DATA-BASED SEMI-AUTOMATIC HAZARD IDENTIFICATION FOR MORE COMPREHENSIVE IDENTIFICATION OF HAZARDOUS SCENARIOS

A Thesis

by

SUNHWA PARK

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	M. Sam Mannan
Committee Members,	Richard Furuta
	William J. Rogers
Head of Department,	M. Nazmul Karim

August 2017

Major Subject: Safety Engineering

ABSTRACT

As chemical process plants have become more involved and complex, the likelihood of hazardous incidents has increased simultaneously. That is, the more complex a facility's systems, the more factors engineers must consider. This results in a higher likelihood of potential hazards being overlooked; thus, the possibility of incidents occurring increases.

Many companies and organizations are struggling to identify their weaknesses and reduce hazardous issues by developing hazard identification (HAZID) tools, particularly for large and complex processes. Even though a considerable number of companies merely pursue this objective to conform to government regulations, their efforts play a critical role in improving their reputations and financial profits. Therefore, the advancement of HAZID tools in the process industries has taken significant strides over the last 40 years.

Despite the substantial development of HAZID methods, traditional HAZID tools need further development because of their weaknesses in identifying possible hazards. In other words, it is evident that unintended incidents that occasionally occur in the chemical process industry require more enhanced HAZID methodologies. Therefore, this study attempts to ascertain the drawbacks of existing HAZID tools so that a new HAZID methodology, data-based semi-automatic hazard identification (DAHAZID), is proposed. Considering potential HAZID methodologies, this study seeks to identify possible scenarios with a semi-automatic and systemic approach. Based on the two traditional

HAZID tools, Hazard Operability study (HAZOP) and Failure Mode, Effects, and Criticality Analysis (FMECA), the DAHAZID method will minimize the limitations of each individual method. Additionally, rather than depending on the HAZID tools to achieve the connectivity of the process system, this study will consider connections with other new technologies in advance. Then, this method can be integrated with proper guidelines regarding process design and safety analysis. To examine its usefulness, the method will be applied to two case studies, and its outcome will be compared to the actual result, performed previously by a traditional HAZOP meeting.

Hopefully, this research can contribute to the further development of the process safety field in practice.

DEDICATION

To my husband, Hoseok Yeo,

To my parents,

To my family

To my friends

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Dr. M. Sam Mannan, for his continuous support that has encouraged me to go into the safety field. Under his competent guidance, I have experienced how to explore academic knowledge practically with people in the industry and passed this safety master program without any difficulties.

I have benefitted especially from discussing my research with Dr. Hans Pasman and Dr. William Rogers of the Mary Kay O'Connor Process Safety Center (MKOPSC). Looking back over the last two years, I acknowledge that this was an invaluable time to learn from their academic knowledge as well as their life wisdom. Another capable adviser at MKOPSC, Dr. Yan-Ru Lin, helped me to progress my research by serving as a team leader.

Additionally, those at Intergraph who helped me perform my research deserve mention. Mr. Frank Joop provided the company's software, SmartPlant P&ID, for educational purposes, and Ms. Anna Elhajj allowed me to attend their official training courses.

Finally, I want to thank my husband, Hoseok, my partner in life, who has dedicated his life to me.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a thesis committee consisting of Professor M. Sam Mannan and Dr. William Rogers of the Artie McFerrin Department of Chemical Engineering, and Professor Richard Furuta of the Department of Computer Science.

The SQL coding languages in Chapter 5 were provided by Amol Jayant Bansod, a student IT worker of the MKOPSC.

All other work conducted for the thesis was completed by the student independently.

Funding Source

Graduate study was supported by a fellowship from Texas A&M University.

NOMENCLATURE

API	American Petroleum Institute
ASME	American Society of Mechanical Engineering
BFW	Boiler Feed Water
BLHAZID	Blended Hazard Identification
BN	Bayesian Network
CAD	Computer-aided Design
CAPE	Computer-aided Process Engineer
CBR	Case-based Reasoning
CHA	CBR-based Analysis
CSB	U.S. Chemical Safety and Hazard Investigation Board
DAHAZID	Data-based Semi-automatic HAZID
DCL	Data Control Language
DDL	Data Definition Language
DML	Data Manipulation Language
FEED	Front End Engineering Design
EPC	Engineering, Procurement, and Construction
EXPERTOP	Expert System for Conducting HAZOP
FHIA	FMECA and HAZOP Integrated Analysis
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis

FPFD	Failure Probability Failure Modes
FSF	Functional Systems Framework
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HDG	HAZOP-Digraph
KFD	the Japanese Failure Knowledge Database
LDG	Layered Diagraph Model
MARS	Major Accident Report System
MOC	Management of Change
NFPA	National Fire Protection Association
OSHA	Occupational Safety & Health Administration
OptHAZOP	Optimal study procedure HAZOP
PFFM	Process Flow Failure Model Analysis
PHA	Process Hazard Analysis
PPE	Personal Protective Equipment
PSM	Process Safety Management
PSV	Pressure Safety Valve
TOPHAZOP	Tool Optimizing HAZOP
RMP	Risk Management Plan
RPN	Risk Priority Number
SFD	Safeguard Flow Diagram
SP P&ID®	SmartPlant Piping and Instrumentation Diagrams®

SQL	Structured Query Language

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Backgrounds and research directions

This section goes over the background that resulted in the motivation for enhancing a hazard identification method. The associated regulations are described initially, followed by some clues from previous process incidents.

1.1.1 Process hazard analysis and regulation

Many companies in the process industry endeavored to prevent possible hazardous events with using Hazard Identification (HAZID)[1] methods. This has been either on their own initiative so that the positive outcomes can help them obtain more commercial competitiveness, or the application is required under government regulations (CCPS, 2008).

HAZID vs. PHA

Often, engineers use the two terms, HAZID and *Process Hazard Analysis* (PHA) interchangeably. However, HAZID is one of the activities required by PHA (Seligmann, 2011). PHA originated as an official U.S term from Process Safety Management (PSM) within the Occupational Safety & Health Administration (OSHA) regulations. When PHA is performed based on the regulation guidelines, it is mandatory to provide specific documentation and follow-up recommendations to confirm its proper execution.

[1] Herein, HAZID means generally hazard identification, and does not refer to a specific tool.

Regarding the regulation of hazard identification and analysis, Appendix A shows several countries' established regulations for process safety.

The limitations of current PHA

Despite the usefulness of PHA, current PHA methods as mentioned in OSHA US Regulations (1992), have limitations. For instance, as Hendershot (2006) asserts, the regulations grant

Table 1 Classical limitations of process hazard analysis (CCPS, 2008; Seligmann, 2011)

Category	Issue	Description
Nature of the method	**Completeness**	There can never be a guarantee that all incident situations, causes, and effects have been considered
	Inscrutability	The inherent nature of some hazard analysis techniques makes the results difficult to understand and use
Nature of the analysis team	**Reproducibility**	Various aspects of hazard evaluations are sensitive to analyst assumptions; different experts, using identical information, may generate different results when analyzing the same problem
	Relevance of experience	A hazard analysis team may not have an appropriate base of experience from which to assess the significance of potential incidents.
	Subjectivity	Hazard analysts must use their judgment when extrapolating from their experience to determine whether a problem is important

the freedom to select one from among myriad PHA techniques, because employers must find the most appropriate methods for their plant. In other words, there are no clear guidelines for selecting optimum PHA techniques, which mainly depends on experience. Table 1 shows the general limitations of current PHA (CCPS, 2008; Seligmann, 2011). The first limitation, completeness, is the most dominating one, as numerous incident scenarios had not been previously recognized as possible.

1.1.2 Analysis of CSB reports[2]

As an independent federal agency, the U.S Chemical Safety and Hazard Investigation Board (CSB) has investigated incidents in the chemical industry since 1998. These exhaustive investigations are directed toward only the more serious chemical industry events. Nevertheless, the reports reveal multiple clues for identifying commonalities among process events, which is particularly pertinent for finding underlying root causes; the analysis of Baybutt (2016a) and Kaszniak (2010) represent the possible root causes of reported incidents by the CSB.

[2] Rather than HAZID, this section uses the PHA term, which has a US regulatory connotation, because this section mentions reports from the CSB, a U.S. federal agency.

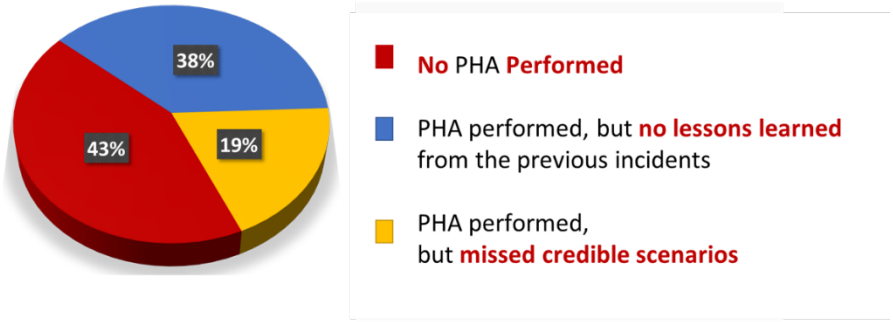


Figure 1. The analysis results of Kaszniak (2010)

Of the forty-six CSB reports published between 1998 and 2008, Kaszniak (2010) pointed out that twenty-one cases were directly associated with PHA. Figure 1 shows the distribution of the twenty-one cases concerning PHA; 43% (9 in 21) of cases fall into "No PHA performed." 38% (8 in 21) are categorized as "no lessons learned" during PHA, and 19% (4 in 21) are described as having "no credible hazard scenario at PHA". Specifically, in about 57% of incidents where a PHA had been performed before the incident, past experiences and conceivable scenarios had been overlooked. These observed data represent the perception of whether a current PHA has worked acceptably well.

Furthermore, Baybutt (2016a) stresses other common aspects of incidents reviewed by the CSB. In particular, he states that there were many failed cases of proper process designs (28%) and safeguards (56%) of the incidents. Since these insufficiencies are generally related to the initial design, the competency of design and process engineers is crucial. Additionally, necessary safeguards were not applied, so the hierarchy of process control,

shown in Figure 2, was not applied effectively. Hence, the analysis of Baybutt (2016a) provides suggestions for a more reliable control system.

Baybutt (2015b) analysed the types of failures and flaws of the primary PHA tool, the hazard and operability study (HAZOP), probably the most often applied HAZID tool in the worldwide chemical industry. One of the many causes of flaws is that in the HAZOP procedure deviation of a process variable is selected first, then in a backward direction is sought for the cause or causes, and subsequently in a forward direction shall be determined in what consequence it will result. In human thinking, however, one tends to start with a cause and then look for following effects. He also summarized competence requirements that are demanded of team members conducting a HAZOP (Baybutt, 2015a).

Figure 2. Hierarchy of safeguards Baybutt (2016a)[3]

[3] Baybutt (2016a) describes a hierarchy of safeguards as seven criteria, including an additional category, 'segregation and separation', filling the space between inherently safer design and passive safeguards. However, we did not include this category in Figure 2, because it has overlapping aspects with other

1.2 Research objectives

1.2.1 Attempt to achieve an enhanced HAZID tool

To achieve a useful HAZID tool, this research proposes a new methodology for more systematic and semi-automated approaches. Rather than focusing on the specific parts of a system, a holistic system analysis is expected to have the strength of identifying the actual root causes and consequences of incidents. Furthermore, with a comprehensive view, process safety management can suggest ideal guidelines to their employees so that the likelihood of possible incidents will be decreased. Furthermore, during a HAZOP meeting, there are too many repetitive tasks, which is tedious for participants and makes them less aware of possible scenarios that require more intensive attention. To minimize repletion and encourage involvement, this study seeks a semi-automated approach with more effective use of HAZID time and more focused attention to critical points.

1.2.2 Practical guidelines

As shown in Figure 2, process design and engineering with respect to plant and safeguards play the most fundamental roles in avoiding adverse events, which can have impacts on process safety (Baybutt, 2016b). This study pursues a more practical method to help process engineers with process safety designs, even at the initial design stage. Therefore, a new tool is expected to help to create an inherently safer design with passive and active design safeguards.

---

categories and some experts assert even that inherently safer design incorporates the meaning of segregation and separation.

1.2.3 The application of cutting-edge techniques

Currently, new technologies facilitate the development of safety techniques. To date, new technologies developed by other disciplines have mainly supported chemical plant control or optimization through, for example, automation and simulation programs. However, it is time to apply several cutting-edge technologies designed to enhance safety of the process industry. For instance, the commercialized process package, SmartPlant Piping and Instrument Diagram® (SP P&ID®) can be applied for better results in the context of safety considerations, whereas its primary application is for effective design efforts. Additionally, this study will briefly employ other computer science and statistics methods and tools, to deal with empirical data for a new HAZID tool.

1.3 Structure of this thesis

In this study, each chapter is organized and described briefly as follows:

Chapter 2: Literature Review and Basic Concepts

Prior to introducing a novel HAZID tool, it is crucial to recognize the traditional methodologies and state-of-the-art ones, which have both contributed to the development of a novel method. Following the classical ones including HAZOP and FMECA, particularly taking into account their strengths and weaknesses, current enhanced attempts are examined, such as methods that integrate methods related to HAZOP and FME(C)A, and semi-automated HAZOP. Then, brief explanations will be given for data mining and Bayesian Network (BN). Since both data mining and BN can support proper data

management, they are introduced to be assist with reader comprehension. Finally, contributors to previous incidents in the chemical plants will be analyzed.

Chapter 3: The Concepts of Data-based Semi-Automatic Hazard Identification

The main concepts of the Data-based semi-Automatic HAZID (DAHAZID) are introduced in this chapter. In light of the information in Chapter 2, the proposed DAHAZID analysis attempts to incorporate multiple factors, from obtaining data to suggesting user-friendly, viable worksheets and safeguards. With the proper combination of these factors, DAHZID pursues more comprehensive and practical ways. In particular, this method attempts to utilize cutting-edge tools, SP P&ID® and SQL, so it suggests a new possibility for the current HAZID tools. To help understand which steps should be required for the new method, which has a prepopulated worksheet, the last section provides an overview of the new method with an overall workflow.

Chapter 4: A Simple Application With The New HAZID

Prior to conducting an actual case study, this chapter illustrates a simple example, grounded in the DAHAZID methodology. Even though data from SQL and SP P&ID® is not utilized, this chapter provides the insights for this new method by performing a simple case study that might be encountered in the initial design stage.

Chapter 5: Boiler Feed Water System Case Study

This chapter sheds light on the usefulness of the DAHAZID method by dealing with an actual process system and its data. By comparing current safety control systems in the actualized process, this chapter serves to highlight the potential of this new semi-automated tool for the following purposes: a detailed engineering stage, periodic PHA, or Management of Change (MOC). At the end of this case study, there will be a comparison between the DAHAZID analysis and a generic HAZOP study, including their processes and outcomes. Based on this comparison, several future works will be suggested in Chapter 6.

Chapter 6: Conclusions and Future work

This chapter offers the conclusion of this research. The characteristic in the DAHAZID methodology is elucidated, mainly with the "trade-off between sophistication and simplicity" issue in the new method. Additionally, this chapter allows for the possibilities of the DAHAZID, followed by future work and contributions in the current HAZID field.

