HAZOP in various engineering fields and HAZOP references. It is expected to be published at the end of this year and is likely to be adopted by CSA as a Canadian standard.

Reference 8, is a UK Defence standard which explains how to conduct HAZOP Studies for systems which include a programmable electronic system (PES). It can also be used as a guide to carry out a HAZOP Study of any system. “It is a detailed guide for those who need it, and a reference for experienced practitioners”.

Reference 9, which was written by the authors of the above mentioned UK Defence standard, covers the general principles of HAZOP and provides guidance on its application to software and PES, as well as descriptions of problems which were experienced and dealt with.

Computer aids, and automation of HAZOP

HAZOP is a structured, disciplined technique, the efficiency and effectiveness of which depends to a large degree on the quality of its documentation. Documentation of the process can be done manually or with assistance of the specialized computer programs. Many functions can be performed manually, however the task of manual documentation for any but a small study becomes too unwieldy.

A number of computer programs exists which are specifically designed to facilitate HAZOP studies. They vary from simple formatted sheets, which facilitate recording the results of the examination and displaying them to the team, to more comprehensive ones, which help in planning and preparation of meetings, recording the examination, documenting results and facilitating follow up. They can be used as a checklist for planning and executing HAZOP. Computer programs can also produce various reports, such as listing risks by cause or consequences, or facilitate production of risk matrices and risk ranking. Some programs contain "Knowledge based libraries" which facilitate the examination process, by acting as memory aids and supplement knowledge, experience and imagination of team members.

Good software program improves efficiency and productivity of HAZOP studies. It ensures consistency of analysis, and provides for easy access to stored information and production of reports in various required formats. Programs should be comprehensive, versatile, capable to be customized, simple to operate, and thus satisfy users requirements and needs. When shopping for a computer program, the above characteristics should be kept in mind. The software should be tested for its suitability, before a final decision is made (Ref. 10).

Computerization of HAZOP should however be limited to the actives and tasks discussed above, and should not encroach on the tasks which require intelligence, in particular on the examination process. Attempts have been made to automate the process of HAZOP examination. In this process, a computerized design representation is subjected to automatic examination using appropriate guide words. The results of this examination can then be reviewed by a study team. However, results of such a study are limited to the hazards identified in the program. The resulting study could not be considered a complete HAZOP since its main characteristic "synergistic examination by a team of experts" is missing. In short, automation of the HAZOP technique has made little headway, and is not recommended.

Conclusions and Recommendations

HAZOP is a very powerful and effective technique which has been used in many applications. Not only does it identify hazards, their causes and consequences and facilitates their mitigation, but also covers operability problems. Its application has spread to a variety of industries, and some applications in nuclear industry have been noted. Its benefits are widely reported in the technical literature. It is an accepted Safety Management System (SMS) analysis method and is approved by some jurisdictions in USA and Europe.

At the present time FTA is widely used in the nuclear industry, but is limited to safety and safety related systems. Its application is confined to assessing nuclear safety related risks FTA can be used to test different assumptions about test, inspection or maintenance intervals and thus facilitate the selection of the appropriate risk reduction and control measures. HAZOP and FTA are two complementary techniques. HAZOP can be used to identify and prioritize hazards, and only selected systems be subject to FTA. FTA coupled with a HAZOP can naturally bring analysts, designers, operators, and maintainers together to provide different information and perspective on the identified hazards. This can not only broaden the pathways of failure that are identified, but will also tend to make them reflect how things actually work rather than how they are supposed (or intended) to work. Their combination is considered by some to be the most effective way to identify, quantify and control risk (Ref. 11) .

It is time the Canadian Nuclear Industry recognized that risk analyses methods are applicable not only to nuclear safety, but also to operability problems, and non nuclear part of the plant and took a larger view at techniques which have proved their value in other fields, such as HAZOP.

References

1. "A Guide to Hazard and Operability Studies", Chemical Industries Association, London, 1977.
2. Trevor A. Kletz: "HAZOP & HAZAN, Notes on the identification and assessment of hazards", The Institution of Chemical Engineers, Rugby, UK, 1992.
3. Ellis Knowlton: "A manual of Hazard & Operability Studies, The creative identification of deviations & disturbances" Chemetics International, Vancouver, Canada, 1992.
4. "Guidelines for Hazard Evaluation Procedures, Centre for Chemical Process Safety of the American Institute of Chemical Engineers, New York, 1992.
5. Private communication between the author and T. Arthur of CRL.
6. International Electrotechnical Commission, Publication IEC60300-3-9, Dependability management-Part3: Application guide-Section:9: Risk analysis of technological systems. 1995.
7. International Electrotechnical Commission, Publication IEC 61882: "Guide for Hazard and Operability Studies HAZOP" (draft).
8. UK DEF STAN 00-58, "A guideline for HAZOP studies on systems which include a programmable electronic system", 1996.
9. Felix Redmill, Morris Chudleigh, James Catmur "System Safety: HAZOP and software HAZOP", Wiley, 1999.
10. Hyatt N., Hyatt M., Spradley J. C. "Buy PHA Software with Confidence", Hydrocarbon Processing, October 1996.
11. Henry Ozog & Lisa Bendixen "HAZARD Identification and Quantification" Chemical Engineering Progress Volume 83, No.4, pp.55-64 (April 1987).