2. BASIC CONCEPTS FROM LITERATURE REVIEW

Chapter 1 outlined the direction of this thesis and suggested the three main goals of this research. This chapter presents an informative background from which to develop a novel HAZID tool. It begins with classical representative HAZID methods followed by advanced current methods and other relevant information.

2.1 Classic HAZID methodologies

For decades, many hazard identification methodologies have been developed and proposed to avoid unintentional events throughout industry. Of the following eight methods, because of their relevance to this research, Hazard and Operability study (HAZOP) and Failure Mode, Effects and Criticality Analysis (FMECA) will be examined in more detail.

2.1.1 Hazard and Operability study (HAZOP)

Introduction of HAZOP

Since the 1970s[4]', HAZOP has been the most applied process hazard analysis method in the process industry (Pasman, 2015). The purpose of this analysis is to identify possible deviations from design intents, as these process deviations might cause undesired events (e.g., injuries, fatalities, and catastrophes). Since HAZOP was introduced, the major working progress of the method has been maintained: under a facilitator's guidance, a

[4] A brief history of HAZOP is presented in Appendix C.1

group of engineers collaborates to identify hazard, develop associated potential failure scenarios, and suggest potential safeguards. Appendix C.2 illustrates a generic example of a HAZOP study.

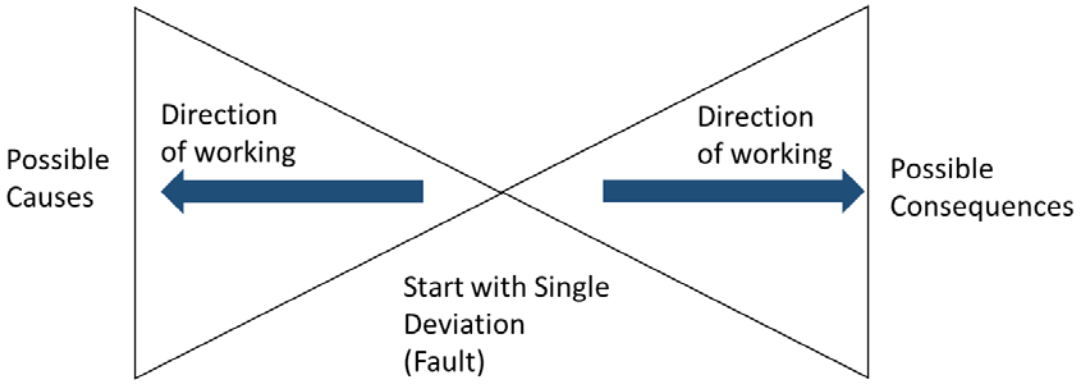


Figure 3. HAZOP progress direction[5] (Redmill, Chudleigh, & Catmur, 1999)

According to Knowlton (1987), one of the greatest strengths of a HAZOP study is its relatively systematic structure (McKelvey, 1988) compared to other conventional analysis tools. For example, Figure 3 shows the structure of a HAZOP study consisting of a start point and working flows. Firstly, HAZID-engineers undertake this analysis with one single deviation, which is made by combining each process variable and guideword (shown in Table 8 in Chapter 3). After selecting a single deviation, engineers identify

[5] This figure will be used to develop the concept of a new method in Chapter 3.

possible causes and consequences. Ideally, all deviations should be applied to simulate all conceivable causes and consequences. Additionally, a HAZOP study requires discussion among participants (typically experts in individual fields, such as processes, piping, mechanics, safety, instruments, and operation), so this working process[6] can lead to more reliable results.

Regarding the detailed properties of HAZOP, considerable work has been done, as shown in Appendix C.3.

Limitations of HAZOP

Despite its significant strengths, a HAZOP study suffers from several major drawbacks. First, the "deviation" that is a key application in HAZOP conversely generates inefficient processes and outcomes (Baybutt, 2015b), as shown in Table 2. Namely, many issues in a HAZOP study tend to arise due to the deviation, designed to identify possible hazardous scenarios systematically. Second, a HAZOP study fails to suggest or review proper safeguards thoroughly and consistently. Because the method heavily depends on the knowledge or experience of its team members, it is hard to cover all needed safeguards after identifying all possible scenarios within a limited time. Third, a HAZOP study does not cover the intrinsic mechanical issues, such as straight mechanical failures, suitability of materials (Duguid, 1999), and pump sizing (Taylor, 2007). Moreover, this analysis

[6] A generic HAZOP procedure is shown in Appendix C.2

mainly focuses on the normal process phase except for abnormal cases, such as start-up and shut-down (Taylor, 2007). Consequently, critical points related to these abnormal situations can be overlooked under a HAZOP guideline. Additionally, a HAZOP study cannot deal with a plant layout. Rather than during the meeting, consequence modeling is conducted separately, so with respect to its scenarios or consequences, process engineers might have less concern about this issue, and it is not easy to connect with other possible causes such as domino effects. Finally, as the fundamental limitation related to human beings, this analysis requires participants more than their abilities (McKelvey, 1988). Under the guidance of a facilitator, people must be familiar with the design intents of the process concerned and the principles of HAZOP before the HAZOP meeting. They also must overcome problems, such as miscommunication, labor-intensive circumstances, lack of knowledge of the possible scenarios, etc. For these reasons, it is noted that a HAZOP study is not a complete method to prevent potential incidents even though it has contributed to the process industry for decades.

Table 2. Limitations associated with "deviation" in a HAZOP study

No	Reason
1	Difficulty of producing deviations
2	Requirement of counterintuitive reasoning
3	Unclear meaning of deviations
4	Absence of an actual case (e.g., multiple deviations might be reviewed simultaneously, but the general principle of HAZOP demands the review of an individual deviation)
5	Repeated deviations and scenarios
6	Lack of propagations
7	Labor-intensive process due to a wide range of deviations → Need to review more significant deviations thoroughly (e.g., low-probability major-consequence hazards)

2.1.2 Failure Mode and Effects Analysis (FMEA)

Introduction of FMEA

In the mid-1960s, FMEA was proposed by NASA for reliability in the aerospace industry (Mikulak, McDermott, & Beauregard, 2008). The objective of the FMEA analysis is to prevent failure modes in a system ahead of time after identifying possible failure modes and their effects (Mikulak *et al.*, 2008; Redmill *et al.*, 1999). In particular, FMEA focuses on how individual equipment can fail, so it starts with the failure modes of a piece of equipment (expressed here as a single cause) in a system, as shown in Figure 4. With the possible failure modes, the FMEA team examines the following consequences for a

system, personnel, and the public. Because there are various possible failure modes and consequences, this method requires a database compiled through previous experiences or brainstorming from expert knowledge.

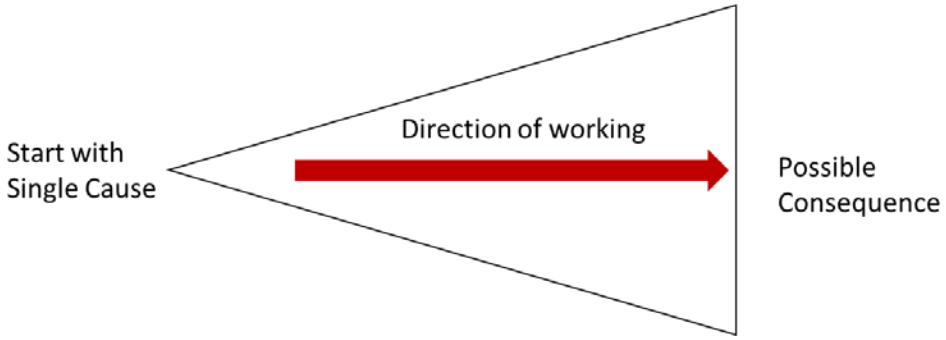


Figure 4. FMECA progress direction[7] (Redmill et al., 1999)

Failure Mode, Effects, and Criticality Analysis (FMECA)

This research separates the two terms, FMEA and FMECA, even though some works use them interchangeably. As a qualitative method, FMEA concerns itself with capturing reliable, trustworthy data (Goodson, 2016), whereas as an extension method of FMEA, FMECA quantitatively pursues a relative ranking to prioritize potential failure modes for actions (Mikulak *et al*., 2008). Table 3 shows an example procedure of the FMECA.

[7] This figure will be used to develop the concept of a new method in Chapter 3.

Table 3. Example procedure of FMECA (Mikulak *et al.*, 2008)

Step	Required Action
1	Review the process or product
2	Identify possible failure modes
3	List possible consequence for individual failure mode
4	Assign a severity ranking for each effect
5	Assign an occurrence ranking for each failure mode
6	Assign a detection ranking for each failure mode and/or effect
7	Calculate the risk priority number for each effect
8	Prioritize the failure modes for action
9	Take action to eliminate or reduce the high-risk failure mode
10	Calculate the resulting RPN as the failure modes are reduced or eliminated

In FMECA, the concept of the Risk Priority Number (RPN) is designed to prioritize equipment failure modes to demonstrate the relative ranking of required actions (Mikulak *et al.*, 2008). Consequently, we can focus on the more important events by eliminating rather trivial cases. The following equation shows a generic calculation used to obtain the RPN.

$$Risk\ Priority\ Number = Severity\ (S) \times Occurrence\ (O) \times Detection\ (D)$$

Equation 1. Generic RPN formulation

In decision making, the results of Eq.1 enable FMECA teams to reach a consensus, although determining for consequence Severity, probability of Occurrence, and probability of Detection can be challenging.

Limitations of FME(C)A

The FMECA functions to examine data exhaustively item by item, rather than seeking a broad point of view. However, this method is unsuitable for a process system, because a FMECA analysis seeks to identify the intrinsic potential of an individual piece of equipment. Moreover, the analysis demands reliable and numerous data, which requires accumulating information over a considerable period (performing accurate analyses, observations, and judgments of each equipment reliability or failure modes). Thus, it is essential to establish a reliable database for proper decision making in an FMECA.

2.1.3 Checklist

The primary purpose of checklists is to ensure a consensus standard with practice (CCPS, 2008; Redmill *et al*., 1999). The arranged list facilitates hazard identification processes, so this method is employed for all process stages. Redmill *et al.* (1999) argued that using a checklist is the most effective method concerning well-defined process systems. In some cases, the checklist method is applied with other HAZID methodologies (e.g., what-

if/checklist or a hybrid approach with other human evaluation tools) to improve efficiency. The major limitation of this method is that checklist analysts are biased by checklists and can fail to cover outside the prepared checklists. For this reason, the practice standards require further development.

2.1.4 What-if

To uncover possible causes and consequences of incidents, this analysis involves continually asking questions starting with “What-if” in a brainstorming approach (CCPS, 2008; EPA, 2008). This unstructured approach has both strengths and weaknesses. Simply, the what-if method encourages engineers to ask and answer various questions at any stage in a project. By answering the questions, the HAZID team can find possible hazards and suggest relevant solutions during this process. However, the results of this method are mainly dependent on the experience and knowledge of the engineers/analysts.

2.1.5 Fault Tree Analysis (FTA)

In a deductive manner (backward thinking), an FTA enables the investigation of possible scenarios in which hazards result in incidents (Crowl & Louvar, 2001). Starting from a well-defined incident (or top event), this analysis requires examining possible causes of the incident backward to base events for which failure data are available. Afterward, the expected scenario is visualized as a fault tree diagram. After developing a complete fault tree, analysts recommend possible safety control systems to prevent the incident. With this method, it is easy to understand the causality of incidents with a visualized fault tree and

to calculate the possibility of incidents quantitatively (even though it can be hard to obtain accurate probability values for base failure events).

2.1.6 Event Tree Analysis (ETA)

In an inductive manner (straightforward thinking), an ETA starts with an incident, the top event in the FTA, and investigates its possible ultimate outcomes (Crowl & Louvar, 2001). This method also graphically represents possible scenarios (with probability estimates), so it is easy to recognize final results. Therefore, this method is applied to prepare responsible actions in advance for potential incidents (CCPS, 2008).

2.1.7 Bowtie analysis

Utilizing prepared ETA and ETA outcomes, a bowtie graph is established to visualize overall scenarios, from actual initial base failure cases to final outcome results, for any incident. Thus, this bowtie consists of the two analysis tools, FTA and ETA, as shown in Figure 5. This figure of a generic bowtie shows possible scenarios from FTA and ETA and barriers to the risk management system (Swuste, Theunissen, Schmitz, Reniers, & Blokland, 2016).

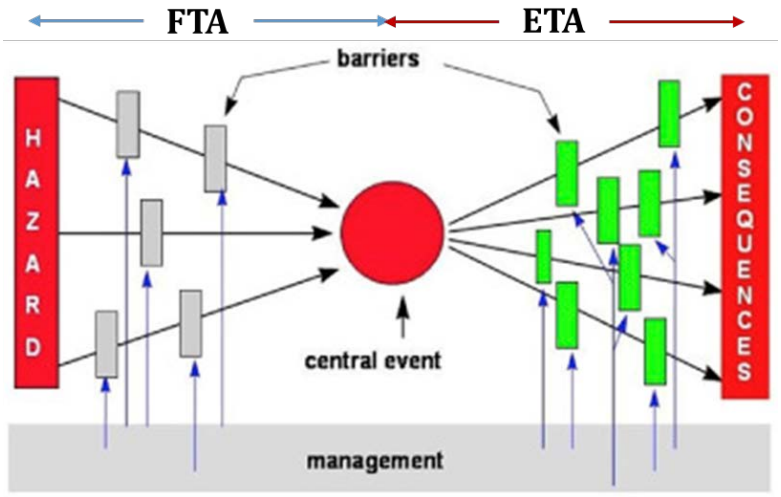


Figure 5. Bowtie metaphor including FTA and ETA (Swuste *et al.*, 2016)

2.1.8 Human Reliability Analysis (HRA)

A Human Reliability Analysis (HRA) evaluates reliabilities associated with human performance (e.g., operation, maintenance) in chemical plants (CCPS, 2008). This analysis examines the performance with several activity types: human activities particularly related to safety issues, categorization of human skills or knowledge, safety culture in a company, and environmental factors that increase human error. Because human errors are not independent factors, in general, it is suggested that an HRA should be performed with other hazard evaluation tools. In addition, quantifying human errors with limited and uncertain data that is highly dependent on conditions and other factors is challenging.

2.2 Integrated HAZOP and FMEA

The ultimate goal of any hazard identification tool is to uncover possible incident scenarios to prevent or reduce the likelihood of adverse events. However, Redmill *et al*. (1999) pointed out that there is no perfect technique or tool that can identify all possible hazards, so combinations of two or more methods should be used to produce more effective results. One of the standard combinations is HAZOP and FMEA. Even though some people mistakenly consider HAZOP and FMEA similar alternatives, HAZOP and FMEA take different approaches and therefore complement each other. Hence, three hybrid methods will be examined in order to develop the next step.

2.2.1 Blended Hazard Identification (BLHAZID)

Based on a system approach, Functional Systems Framework (FSF), Seligmann (2011) and Seligmann *et al.* (2012) developed an efficient integrated methodology called Blended Hazard Identification (BLHAZID). They proposed blending the results of two HAZID tools: HAZOP and FMEA. Their heavily computerized method applies a structured language that enables the implementation of a system approach, since it has a broad range of coverage and holds causality knowledge in triplets. Figure 6 describes the overall concept of the BLHAZID analysis with the FSF notion that draws the structure–function–goal relationships in chemical plants. First, the structure consists of two parts:

components[8] (Plant, People, and Procedures) and streams (of information, materials, signals reading control systems, and communication among people). Second, the function herein is made up of a set of capabilities, and it used to connect the foregoing structures for a system goal. Finally, there is a discussion of how to express the process system goal in a system.

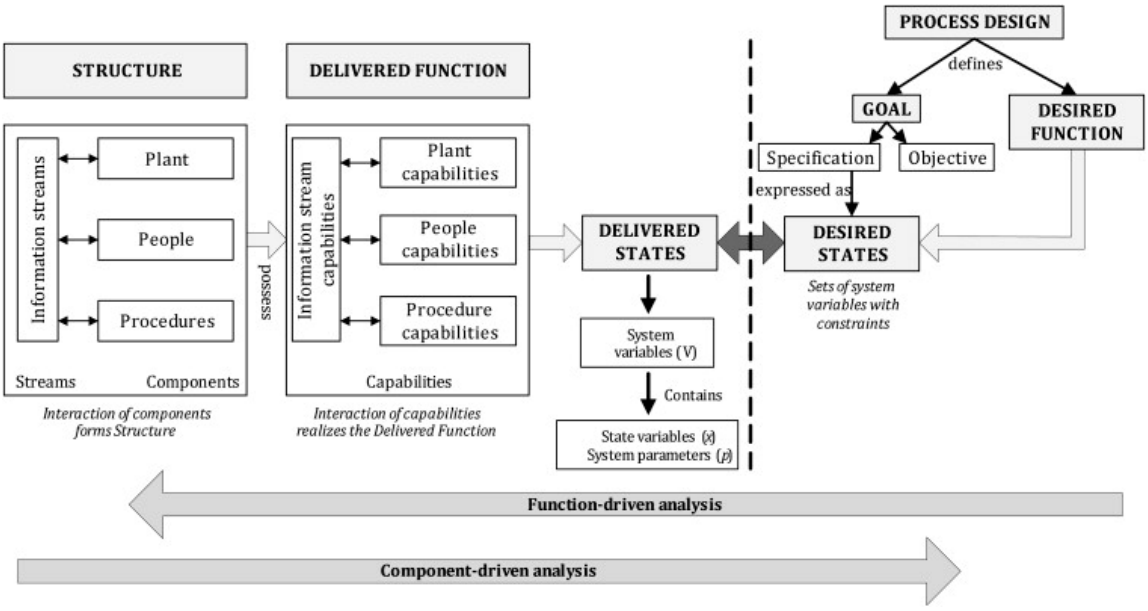


Figure 6. HAZID methods viewed in the FSF (Seligmann *et al*., 2012)

[8] As factors that can cause the failure of a system, the three components, Plant, People, and Procedures (P^3), were introduced by I.T Cameron, Seligmann, Hangos, Lakner, and Németh (2007), but only the plant aspect was dealt with by Seligmann (2011).

Moreover, the two different approaches, HAZOP and FMEA, are described as function-driven analysis and component-driven analysis, respectively, at the bottom of the figure. HAZOP seeks to identify possible deviations grounded in process design intents, and FMEA serves to identify possible component failure modes. That is, there are complementary and overlapping spaces, as shown in Figure 6.

According to Seligmann *et al.* (2012), the outcomes of BLHAZID have a broad range of coverage with detailed causality knowledge of a system by means of structured languages. Associated with all FSF entities in a system, these structure languages[9] were developed to capture more causality of hazards effectively and consistently. Hence, the results of this method might be applied to subsequent tasks, such as training and diagnosis of faults. Because the handling of all structured languages is complex, an inference engine was also generated. Németh *et al.* (2011) proposed visualized causal approaches using the structure languages.

2.2.2 Process Flow Failure Modes Analysis (PFFM)

The work of Ego and MacGregor (2004) and MacGregor (2013) introduced a new methodology, Process Flow Failure Modes (PFFM) Analysis, which, in terms of its character, lies between HAZOP and FMEA. As the name implies, the aim of PFFM is to

[9] BLHAZID has three types of structure languages: general process system, process-specific knowledge, and BLHAZID-generated knowledge. In particular, the general process system is similar to the HAZOPExpert tool of Vaidhyanathan, Venkatasubramanian, and Dyke (1996), which will be explained in Subsection 2.3.2.

maximize the guide variable of the process flow, because the way of thinking is similar to the reasoning of operating personnel (Ego & MacGregor, 2004). MacGregor (2016) claimed that PFFM is a more efficient and straightforward method than a HAZOP study, as it encourages participants to be more active during PHA meetings. PFFM can increase the completeness of scenario identification significantly. In case studies, more than a doubling of the number of scenarios compared with HAZOP has been demonstrated. PFFM modified a P&ID and PFD into a more effective process diagram, the so-called Safeguard Flow Diagram (SFD), including safety control systems from the PFD but deleting irrelevant figures from the P&ID. With the SFD, the team can minimize errors, because it is relatively easy to interpret the process of a diagram that indicates different colors. The method also makes use of a unique list composed of various failure modes regarding process equipment accumulated over the years.

2.2.3 FMECA and HAZOP Integrated Analysis (FHIA)

The study of Giardina and Morale (2015) suggested FMECA and HAZOP integrated as an analysis, FHIA. By means of the RPN in an FMECA analysis, FHIA allows the ranking of both human errors and component failures. According to Giardina and Morale, it should be noted that this method incorporates human error into the incident occurrence parameter in Table 4 for an enhanced RPN. This is needed, because it was difficult for the traditional RPN to recognize correlations of incidents and dependencies among equipment and human errors (Giardina, Castiglia, & Tomarchio, 2014). Moreover, it was useful to apply

HAZOP aspects to identify incident scenarios with the cause–deviation–consequence logical structure.

Table 4. FMECA scale for the probability of component failures and human errors (Giardina & Morale, 2015)

Component failure occurrence probability (operating day)		Human error occurrence probability	Rank
Unlikely, unreasonable to expect failure to occur	<1:20,000	Less than every 5 years	1
Low failure rate	1:20,000	In 3–5 years,	2
	1:10,000	In 1–3 years	3
Occasional failures	1:2000	Per year	4
	1:1000	In 6 months	5
	1:200	In 3 months	6
Repeated failures	1:100	Per month	7
	1:20	Per week	8
Inevitable failure, almost certain to cause problems	1:10	Every few days	9
	1:02	Per day	10

2.3 HAZOP automation attempts

Given that this thesis attempts a new semi-automatic hazard analysis, this section reviews the overall history of automatic HAZID methods. It is noted that each automatic tool has developed to supplement previous versions, such as by making more user-friendly conditions and handling a broader range of processes. Therefore, the transitional overview of automated HAZID methods will be a worthwhile step toward the proposal of a new approach.

2.3.1 Faisal I. Khan and S.A. Abbasi *et al.* (1995-2009)

As HAZEXPT (F.I Khan & Abbasi, 1995) is the initial step of their models, Khan and his coworkers made progress toward a more enhanced semi-automated HAZOP, as presented in Figure 7. The authors proposed a HAZOP knowledge-base that consists of "process-specific" and "process-general" components for hazard identification in HAZEXPT (Faisal I Khan & Abbasi, 1997a). Based on the HAZOP knowledge-base, an optimal study procedure HAZOP (OptHAZOP) and Tool for optimizing HAZOP (TOPHAZOP) were developed in order (Faisal I Khan & Abbasi, 1997a, 1997b). OptHAZOP attempted to eliminate repetitive tasks in a semi-automated HAZOP study, whereas TOPHAZOP sought a more enhanced systematic structure that incorporates 1) knowledge-base, 2) inference engine, and 3) user interface. Notably, OptHAZOP focuses on generating process deviations efficiently by using the interaction between process-general and specific aspects within knowledge-base. Faisal I Khan and Abbasi (2000) stressed that Expert system for conducting HAZOP (EXPERTOP) contains more knowledge (e.g., seven different operations commonly occurred in the chemical process plants) and EXPERTOP also has a graphical user interface that enables a user-friendly environment. Finally, Rahman, Khan, Veitch, and Amyotte (2009) developed ExpHAZOP+ that incorporates "fault propagation algorithm" to identify downstream causes and consequences from the recognized upstream events.

2.3.2 Venkat Venkatasubramanian *et al.* (1990-2005)

Venkatasubramanian and his coworkers progressed more viable HAZOP semi-automation, as shown in Figure 8. Similarly, they undertook a task to reduce repetitive tasks required in a HAZOP meeting and established a knowledge-based framework (generic and specific knowledge) at the beginning. Additionally, Venkatasubramanian and Vaidhyanathan (1994) considered in HAZOPExpert propagation cases due to deviation of a chemical process variable. Then, Vaidhyanathan and Venkatasubramanian (1995) developed HAZOP-Digraph (HDG) model with two main reasons: 1) to provide a graphical infrastructure that represents causality for a user-friendly environment; 2) to identify the abnormal causes and consequences that should be added into the diagraph of HDG. Subsequently, a semi-quantitative approach that filters and ranks HAZOP results in the HDG was proposed, which led to reduction of almost half of the unrealistic scenarios of the previous step (Vaidhyanathan & Venkatasubramanian, 1996b). Based on the case study of a batch process, Srinivasan and Venkatasubramanian (1998) established Bath ExpertHAZOP with Petri Net that represents tasks in terms of procedural and time-intervals. Finally, a newly developed software, PHASuite was designed primarily with four parts: information sharing, representation, knowledge base, and reasoning engine. Furthermore, the notion of "ontology" (as a philosophy origin, Artificial intelligence borrows this concept to take account into the subject of existence) was employed to share process information and its results with other systems (C. Zhao, Bhushan, & Venkatasubramanian, 2005a, 2005b).

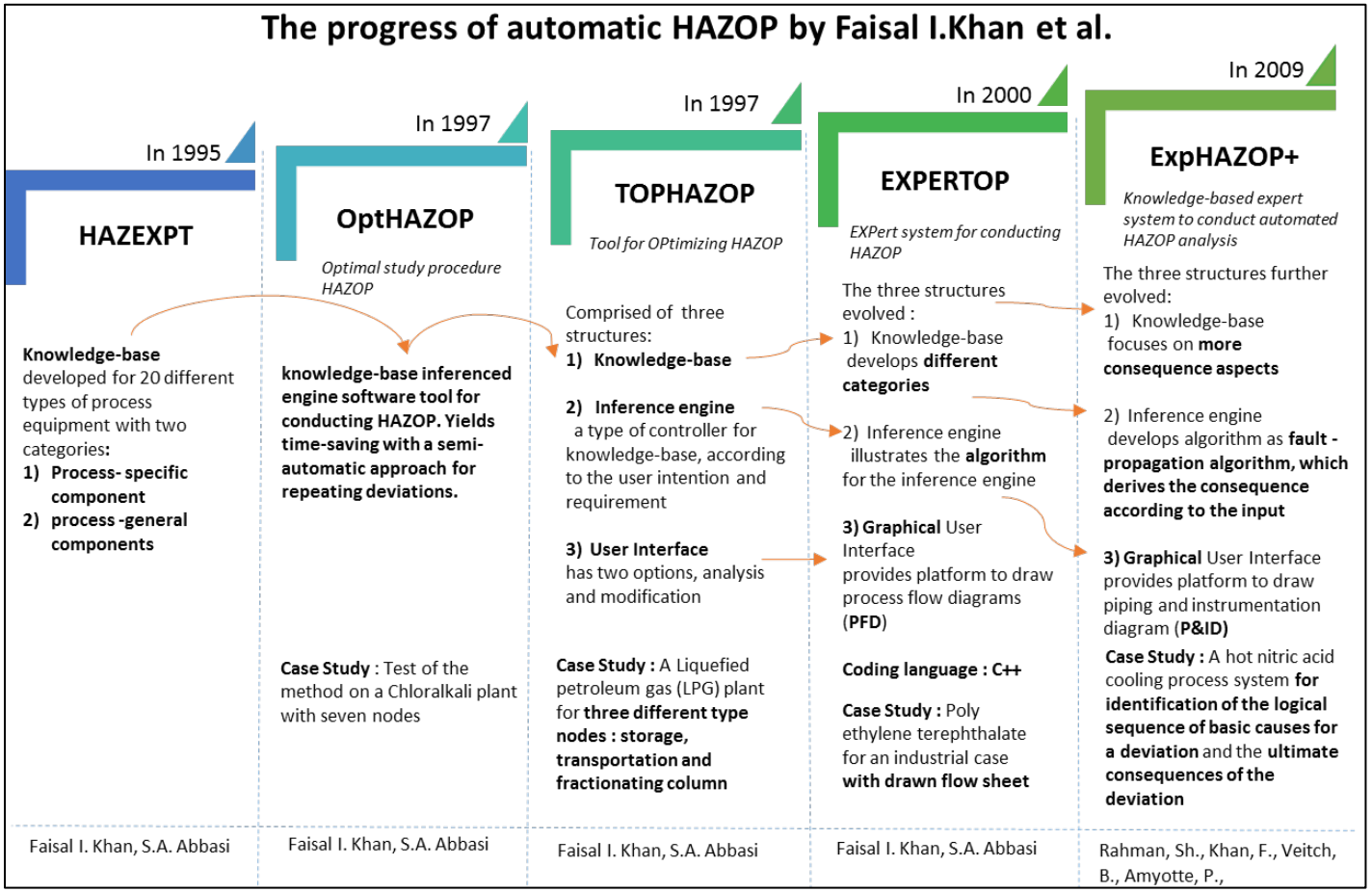


Figure 7. The semi-automated HAZOP progress by Faisal I.Khan *et al.* (Ian T. Cameron *et al.*, 2017)