APPENDIX- Example of HAZOP

(Adapted from Reference 7)

The purpose of this simplified example is to introduce the reader to the basics of the HAZOP examination method. The example is based on one given in the original publication on HAZOP (Ref 1).and is also included in Reference 7.

Consider a simple process plant, shown in figure A1 below. Materials A and B are continuously transferred by pump from their respective supply tanks to combine and form a product C in the reactor. Suppose that A must always be in excess of B in the reactor to avoid an explosion hazard. A full design representation would include many other details such as the effect of pressure, reaction and reactant temperature, agitation, reaction time, compatibility of pumps A&B, etc., but for the purposes of this simple illustrative example they will be ignored. The part of the plant being examined in this example is shown in bold.

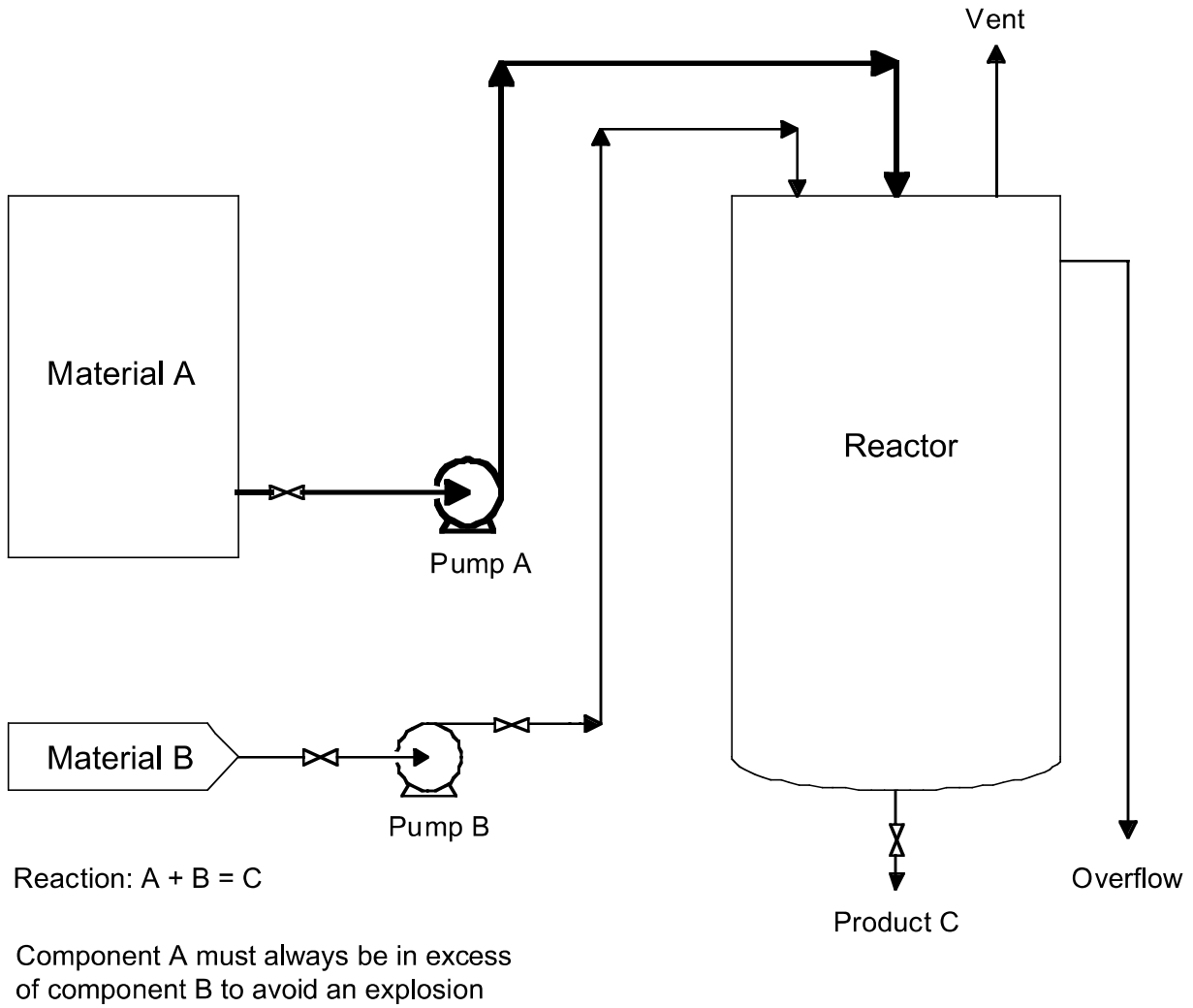


Figure A1 - Simple flow sheet

The part of the system selected for examination, is the line from the supply tank holding A to the reactor including pump A. The design intent for this part is to continuously transfer material A from the tank to the reactor at a rate greater than the transfer rate of material B. The design intent expressed in terms of input material, activity performed, source from where material is taken, and its destination is given in the following header:

Material	Activity	Source	Destination
A	Transfer (at a rate > B)	Tank for A	Reactor

Each of the guide words indicated in Table 1 (plus any others agreed, as appropriate, during the preparatory work) are then applied to each of these elements in turn and the results recorded on HAZOP worksheets. Examples of possible HAZOP outputs for the "material" and "activity" elements are indicated in the work sheets which follow, where the "by exception" style of reporting is utilised and only meaningful deviations are recorded. Having examined each of the guide words for each of the elements relevant to this part of the system, another part (say the transfer line for material B) would be selected and the process repeated. Eventually all parts of the system would be examined in this manner and the results recorded.

STUDY TITLE: PROCESS EXAMPLE **SHEET: 1**

P and ID NO: **REV. NO:**

DATE: **December 17, 1998**

TEAM COMPOSITION: LB, DH, EK, NE, MG, JK

MEETING DATE: **December 15, 1998**

PART CONSIDERED: **Transfer line from supply tank A to reactor**

DESIGN INTENT: **Material:** "A" **Activity:** "Transfer continuously at a rate greater than B"

Source: "Tank for A" **Destination:** "Reactor"

No.	Guide word	Element	Deviation	Possible causes	Consequences	Safeguards	Comments	Actions required	Action allocated to
1	No	Material A	No Material A	Supply Tank A is empty	No flow of A into reactor. Explosion	None shown	Situation not acceptable	Consider installation on tank A of a low-level alarm plus a low, low-level trip to stop pump B	MG
2	No	Transfer A (at a rate >B)	No transfer of A takes place	Pump A stopped, line blocked	Explosion	None shown	Situation not acceptable	Measurement of flow rate for material A plus a low flow alarm and a low flow which trips pump B	JK
3	More	Material A	More material A: supply tank over full	Filling of tank from tanker when insufficient capacity exists	Tank will overflow into bounded area	None shown	Note: This would have been identified during examination of the tank	Consider high-level alarm if not previously identified	EK

4	More	Transfer A	More transfer. Increased flow rate of A	Wrong size impeller. Wrong pump fitted	Possible reduction in yield. Product will contain large excess A	None		Check pump flows & characteristics during commissioning. Revise the commissioning procedure	JK
5	Less	Material A	Less A	Low level in tank	Inadequate net positive suction head. Possible vortexing and leading to an explosion. Inadequate flow	None	Unacceptable. Same as 1	Low level alarm in tank. Same as 1	MG
6	Less	Transfer A. (at rate >B)	Reduced flow rate of A	Line partially blocked, leakage, pump underperforming etc.	Explosion	None shown	Not acceptable	Same as 2	JK
7	As well as	Material A	As well as A there is other fluid material also present in the supply tank	Contaminated supply to tank	Not known	Contents of all tankers checked and analysed prior to discharge into tank	Considered acceptable	Check operating procedure	LB
8	As well as	Transfer A	As well as transferring A, something else happens such as corrosion, erosion, crystallisation or decomposition	The potential for each would need to be considered in the light of more specific details					NE

9	As well as	Destination reactor	As well as to reactor. External leaks	Line, valve or gland leaks	Environmental contamination. Possible explosion	Use of accepted piping code/ standard	Qualified acceptance	Locate flow sensor for trip as close as possible to the reactor	DH
10	Reverse	Transfer A	Reverse direction of flow. Material flows from reactor to supply tank	Pressure in reactor higher than pump discharge pressure	Back contamination of supply tank with reaction material	None shown	Position not satisfactory	Consider installing a non-return valve in the line	MG
11	Other than	Material A	Other than A Material other than A in supply tank	Wrong material in supply tank	Unknown. Would depend on material	Tanker contents identity checked and analysed prior to discharge	Position acceptable		
12	Other than	Activity transfer A	Other than transfer	Completely different activity e.g. freeze, crystallise. Explode	Unknown			Investigate possibilities and report	JK
13	Other than	Destination reactor	External leak. Nothing reaches reactor	Line fracture	Environmental contamination and possible explosion	Integrity of piping	Check piping design	Specify that proposed flow trip should have a sufficiently rapid response to prevent an explosion	MG