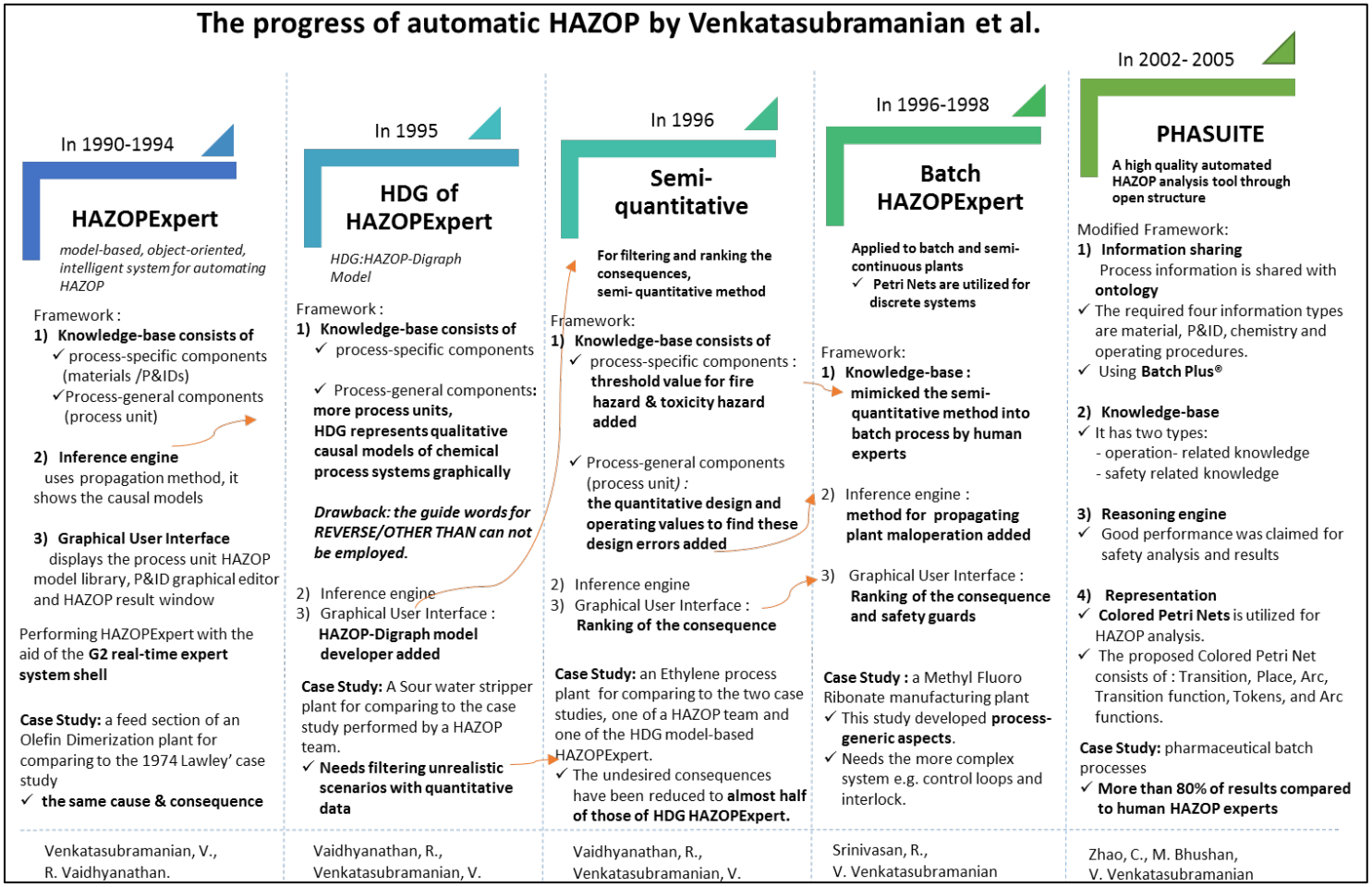


Figure 8. The semi-automated HAZOP progress by V. Venkatasubramanian *et al.* (Ian T. Cameron *et al.*, 2017)

2.3.3 STOPHAZ project (1999-2000) [McCoy *et al.*, 1999; McCoy *et al.*, 2000]

The Layered Digraph Model (LDG) was proposed by Cui, Zhao, Qiu, and Chen (2008). As an extension of "non-routine HAZOP analysis" (Vaidhyanathan & Venkatasubramanian, 1996a, 1996b), LDG HAZOP attempts to show all guide words and their interactions with three-dimensional modeling; the deviations in the "parent" node (of LDG) function to direct the deviations in a "child" node within one workspace. Moreover, it is presumably possible to connect with other workspaces. For this reason, the authors claim that LDG identifies more scenarios than a conventional HAZOP study. Additionally, Cui, Zhao, and Zhang (2010) utilized SP P&ID® to improve the efficiency of the LDG HAZOP after extracting process data automatically. Afterward, the same group developed CBR-based Analysis(CHA) (J. Zhao, Cui, Zhao, Qiu, & Chen, 2009), which is an expert system by learning Case-based Reasoning (CBR). The method employs the idea of ontology identically with the approach of PHASuite, so it attempted to have the human ability to reason. For example, a new problem is judged by a similarity algorithm based on built-in indexes. For this development, the authors borrowed the concept of computer-aided process engineering (CAPE) to have a more organized structure (e.g., problem/situation, solution, and outcome description).

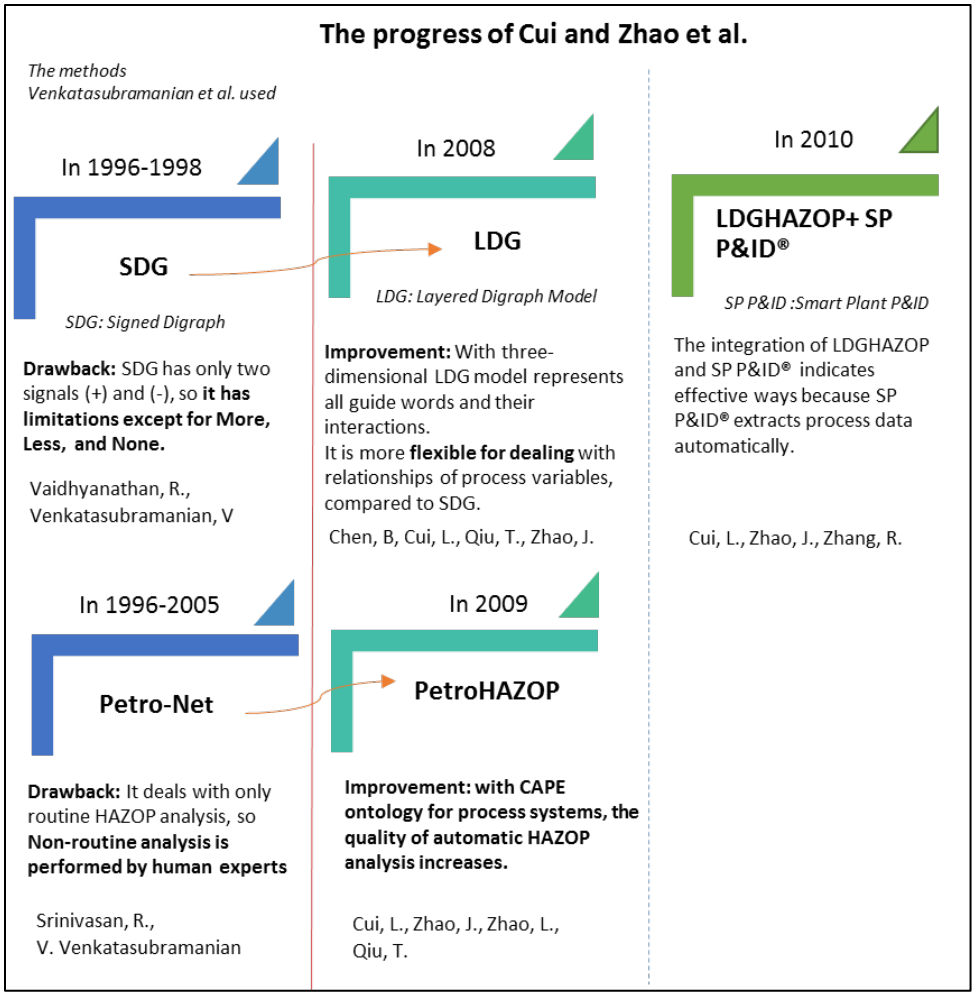


Figure 9. The semi-automated HAZOP progress by Cui and Zhao *et al.* (Ian T. Cameron *et al.*, 2017)

2.4 Data management

2.4.1 Introduction of data mining

As previously mentioned, it is essential to manage the amount of information, since the process industry has become complex. For this reason, we cannot merely rely on unaided human brains to deal with the current complex situations. In other words, we are living in the information age. In order to judge wisely in this modern world, it is crucial, even for the process and safety domains, to process interdisciplinary tasks within the computer science domain.

Of the various computer science fields, data mining can contribute to solving issues associated with the process and safety industry. The data mining process involves discovering precious knowledge from numerous data sources (Han, Pei, & Kamber, 2011); enabling people to reveal useable relationships and patterns from original data (Sumathi & Sivanandam, 2006), with the mechanism shown in Figure 10. It is therefore probable, that data mining capability will reveal hidden process relationships.

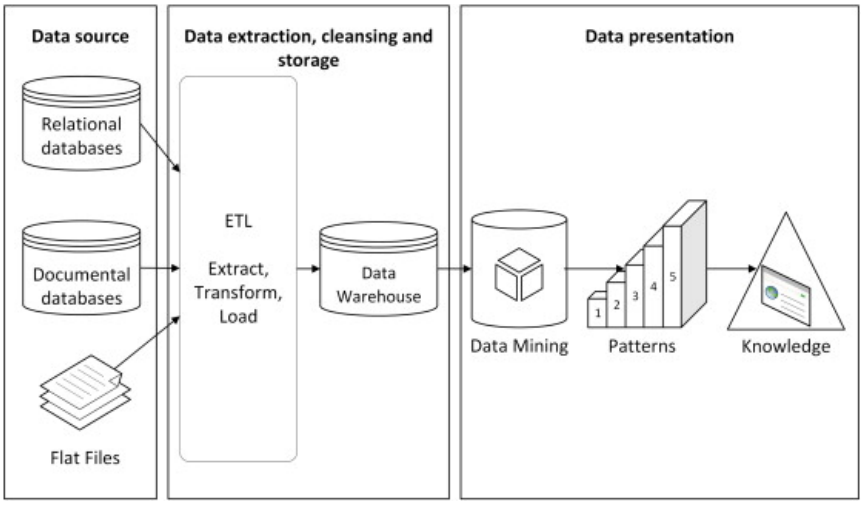


Figure 10. Typical data mining process (Han *et al.*, 2011)

Particularly, with respect to the data mining methodology, Han *et al.*, (2011) propose five aspects, one of which is "Boosting the power of discovery in a networked environment." This aspect highlights the mutual connections among most data objects, regardless of database relations, the Web, or files. Hence, the interconnection environment of raw data can be boosted with semantic links among other data.

2.4.2 Structured Query Language (SQL)

As a standard computer language, SQL functions to maintain and apply data in "relational" databases (Rockoff, 2016). In general, SQL consists of three main elements: Data Manipulation Language (DML), Data Definition Language (DDL), and Data Control Language (DCL). One of the advantages of SQL is that it has a more natural tendency (such as its similarity with declarative language) than other computer languages, such as

Basic or C^{++}. Therefore, this similarity enables people to achieve desired tasks more efficiently. The SQL language is relatively straightforward, because its data is retrieved only from relational databases rather than from entire databases. For example, in the SQL language, it is common to have a single statement for the desired target. The representative vendors of SQL are Oracle and Microsoft.

2.5 Useful statistical tool - Bayesian Network

Although there have been numerous data for independent statistical values (e.g., the probability of control valve or pump failure) in the chemical industry, these individual numbers are insufficient to predict possible hazards of a complex system. In light of this, Bayesian Network (BN) analysis will be suggested. BN is widely used to predict conditionally dependent statistical relationships (F. Khan, Rathnayaka, & Ahmed, 2015). Currently, the safety field utilizes this approach in applications with other HAZID tools or risk assessment tools. In this research, BN analysis will be suggested for future work.

2.6 Design error as a contributor to incidents

Without the lessons learned from previous incidents, we cannot achieve a more enhanced process safety management system. For this reason, this subsection reviews which contributors have were identified in the previous chemical process industry incidents.

2.6.1 Design errors in the process design lifecycle

Baybutt (2016b) emphasized "process lifecycle" issues as overlooked in the chemical process industry. A standard safety management program (OSHA PSM, 14 elements) and a risk-based process safety management program (RMP RBPS, 20 elements) have contributed to the process safety field. However, he argued that no program incorporates lifecycle issues, one of which is process design errors at the engineering stage, even though they can affect incidents significantly.

Definition of design error

Even though process engineers strive to make satisfactory designs, they can make mistakes (Kidam & Hurme, 2012). This is because engineers are human and they typically face time pressure during all project stages. Thus, it is almost impossible to create an infallible design.

Prior to further analysis, it is necessary to define design error, because it is not straightforward. According to Taylor (1975), the definition of "design error" is as follows:

"*During analysis of incident records, a design error is deemed to have occurred, if the design or operating procedures are changed after an incident has occurred*."

That is, design errors are associated with both design and operating procedures (including the operator–technical interface) (Kidam & Hurme, 2012). Based on the definition, it is

essential to examine whether there is an underlying correlation between design errors and each design phase.

Design errors in process design lifecycle

Based on their early research indicating that design-related errors are the primary incidents in the chemical process industry (Kidam, Hurme, & Hassim, 2010), Kidam and Hurme (2012) analyzed design errors occurring in different stages of the process lifecycle by utilizing the Failure Knowledge Database (FKD, 2011). They concluded that each design phase has different types of design errors, so each stage has unique critical points: 1) R&D and preliminary phase: process conditions, chemical reactivity, and incompatibility, 2) Basic engineering phase: construction material and layout, and 3) Detailed engineering phase: layout and protection system.

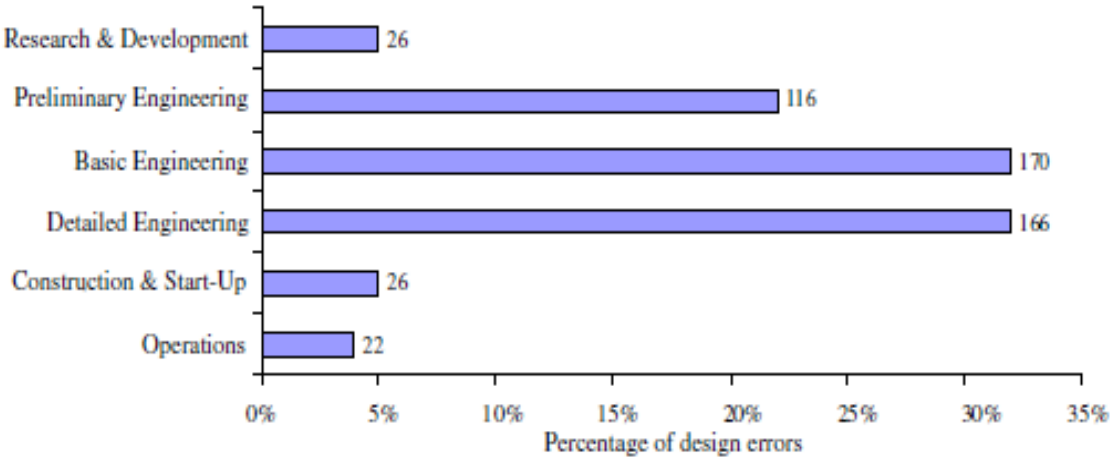


Figure 11. Distribution of design errors throughout the plant lifecycle (Kidam & Hurme, 2012)

Figure 11 shows that the basic and detailed engineering phases generated about 55% of total design errors. However, the process analysis in the initial stage is critical as well. If a proper hazard analysis is carried out in the early process design stage, the combinational results can eliminate erroneous process data (Kidam & Hurme, 2012). Conversely, many errors in the basic or detailed engineering phase are affected by the R&D or preliminary phases because of incorrect design conditions.

Consequently, this subsection offers safer designs for each stage in the chemical process industry and insights on how they can be reflected in the new HAZID tool.

2.6.2 Contributions of equipment failure modes to incidents

Several studies have revealed that "equipment failure" is the factor that contributes most to incidents caused by human factors in the chemical process (Kidam & Hurme, 2013; Nivolianitou, Konstandinidou, & Michalis, 2006; Prem, Ng, & Mannan, 2010). For example, Figure 12 compares the results of Nivolianitou *et al.* (2006) and Prem *et al.* (2010) in which Major Accident Report System (MARS) data[10] and Risk Management Plan (RMP) data[11] were utilized, respectively. There is no hybrid zone, such as equipment failure + human and equipment failure + environment, in the figure, because Prem *et al.* (2010) divided the two aspects roughly into equipment and human. However, it is stressed

[10] Investigated period was 1985–2002.
[11] Investigated period was 1994–2009.

that the effect of equipment failure accounts for most previous incidents in the chemical process industry, and the human aspect takes second place.

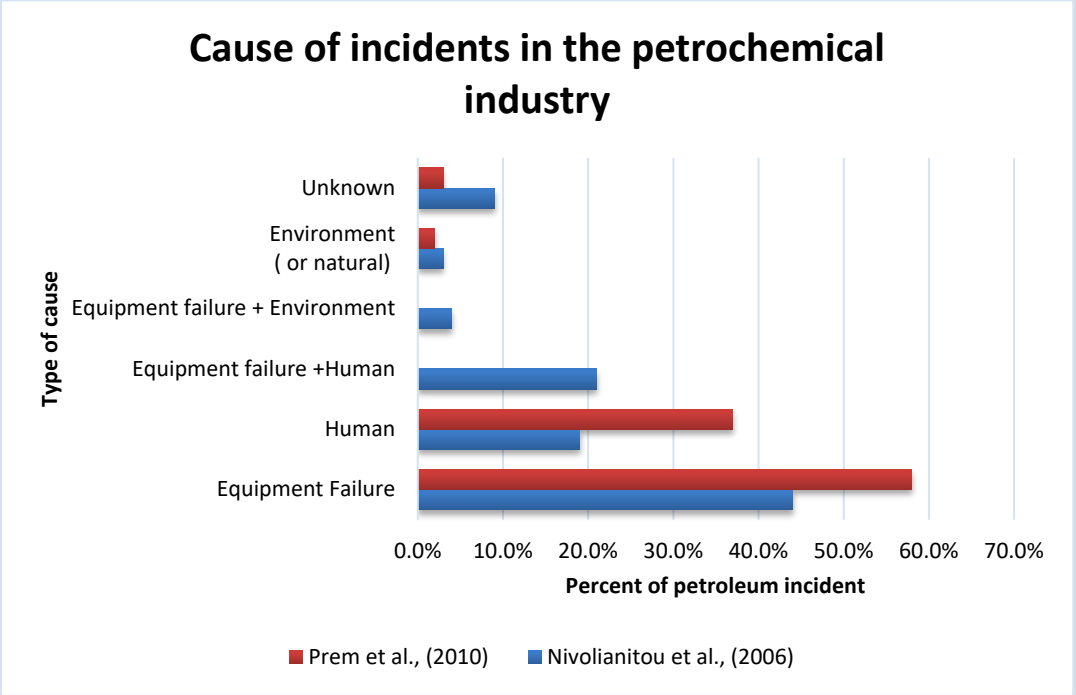


Figure 12. Distribution of contributors to chemical incidents

Furthermore, Kidam and Hurme (2013) investigated equipment as contributors to chemical process incidents. Using the 364 case data samples from the FKD (2011), they mainly analyzed four aspects: 1) distribution of failure equipment and comparison with previous analyses, as shown in Figure 13; 2) contributors to equipment accidents, as shown in Table 5; 3) main contributor to chemical incidents; and 4) correlations between

the main contributors and sub-contributors. Consequently, Kidam and Hurme (2013) proposed a “checklist for equipment safety enhancement” enabling the prioritization of the more important aspects depending on equipment type.

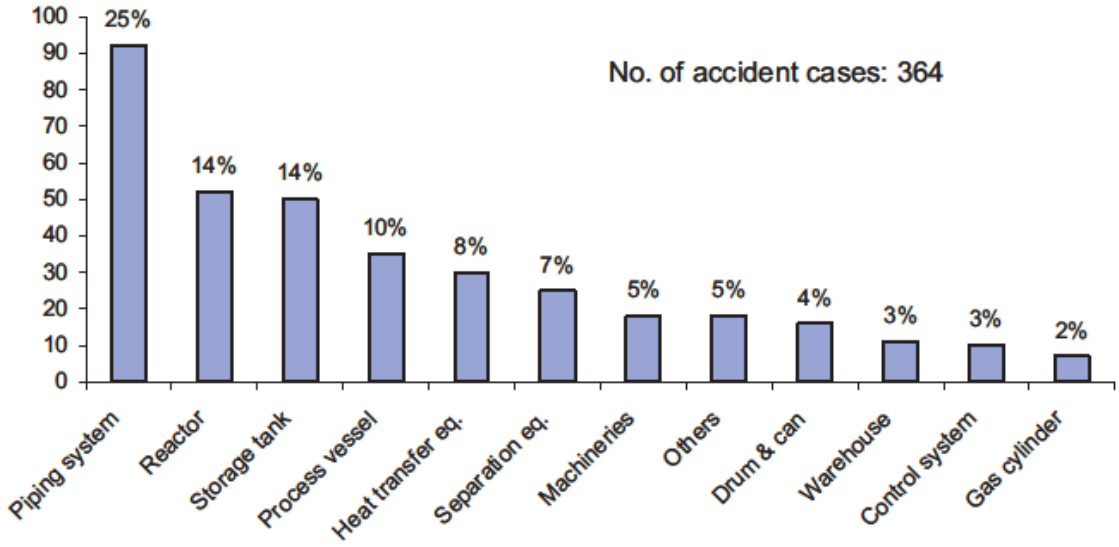


Figure 13. Proportions of incidents caused by specific equipment (Kidam & Hurme, 2013)

Figure 13 shows the proportions of incidents caused by specific equipment. Considering a domino effect, only the equipment-initiated incidents are counted for in these proportions. About one-fourth of the chemical process incidents arose due to piping systems. The second most common causes of chemical process incidents were reactors and storage tanks, both at 14%, followed by process vessels, heat transfer equipment, and separation equipment. The ranking of equipment contributions to incidents provides a

reliable estimation, as it is the same method as that used in the analyses of Instone (1989) and Marsh Inc (1987), which investigated the petrochemical industry.

Table 5. Number and proportion of contributors in equipment related incidents (Kidam & Hurme, 2013)

Incident contributor	Piping system	Storage tank	Reactor	Heat transfer Eq.	Process vessel	Separation Eq.	Total
Human/organizational	41 (18%)	36 (33%)	12 (16%)	12 (16%)	12 (17%)	9 (15%)	122 (20%)
Contamination	17 (7%)	6 (5%)	12 (16%)	11 (15%)	14 (19%)	15 (25%)	75 (12%)
Heat transfer	17 (7%)	10 (9%)	17 (23%)	11 (15%)	8 (11%)	9 (15%)	72 (12%)
Flow related	23 (10%)	15 (14%)	6 (8%)	9 (12%)	10 (14%)	8 (13%)	71 (11%)
Reaction	10 (4%)	3 (3%)	17 (23%)	2 (3%)	12 (17%)	9 (15%)	53 (9%)
Layout	25 (11%)	6 (5%)	1 (1%)	4 (5%)	5 (7%)	3 (5%)	44 (7%)
Fab. const. and inst.	30 (13%)	5 (5%)	2 (3%)	5 (7%)	1 (1%)		43 (7%)
Corrosion	22 (9%)	4 (4%)	3 (4%)	8 (11%)	1 (1%)		38 (6%)
Construction material	19 (8%)	4 (4%)	3 (4%)	8 (11%)	2 (3%)	1 (2%)	37 (6%)
Static electricity	2 (1%)	6 (6%)	2 (2%)	3 (4%)	5 (7%)	3 (5%)	21 (3%)
Mechanical failure	8 (3%)	4 (4%)			2 (3%)	1 (2%)	15 (2%)
External factor	4 (2%)	9 (8%)					13 (2%)
Vibrationa	8 (3%)			1 (1%)			9 (1%)
Erosiona	6 (3%)						6 (1%)
Utility related	2 (1%)					23 (%)	4 (1%)
Total contributors	234 (37%)	108 (17%)	75 (12%)	74 (12%)	72 (12%)	60 (10%)	623
Contributors per accident	**2.5**	**2.2**	**1.4**	**2.5**	**2.1**	**2.4**	**2.2**

Additionally, it is noted that on average, 2.2 elements (human related or technical aspects) affected each equipment incident, as shown in Table 5. That is, most chemical incidents occur when about 2.2 cause aspects are integrated, and the chances of incidents are reduced with a single factor. This table points to the correlations with specific contributors with each type of equipment. For example, about 33% of previous incidents related to

storage tanks occurred because of human/organization factors, which is a relatively big portion compared to the others. In this regard, we can prepare measures to avoid repeating similar events with storage tanks considering human aspects. Consequently, with this useful information, we can focus on individual equipment and its relevant contributors to incidents for an enhanced hazard analysis tool.

2.7 Chapter summary

In order to provide a basic background, this chapter has covered a wide range of topics, such as HAZID tools, data mining, and contributors to incidents in the chemical industry. By building on classical HAZOP and FMECA, a new HAZID tool will be proposed in the following chapter. For this tool, information related to data mining, especially the SQL language, and the approach that considers individual equipment for hazard identification will be utilized.

3. DATA-BASED SEMI-AUTOMATIC HAZARD IDENTIFICATION – THE CONCEPT

This chapter proposes the Data-based semi-Automatic HAZID analysis for deriving this overall insight that will enhance hazard identification with respect to chemical plants.

3.1 Introduction

"The whole is greater than the sum of its parts." (Bunge, 1979)

Rather than separating each component of a system, their combination enables people to imagine the bigger picture of functioning of an ensemble in the system; this holds in general, but certainly for a plant in which components may be connected over relatively large distance and in a complex way. For a comprehensive understanding, a critical point is deriving the proper connections among linked components of a system from the Piping and Instrumentation Diagram (P&ID) material, based on the fluid direction. Through defining and describing these links in the analysis sheets, the limitations of HAZOP and FMECA methods will be attenuated. This will also help to reduce the drawback in the HAZOP procedure of missing cause-effect relations because of initiating at a deviation and having to search back against flow direction for a cause.

3.2 Building stones of the DAHAZID analysis

Overall, as shown in Figure 14, this study highlights an integrated relationship of the following three factors: process data, applications of the relevant data, and proper HAZID tools. Keeping in mind that any one factor is not entirely responsible for the prevention

and/or protection of possible incidents, the DAHAZID analysis attempts to achieve more intertwined research attributes - correlations among process information, previous experiences, and appropriate current theories to develop more systematic approaches based on lessons learned.

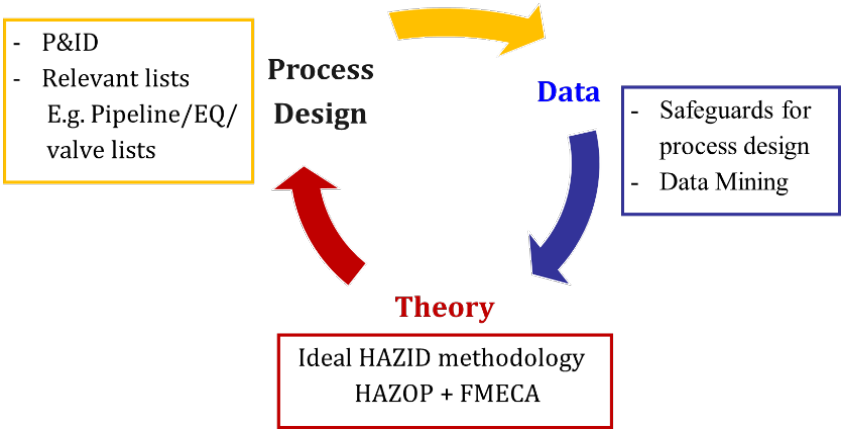


Figure 14. Conceptual stones of the DAHAZID methodology

3.3 Process design condition

We know that P&IDs and associated process documents serve besides others the fundamental role in the process industry of indicating the intended process conditions. Process engineers make or develop these documents based on a process design scheme, particularly giving more weight to the process perspectives, such as process optimization, than to safety aspects. Whenever they perform HAZOP and FMEA, PHA teams review the current process designs and the process conditions by employing the multiple

documents simultaneously. Because of this multiplicity of documents, consistency in the information should avoid confusion and misunderstanding.

However, there are likely to be burdensome aspects in dealing with the multiplicity of process papers. Worst of all, humans are prone to errors, so there might be inconsistencies among different documents (e.g., the line list and its P&IDs). In addition, it takes considerable time to review all data while conducting a HAZID meeting. In general, engineers should be ready to open any relevant documents during a HAZOP study and to respond to the information, rather than to review incorrect data under time-sensitive conditions.

3.3.1 Introduction of SP P&ID®

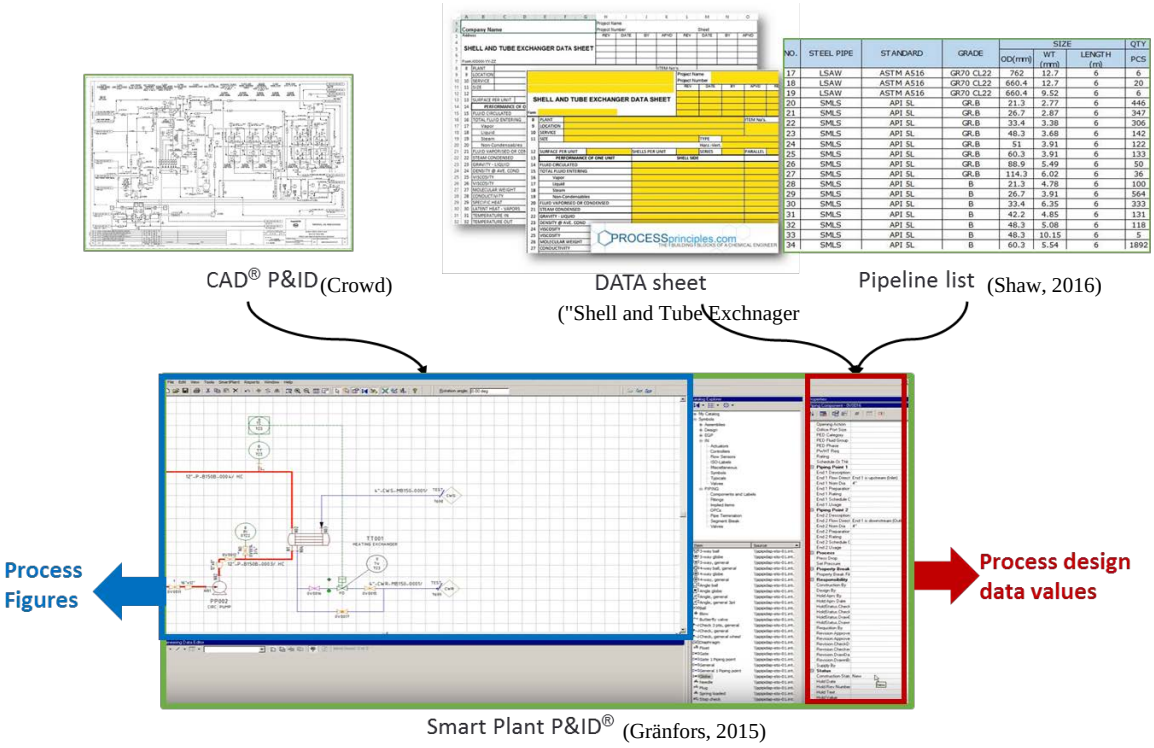


Figure 15. Trade-off between SmartPlant P&ID® and traditional manners

Recently, a cutting-edge software, Intergraph's SmartPlant Piping and Instrumentation Diagrams® (SP P&ID®), was commercialized by Intergraph. It not only represents the process diagram, like Auto Computer-aided Design (CAD)® P&ID, but also it encompasses various data, so it enables the handling of process data and symbols simultaneously, as shown in Figure 15. Additionally, there are benefits with SP P&ID® in comparison with older packages such as saving time and presence of highly accurate data, with SP P&ID® in comparison. Figure 16 and Figure 17 (below) show examples of extracted process data through SP P&ID® in a Microsoft EXCEL file.

Piping Component

Piping Comp Subclass	Piping Comp Type	PipeRun Item Tag	Piping Comp Class	Piping Comp Subclass	Nominal Diameter	End 2 Nom Dia
Valve	Gate valve	LP-SCW-1-01508-C1D-1"-Ih	In-line component	Valve	1"	1"
In-Line Fitting	Concentric diameter change	LP-SCW-1-01101-A6D-10"-IS	In-line component	In-Line Fitting	10"	8"
Valve	Gate valve	SL-1-01108-A6D-4"-Ih	In-line component	Valve	4"	4"
Valve	Gate valve	LP-SCW-1-01101-A6D-10"-IS	In-line component	Valve	10"	10"
Valve	Gate valve	DMW-1-01202-ASL1D-8"-Ih	In-line component	Valve	8"	8"
In-Line Specialty Component	Drain connector	WW-1-01101-A6D-4"-Ih	In-line component	In-Line Specialty Comp	4"	4"
In-Line Specialty Component	Drain connector	WW-1-31103-115201D-14"-IS	In-line component	In-Line Specialty Comp	14"	14"
In-Line Fitting	Concentric diameter change	DMW-1-01202-ASL1D-8"-Ih	In-line component	In-Line Fitting	8"	6"
In-Line Fitting	Flange	SL-1-01101-A6D-12"-Ih	In-line component	In-Line Fitting	12"	12"
Valve	Gate valve	DMW-1-01202-ASL1D-8"-Ih	In-line component	Valve	8"	8"
In-Line Fitting	Concentric diameter change	LP-SCW-1-01101-A6D-10"-IS	In-line component	In-Line Fitting	10"	8"
Valve	Gate valve	-1-106668-2"-Ih	In-line component	Valve	2"	2"
In-Line Fitting	Concentric diameter change	BFW-1-01103-A6D-3"-N	In-line component	In-Line Fitting	3"	2"
Valve	Gate valve	CWS-1-01101-L1D-2"-N	In-line component	Valve	2"	2"
Valve	Gate valve	SL-1-01104-A6D-6"-Ih	In-line component	Valve	6"	6"
In-Line Fitting	Flange	-1-V1003-A6D-2"-Ih	In-line component	In-Line Fitting	2"	2"
In-Line Fitting	Flange	-1-V1003-A6D-Ih	In-line component	In-Line Fitting		
In-Line Fitting	Concentric diameter change	CWR-1-01101-L1D-2"-N	In-line component	In-Line Fitting	2"	1 1/2"

Figure 16. Parts of piping component list from SP P&ID®

Instrument

Item Tag	Pipe Item Tag	Description	End 2 Nom Dia	Instr Class	Instr Type	End Component	End Nom Dia
PSV-3111	**SL-237-01102-A6D-3"-Ih**	**EXCESSIVE HEAT INI**	**4"**	**Relief devices**	**Angle press relief va**	**False**	**3"**
LCV-3111	**DMW-237-01202-ASL1D-6"-Ih**		**6"**	**Control valves and regulate**	Globe control valve	False	6"
LCV-3117	**LP-SCW-237-01101-A6D-8"-IS**		**8"**	**Control valves and regulate**	Globe control valve	False	8"
FE-3111	DMW-237-01202-ASL1D-10"-Ih		10"	Other in-line instruments	Orif plate & flanges	False	10"
FO-3112	SWR-237-01101-115201D-8"-N		8"	Other in-line instruments	Orif plate & flanges	False	8"
FO-3111	SL-237-01106-A6D-3"-Ih		3"	Other in-line instruments	Orif plate & flanges	False	3"
FE-3112	SL-237-01101-A6D-12"-Ih		12"	Other in-line instruments	Orif plate & flanges	False	12"
PSV-3112	**SL-237-01104-A6D-3"-Ih**	**EXCESSIVE HEAT INI**	**4"**	**Relief devices**	**Angle press relief va**	**False**	**3"**

Figure 17. Parts of instrument list from SP P&ID®

Consequently, SP P&ID® can manage a wide range of process data and figures of typical P&IDs, so it enables engineers to use the data more effectively. Especially, among these data of SP P&ID®, pipeline tag numbers and their directions are used in terms of a HAZOP aspect, and process design conditions are used in case of FMECA. The following section provides a description of how to use these data properly for the purpose of continued hazard identification.

3.4 Application of valuable data

The purpose of this section, associated with the application of data, is twofold: to deal with the process data in the HAZID procedure and to make use of accumulated industry experiences, especially regarding equipment failure scenarios and safeguards. First, interested data can be extracted with the aid of SP P&ID® so that it will help to achieve a simpler and more consistent semi-automated analysis. Accumulated industry experiences, herein taken from the CCPS book (CCPS, 1998) *Guidelines for Design Solutions for Process Equipment Failures*, will be employed for equipment failure scenarios and safeguard recommendations.

3.4.1 Connectivity of a process plant

To date, in almost all process plants, discrete process documents have conventionally been summarized, used and stored as Microsoft EXCEL files, without further data processing. In other words, in chemical plants few attempts are made of data mining to deal with their process data effectively; only the correctness of each input documentation was satisfied. This study, thought, will conduct a data mining operation to extract valuable information hidden in the data mass by applying Structured Query Language (SQL) of Microsoft® SQL Server 2012. The following subsection explains which data can be mined.

Our body maintains its health when its organs and physical structures are working properly thanks to blood vessels, which make links throughout the whole physical structure. Analogously, in the process industry, pipelines might be regarded as the blood vessels of chemical plants, since they connect all process components; almost all plant elements have

connections with piping and piping components so that an overall process system can be recreated based on the links. For this reason, when process engineers make a process document for any process component, it is common to report the associated piping numbers to designate an accurate location of each item. For instance, Figure 18, which shows a part of a Pressure Safety Valve (PSV) data sheet, refers to a pipeline number and its size. Generally, all the lists for pipes, equipment, and instruments incorporate piping numbers, as shown in Figure 19. Based on this, the piping numbers can be used to interconnect the entire process. Consequently, because nearly all process data documents involve piping numbers, this study will exploit process piping numbers to connect the main process components (equipment, valves, pipelines, devices, *etc*.).

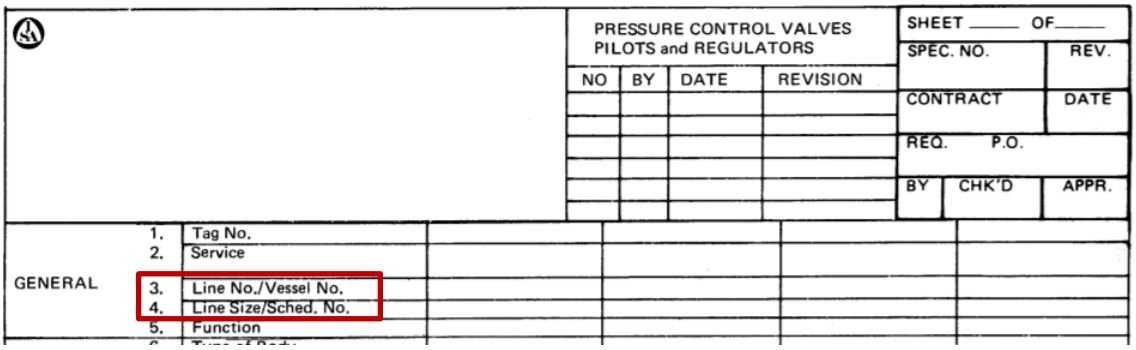


Figure 18. Part of a PSV data sheet

Adopted from ISA The Instrumentation Systems and Automation Society (1981)

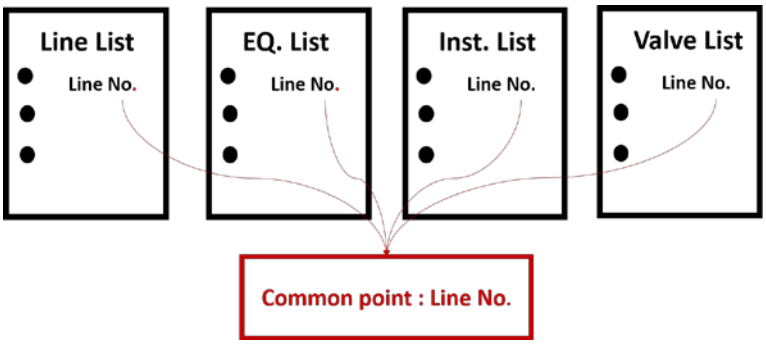


Figure 19. Line numbers as a common point

Based on the data mining process in Figure 10, the data mining in this study will be performed in three steps: data source (e.g. process design condition), data extraction with SQL, and data presentation (as prepopulated worksheets that will be explained in Subsection 3.5.2). Fortunately, we can save time with SP P&ID®, since the data source and data extraction steps can be performed at nearly the same time with the program. For example, Figures 16 and 17 can be extracted once people input the process symbol with its corresponding data. Moreover, another critical benefit is that the extracted EXCEL file contains a flow directions for pipes under the categories “from” and “to” respectively, the exact pipe number for each valve, and the inlet or outlet pipes of equipment. This useful information is collected in case a P&ID figure is created properly and provided with data.

For reference, albeit pipeline numbers are critical data for this DAHAZID method, it might be not necessary to consider whether generic data sheets indicate pipeline numbers in this

study. This is because this study will utilize SP P&ID®[12] that composes data automatically when its figure is drawn. However, this background might be useful, provided that we use more traditional data such as a Microsoft EXCEL or PDF file. Hence, it can be an alternative to illustrate this new HAZID method without SP P&ID® by taking into account various design conditions.

3.4.2 Safeguards and recommended proper guidelines

Often, there is a tendency in the chemical industry to separate chemical process and safety domains. However, process engineers should identify hazards to result in an inherently safer design (including operating procedures) of process plants, while considering economic aspects. Some process engineers might overlook the safety considerations, believing that it is enough to follow their current project guidelines or industry standards. However, these rules or guidelines are not sufficient to minimize potential hazards. As many CSB[13] incident investigation reports have found, there are also flaws in the recommended practices of the American Petroleum Institute (API), the American Society of Mechanical Engineers, and the National Fire Protection Association (NFPA) (Baybutt, 2016a), which are regarded as the most credible engineering guidelines. In case safer design schemes are not taken into account within initial design processes, numerous extra safety measures might be suggested during a HAZOP study, which is conducted at about

[12] SP P&ID® might be a cornerstone example of *Industry 4.0*, which is the current trend of automation and data exchange in the manufacturing equipment sector for smart factories (Group, 2013). Taking into account this trend phenomenon, this study exclusively describes the strength SP P&ID® in this context. There will be more descriptions its strength and weakness in Subsection 6.1.2.

[13] The associated table will be represented in Appendix B

the middle of projects. In addition, however, they might struggle to find the safety issues from the HAZOP meeting, which could cause unnecessary economic losses. Therefore, safety and process performances are unavoidably dependent.

Generic design solutions

It is required for engineers to make an appropriate choice among numerous process safety designs by taking into account their benefits. According to CCPS (1998), safety system designs correspond to one of the following four categories: (1) inherently safer, (2) passive, (3) active, and (4) procedural. As mentioned in Section 1.1.2, proper safety system design is fundamental to reduce potential adverse events. Figure 20 presents an approximated comparison regarding expenses and the complexity of each safeguard. Because it is impossible to install all potential safe guards, for safeguard solutions, process safety design engineers must balance effectiveness, complexity/ reliability, and cost. In other words, process engineers should seek a safer system by properly taking into account at the same time their own circumstances, such as their cost benefits and regulations.

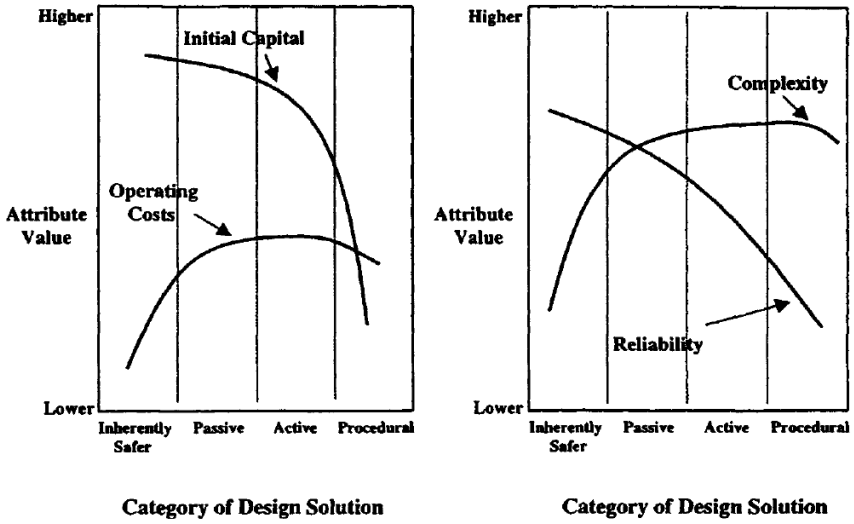


Figure 20. Comparison of cost and functional attributes for design categories (CCPS, 2008)

Crowl and Louvar (2001) provided the definitions and examples of the four design solutions in Table 6. There are often overlaps between the inherently safer and passive design solutions. Consequently, this study will integrate these categories into one solution (CCPS, 1998) when the proper guidelines are outlined in the next section.

Of the components shown in Figure 2. Hierarchy of safeguard in Chapter 1, the last two, but nevertheless critical safeguards, PPE and emergency response, are not covered by this study.

Table 6. The four design solutions (Crowl & Louvar, 2001)

Design Solution	Definition	Example
Inherently Safer[14]	To eliminate or mitigate hazards with less hazardous conditions or materials	Compatibility between heat exchanger and process fluid
Passive	To add safety features that do not require action from any devices. The associated devices are unrelated to process variables.	Double tube-shell construction
Active	To add active safety features depending on process variables	Installation of a PSV
Procedural	To require a person from performing an action to prevent potential incidents	Periodic sampling of a low-pressure fluid

Guidelines for failure scenarios and design solutions

To date, many engineers depend on personal experiences regarding failure modes and safe design solutions. However, we should expect to have more reliable solutions using guidelines from the accumulated experiences of a myriad of process experts, rather than just relying on our relatively unsupported intuition. Moreover, provided that the guidelines are clear to follow, the expected actions for process safety can be coherent across the process industry. This aspect might also influence young engineers to grasp process safety concepts without restrictive difficulty. CCPS (1998) introduced the equipment failure modes and their safety design solutions, (inherently, passive, active, procedural) for ten

[14] Crowl and Louvar (2001) gives four approaches for an inherently safer design: minimize, substitute, moderate and simplify

equipment types[15]. Since the guideline includes nearly every component required in the chemical industry, it would be useful to apply safer designs based on expected failure modes. Of course, companies can customize this guideline by suggesting modifications to it or updating.

For example, it is assumed that level controls on a vessel fail when the vessel sustains a low level, compared to the normal operation condition. Thus, according to CCPS (1998), we can determine the potential design solutions, as provided in Table 7, as part of sixty-one failure scenarios for a vessel. To this regards, in a study after stimulating our imagination by assuming operational deviation, we first we have to select equipment failure modes according to the CCPS (1998) reference. Next, depending on the expected vessel failure modes, process engineers can select safeguard solutions from among the sixty-one cases. Once engineers/analysts have identified a relevant failure scenario, the guideline suggests corresponding recommendations for designing a newly suggested measure and information for reviewing current process designs. For the DAHAZID analysis, the guidelines will serve to make viable a new, semi-automated HAZOP.

[15] Vessel, reactors, mass transfer equipment, heat transfer equipment, dryers, fluid transfer equipment, solid-fluid separators, solids handling and processing equipment, fired equipment and piping and piping components.

Table 7. Example design solutions for vessel (CCPS, 1998)

Equipment :Vessel

No.	Operational Deviations	Failure Scenarios	Potential design solutions		
			Inherently Safer/Passive	**Active**	**Procedural**
45	Low Level	Level control failure	• Locate underflow nozzle to maintain a minimum liquid level in the vessel	• Low level alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve	• Manual shutoff on low level indication

3.5 A new semi-automated hazard identification method

By suggesting HAZOP and FMECA prepopulated worksheets, this section employs a hybrid HAZID approach applying HAZOP and FMECA attributes in conjunction with previous steps. Because HAZOP is incapable of predicting an inherent failure mode of a process component, it is necessary to compensate this insufficient knowledge with FMECA. In this sense, the DAHAZID analysis integrates the two HAZID tools, HAZOP and FMECA; by making use of the system connectivity in Section 3.4.1, the DAHAZID tool enables the determination of possible causes and consequences in a system with the HAZOP perspective. Meanwhile, with the FMECA attribute, the new tool weighs the

possible failure mode associated with the particular environment of a system, problems intrinsic to each piece of equipment, and human errors.

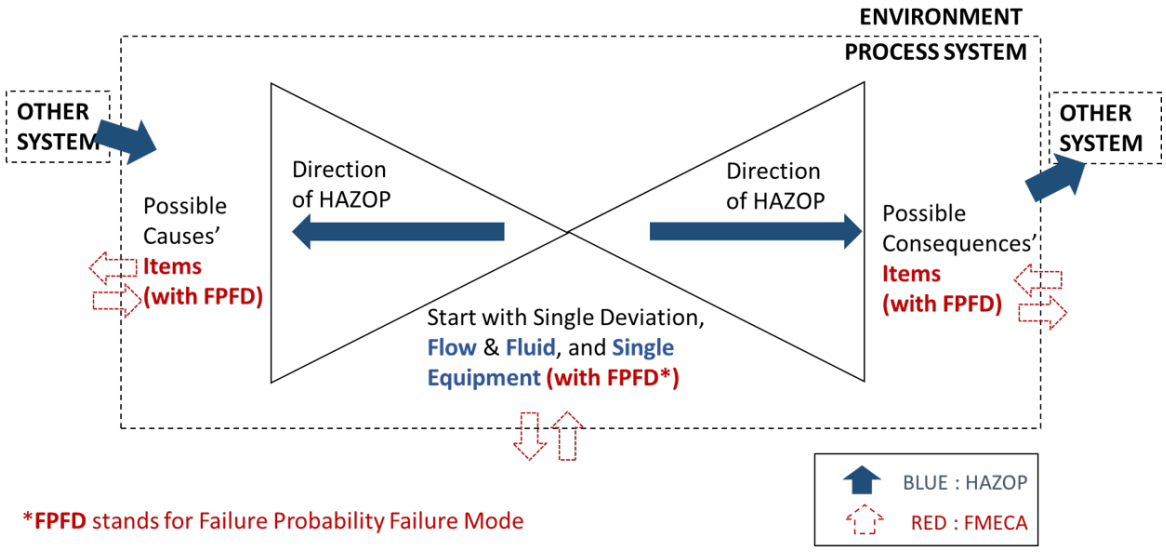


Figure 21. Working directions of DAHAZID methodology

Derived and combined from Figures 3 and 4, Figure 21 shows the overall workflow of the DAHAZID methodology. The navy-blue and red-arrows present HAZOP and FMEA attributes, respectively. Regarding the HAZOP attribute, the significant characteristics of this method are to have a clear starting point (*one reference equipment*) and only one single guide parameter (*flow*) for possible causes. Following that one equipment is designated as a reference equipment, analysts can easily imagine possible scenarios merely by considering *no, less, or more flow* for possible causes. Meanwhile, FMECA

functions to review the failure modes of each piece of equipment and potential effects, including their Failure Probability Failure Modes (FPFD) to obtain a quantitative indication. To support effectively these notions, the DAHAZID analysis utilizes the following “prepopulated worksheets” that take advantage of HAZOP and FMECA.

3.5.1 Failure scenarios associated with HAZOP attributes

Pre-requisite condition and aim

Based on the piping connectivity with fluid directions in Subsection 3.4.1, a prepopulated worksheet will be introduced to achieve a semi-automated analysis. For a reliable result, a HAZOP study requires proper guidelines under the leadership of a skilled HAZOP facilitator (MacGregor, 2013). That is, it is an uncommon occurrence to prepare a HAZOP without a facilitator in advance. Additionally, even in the HAZOP studies with experts, their outcomes are always non-identical. However, this HAZOP attribute that worksheet proposed here generates directions to engineers implicitly with respect to identification of possible causes and consequences. This aspect prompts a self-directed study and triggers more discussions among engineers, which will lead to review hazardous scenarios more thoroughly and to save time for a HAZOP review meeting. Consequently, the following sections explain how to create the pre-populated worksheet.

Workflow with fluid directions

As mentioned above, the HAZOP attribute worksheet in DAHAZID examines one process parameter, flow, regarding possible causes. The strength of this approach is to use

straightforward thinking alongside theses flow directions, whereas the main drawback in a HAZOP study is counterintuitive brainstorming from deviation to cause upstream and to effect downstream. In a theory, during a HAZOP meeting, a HAZOP team following from a combination of a process variable and guide word, as shown in Table 8; to find all deviations, participants should match multiple process parameters with guide words. Yet, this process raises several issues. First, it is cumbersome to apply combined simultaneous deviations (typical deviations are shown in Table 8). Second, the required thinking in HAZOP is counterintuitive, because we must find possible causes for a proposed deviation. That is, this step as already mentioned requires backward thinking (Baybutt, 2015b; MacGregor, 2013). Alongside the combination of a process variable and guideword, the way of thinking is not aligned with common sense and the backward thinking does not lead to identifying all causality. In contrast, there will be more opportunities to review all possibilities clearly, if the study is conducted in a natural sequence. For these reasons, the DAHAZID analysis seeks a more visible workflow along the fluid direction of a system.

Table 8. HAZOP deviation matrix (Crawley & Tyler, 2015)

Guide words / Process Variables	**More**	**Less**	**None**	**Reverse**	**Part of**	**As well as**	**Other**
Flow	High flow	Low Flow	No Flow	Back Flow	Wrong concentration	Contaminants	Wrong material
Temperature	High Temperature	Low Temperature					
Pressure	High Pressure	Low Pressure					
Level	High Level	Low Level	No Level				

Reasons for the fundamental variable, flow

There are two main reasons this study chooses flow as a fundamental parameter for a system. First, similar to pipelines, the flow has connections with other process variables, such as temperature, pressure, and level. For example, the low flow of an inlet line brings about a low level for a vessel, or conversely the low flow of an outlet line can generate a high level for a vessel. Additionally, if more flowrate goes through hot-side of a heat exchanger, the temperature of the opposite side (cold-side) in the heat exchanger will be higher than design intent. In other words, flow is likely to propagate fault and to influence other process variables. Furthermore, it is convenient to have a simpler approach along the flow direction. Rather than reviewing all process variables regarding possible causes, it is much easier to examine possible causes that are likely to occur hazardous consequences. For example, with this new method, we are only required to review the

possibilities of no flow, less flow, and more flow on each item, which will be indicated on the prepopulated worksheets.

In case of mixtures partial flow rates of components shall be tracked.

Another factor to consider with flow, fluid type

It is noted that every fluid has its own properties and may therefore exhibit different phenomena under the same conditions. For instance, at the same pressure and temperature, water and steam have different physical properties even though they have identical chemical structure. Assuming one inlet line for steam supply is blocked, by cooling the line might result in a vacuum state, which does not occur in a water supply line. Consequently, it is also necessary to review potential scenarios regarding fluid type under operational conditions.

Prepopulated worksheets for the HAZOP aspect

The starting point of this method is one item of static or rotating equipment, herein named as *reference equipment*, and possible incident causes or consequences would connect with the equipment given in the directions of flow. Based on the notion, by making use of SQL language, this research proposes to create prepopulated worksheets along two approaches, *path 1* and *path 2*, respectively. Microsoft SQL Server 2012®[16] is applied to sort the

[16] Amol Jayant Bansod, an IT student staff of MKOPSC, made the relevant codes with the SQL program based on this paper's notion.

possible cause items in paths 1 and 2; path 1 contains potential failure causes on inlet lines from a reference equipment, whereas path 2 predicts potential causes on outlet line problems of the reference equipment. In accordance with the worksheets, we can perform a semi-automated HAZOP based on the previous two prerequisites, only flow as a possible primary deviation and on recognizing fluid characteristics. Figure 22 represents how this research leads to HAZOP worksheets. In Figure 22 and Figure 23, cells starting "#" mean that the cell will be filled with SQL coding to construct a prepopulated worksheet. Then, the yellow empty column under "Check" must be reviewed by HAZID process engineers. In the spreadsheet, as expected, other variables such as level appear as a consequence. Once failure scenarios are selected, the corresponding safeguards can be suggested from accumulated experience (e.g., CCPS, 1998)

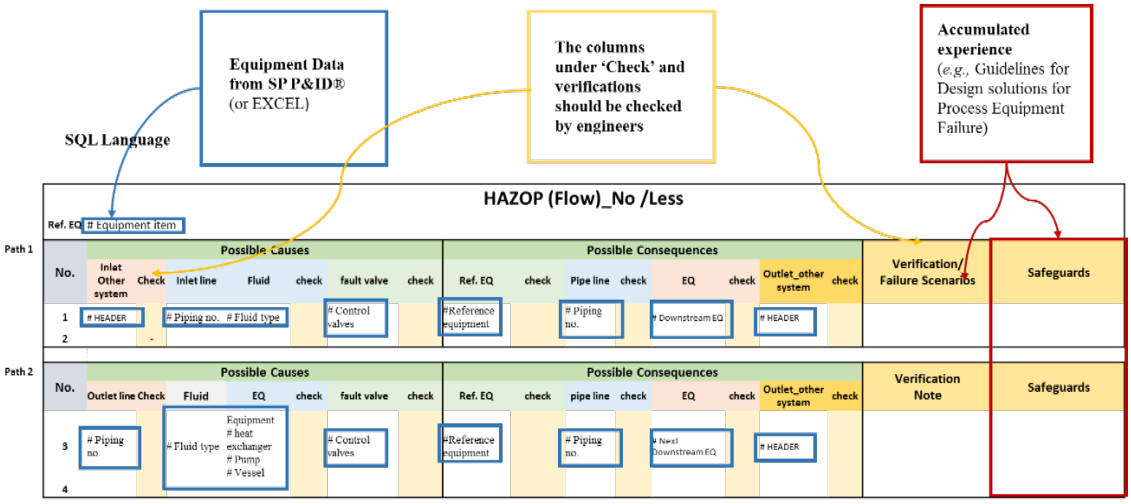


Figure 22. Sample guideline for prepopulated HAZOP worksheet

3.5.2 Failure scenarios associated with FMECA attributes

Regarding the failure mode of each item in a plant, FMECA is important in the methodology for identifying causality. HAZOP does not take account of failure modes of an individual item, but FMECA represents equipment designs and potential faults of each component. Thus, including and utilizing the FMECA features, the new tool generates failure modes of each equipment.

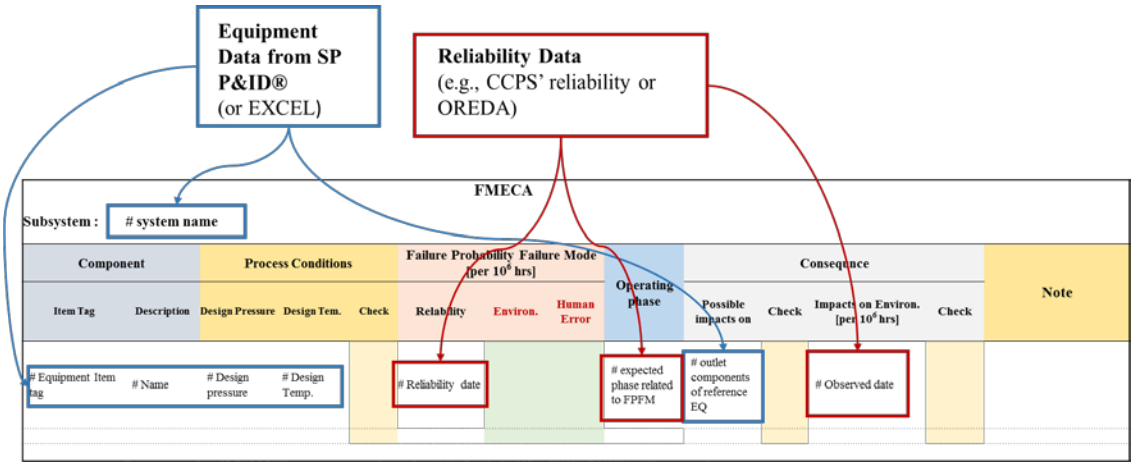


Figure 23. Sample guideline for prepopulated FMECA worksheet

Figure 23 illustrates a sample prepopulated FMECA worksheet, which is composed of two types of data, process data, and Failure Probability Failure Mode (FPFM). Analogous to the previous prepopulated HAZOP worksheet, we can acquire process design data with the aid of SP P&ID® and SQL, and we also add FPFM, which can be borrowed from authorized data sources (e.g., the CCPS (1989) reliability handbook, or the databases of

HSE (2012) or OREDA (2015)). For more enhanced predictions of equipment reliability and failure modes, it is essential to seek practical data analysis methods, which minimize laborious tasks and maximize accuracy of the analysis. Also, other possible failure causes (such as environment and human error) must be considered as well as how to reduce and identify them.

3.6 Overall workflow of new HAZID

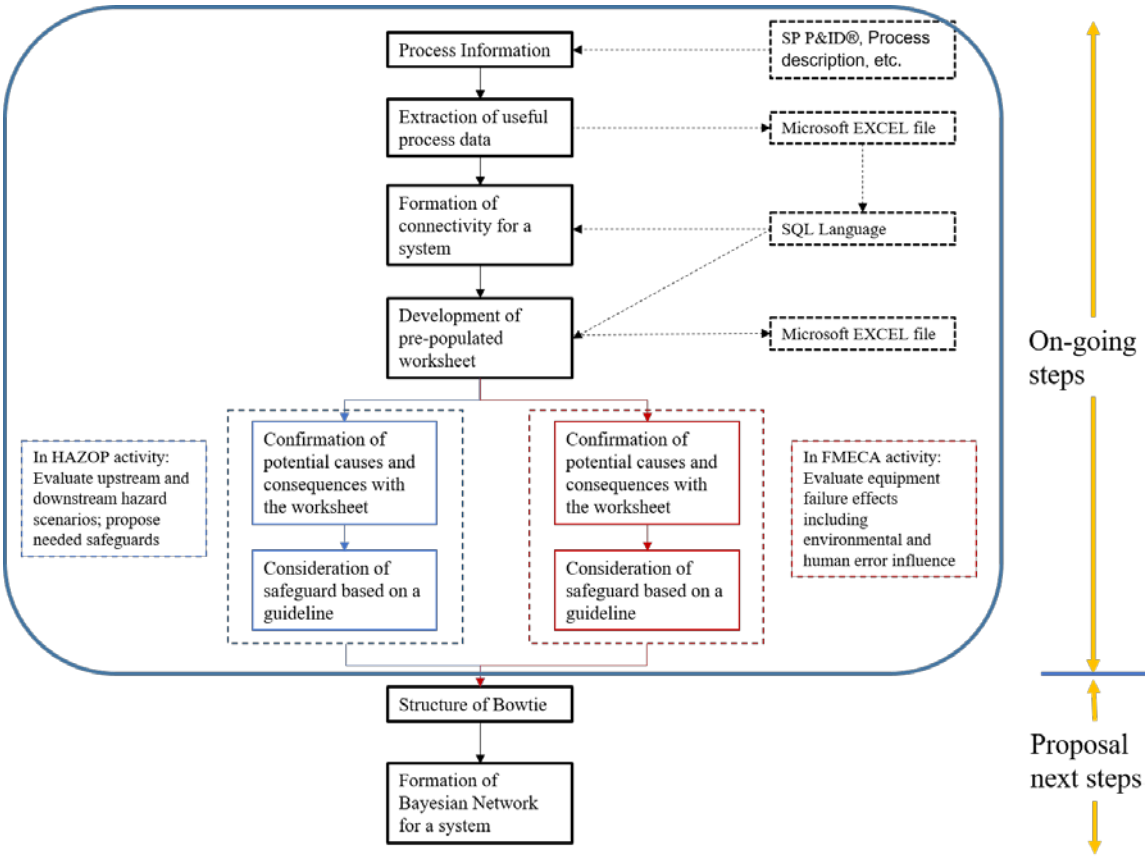


Figure 24. Workflow diagram of DAHAZID analysis

Figure 24 shows the overall workflow of the development of the DAHAZID method with an on-going and a future part, while within the on-going part the actual work process is shown as followed here. Because of the several steps and the application of supporting technologies, it seems rather complex. The on-going part develops as shown in this paper; the proposed next steps will still take a further effort. However, the result will be in a new semi-automated HAZID, DAHAZID, in which an HAZID-team will obtain the information in a more convenient and consistent way, so that the team can focus on the essentials of identifying and defining scenarios and is not delayed by fuzzy information deficiencies. Once this development is completed, the achievement of safer process designs can be expected in a more time-efficient way.

3.7 Chapter summary

Taken together, this chapter illustrates how DAHAZID analysis results in a more effective HAZID tool based on prepopulated worksheets. In contrast to traditional HAZID methods, it is relatively easy to predict possible scenarios and suggest safeguards consistently employing a new approach. That can be helpful for engineers facing time pressures and potentially missing scenarios. To demonstrate the potential of the superior HAZID tool, the following chapters will show simple case studies.

4. A NEW METHODOLOGY – A SIMPLE APPLICATION

Prior to undertaking an actual case study, this chapter illustrates a simple application of how this new method can be useful without any SP P&ID®, especially for the initial design stage.

4.1 Simple case study using HAZOP attributes in DAHAZID

4.1.1 Making connections with pipelines

Based on a simple process diagram, as in Figure 25, which could be encountered in the basic design stage, an application of the new method will be performed. Because this diagram does not contain any safety device as an initial stage design, the new method will be used to identify possible hazardous scenarios and suggest corresponding safeguards.

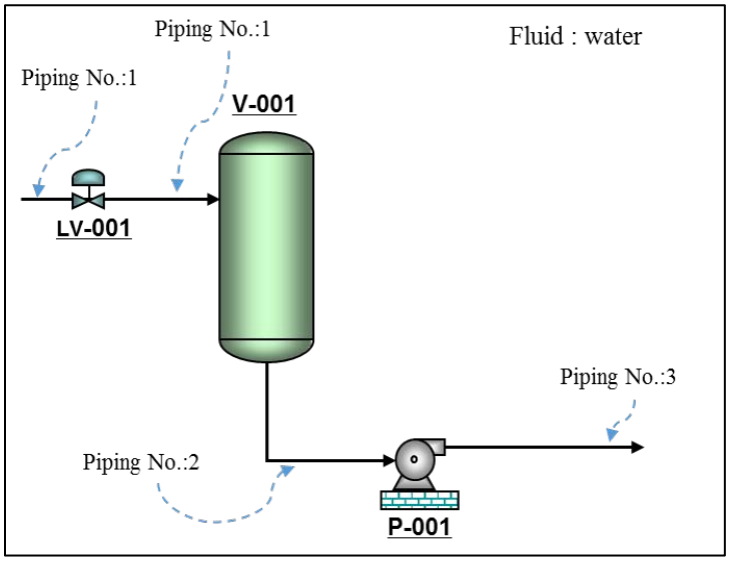


Figure 25. Simple process diagram

Firstly, it is essential to assign pipeline numbers and equipment item tags, as shown in Figure 25. To avoid confusion, simple Arabic numbers are assigned to pipeline numbers, such as 1, 2, and 3, whereas actual pipeline numbers incorporate a variety of information[17]. Then, we can acquire the connection alongside the fluid (or pipeline) direction of the simple diagram in Figure 25: Piping No. 1 →LV-001→ piping No. 1→V-001 → Piping No. 2 → P-001→Piping No. 3. In an actual case study in the next chapter, this connection will be obtained with the aid of SP P&ID® and the SQL language.

4.1.2 Prepopulated worksheet

Once the item tag numbers are marked and their connections are extracted, it is first necessary to select one reference item, here, we use “V-001” for this purpose.

Table 9. Expected HAZOP worksheet from SQL code

	HAZOP (Flow)_No /Less																	
	Ref. EQ	V-001																
Path 1	No.	Possible Causes								Possible Consequences								
		Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check		Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet_other system	check	
	1	Null		1	Water		LV-001			V-001		2		P-001		Null		
Path 2	No.	Possible Causes								Possible Consequences								
		Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check		Ref. EQ	check	Other outlet pipe line	check	Other downstream EQ	check	Outlet other system	check	
	2	2		Water	P-001		Null			V-001		3		-		-		

[17] In general, pipeline numbers include the following details: process unit, process fluid, piping materials and their size, types of insulation, *etc.*

After selecting the reference equipment, it is time to employ the DAHAZID analysis with a prepopulating worksheet, such as shown in Table 9, which is obtained automatically from the SQL code[18]. At this stage, it is necessary to fill in the light yellowish space in Table 9, and its outcome can be Table 10. The purpose of this worksheet is to readily stimulate our imagination regarding whether there are unintended events occurring as a consequence of 1) possible suggested cause items and 2) deviations of process variable, *flow*, for possible causes, such as "*No or Less Flow*."

Table 10. Simple study of the process diagram of Figure 25

HAZOP (Flow)_No /Less

Ref. EQ V-001

	No.	Possible Causes							Possible Consequences							
Path 1		Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet_other system	check
	1	Null	-	1	Water	None	LV-001	NF	V-001	LL	2	N	P-001	NF	Null	-
Path 2	No.	Possible Causes							Possible Consequences							
		Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Ref. EQ	check	Other outlet pipe line	check	Other downstream EQ	check	Outlet other system	check
	2	2	-	Water	P-001	NF (LF)	Null	-	V-001	HL	3	NF	Null	-	Null	-

The abbreviations in Table 10 are NF (No Flow), LL (Low Level), LF (Less Flow) and HL (High Level)

[18] Although this worksheet was prepared by adapting Figure 18, we can modify this worksheet if there is something to improve it. Additionally, Microsoft SQL Server 2012® will be applied to sort the possible cause items into two approaches, option 1 and option 2, in an actual case study. However, the anticipated information is inserted manually this time.

It is necessary here to clarify exactly what is meant by the identification of possible scenarios with *path 1* and *path 2*. Firstly, the inlet line of path 1 in Table 10 consists of two process components, a control valve (LV-001) and pipeline (No. 1), so these components are possible cause items. For instance, there might be some problems with the piping, such as a leak of from piping no. 1, or a failed operation mode of the control valve, LV-001, so either case can have an accidental impact, (e.g., low level) on the vessel. In addition, the anticipated event might influence the downstream equipment, P-001. Similarly, the anticipated process items of path 2 that start from a reference item downstream might result in any impact on the reference equipment or other downstream equipment. Because of the *no/less flow* on the pump, P-001, in Figure 25, the level of the vessel, V-001, is expected to increase due to the unintended event.

4.1.3 Selection of proper safeguards

By making use of CCPS (1998), we can propose safeguards for any equipment failure mode, based on possible scenarios. For example, Table 11 shows the verification of three potential failure scenarios followed by the suggestion of proper safeguards. One of the three failure scenarios is *Low Level* on the vessel, V-003, and the description in Table 3/No.4 at CCPS (1998) corresponds with the failure scenarios.

Table 11. Simple example of HAZOP attribute with safeguards

HAZOP (Flow)_No /Less for Ref. EQ : V-001

No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards 1) Inherently Safer/Passive 2) Active, 3) Procedural
	Inlet Other system	Check	Inlet line	Fluid	check	fault valve	check	Ref. EQ	check	Pipe line	check	EQ	check	Outlet_other system	check		
1	Null	-	1	Water	None	LV-001	NF	V-001	LL	2	N	P-001	NF	Null	-	**V-003 : Low level (LL)_** (T3/No.41) Level control failure	1) Locate underflow nozzle to maintain a min. liquid level in the vessel 2) Low Level Alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve 3) Manual shutoff valve (or by-pass) on low level indication
																P-004 : Low Flow (LF)_ (T8/No.8) Reduced flow to the inlet of a centrifugal pump causing cavitation, excessive vibration and damage to pump seal	1) Eliminate suction system restrictions 2-1) Low flow shutdown interlock 2-2) High vibration (or high speed) shutdown interlock 2-3) Automation recirculation from discharge to suction side on low flow alarm 3) Operator action in response to low flow indication and/or high vibration

No.	Possible Causes							Possible Consequences								Verification Note	Safeguards
	Outlet line	Check	Fluid	EQ	check	fault valve	check	Ref. EQ	check	pipe line	check	EQ	check	Outlet_other system	check		
2	2	-	Water	P-001	NF (LF)	Null	-	V-001	HL	3	NF	Null	-	Null	-	**V-003 : High level (HL)_** (T3/No.37) Over-fill _level control failure causing spill	1-1) Install open overflow nozzle to containment system 1-2) Closed loop filling 1-3) Diking or drainage to remote impounding 2) High level alarm and automatic feed/cutoff/isolation 3) Instruction to stop feed when level reaches a certain point

Verification/ Failure Scenarios	Safeguards 1) Inherently Safer/Passive 2) Active, 3) Procedural
V-003 : Low level (LL)_ (T3/No.41) Level control failure	1) Locate underflow nozzle to maintain a min. liquid level in the vessel (A) 2) Low Level Alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve (B) 3) Manual shutoff valve (or by-pass) on low level indication (C)
P-004 : Low Flow (LF)_ (T8/No.8) Reduced flow to the inlet of a centrifugal pump causing cavitation, excessive vibration and damage to pump seal	1) Eliminate suction system restrictions 2-1) Low flow shutdown interlock 2-2) High vibration (or high speed) shutdown interlock 2-3) Automation recirculation from discharge to suction side on low flow alarm (D) 3) Operator action in response to low flow indication and/or high vibration

Verification Note	Safeguards
V-003 : High level (HL)_ (T3/No.37) Over-fill _level control failure causing spill	1-1) Install open overflow nozzle to containment system (E) 1-1) Install open overflow nozzle to containment system 1-2) Closed loop filling 1-3) Diking or drainage to remote impounding 2) High level alarm and automatic feed/cutoff/isolation (F) 3) Instruction to stop feed when level reaches a certain point

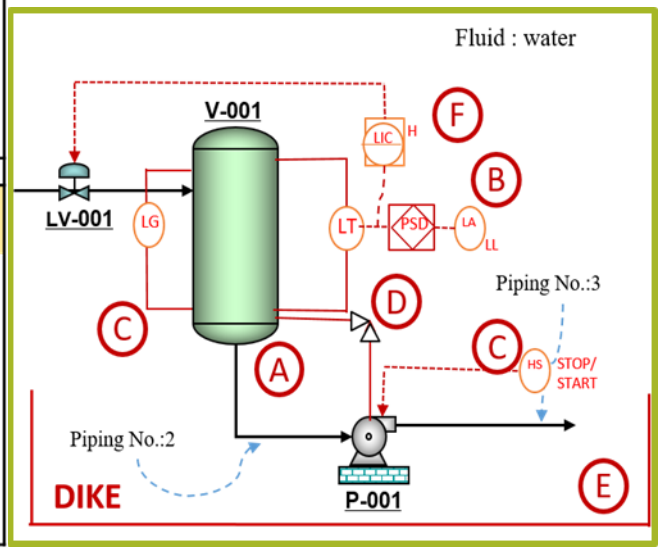


Figure 26. Design safety process devices with safeguards

For the enlarged safeguards in Table 11, Figure 26 shows the types of suggested safeguards and how they might be applied. Of the multiple safeguards, this study selects six recommendations, which are marked A to F and applied to the previous simple diagram.

4.2 Simple case study using FMECA attributes in DAHAZID

To propose the FMECA function, Table 12 shows a simple example, especially focusing on FPFM for which data were borrowed from OREDA (2015). OREDA (2015) shows the reliability data, including the percentage of observed multiple failure modes, so that the possibilities of environmental impacts are also calculated in Table 12. It is based upon probability of environmental impacts if there is an external leakage from process equipment.

Table 12. Simple example of FMECA Attributes

FMECA												
Subsystem : A simple diagram												
Component		Failure Probability Failure Mode [per 10^6 hrs.]					Operating phase	Consequence				Note
Item Tag	Description	Reliability [1)]	Fail to close on demand	Fail to open on demand	Environ.	Human Error		Possible impacts on	Check	Impacts on Environ. [per 10^6 hrs.]	Check	
LV-001	Valves-operated-pneumatic	38.03	-	19.02			All	V-001		-		Based on the calendar time, the mean values of all failure modes are selected.
V-001	Vessel	26.85	-	-			Normal	P-001		-		Based on the calendar time, the mean values of all failure modes are selected.
P-001	Centrifugal pump	114.66	-	-			all phases	other sub-system		-		Based on the calendar time, the mean values of all failure modes are selected.

Reliability data is adopted from OREDA (2015)

4.3 Chapter summary

This chapter presented the progress of the DAHAZID analysis with a simple diagram. The data, included in prepopulated worksheets, were manually filled because the process diagram indeed is simple. However, it is believed that the findings offer insights into the potential of the DAHAZID tool at the initial stage of a project. The following chapter examines an existing process to evaluate the tool's potential after the design stages have been done or even start-up has occurred.

5. BOILER FEED WATER (BFW) SYSTEM CASE STUDY

This chapter presents how to perform a case study for a Boiler Feed Water (BFW) system with the DAHAZID analysis. It might seem that this case study mainly depend HAZOP attributes because of their page length compared to FMECA, but it is important to note that both approaches are indispensable in the DAHAZID method for a more comprehensive identification.

5.1 Process description (BFW system)

At chemical plants, the BFW package was designed to supply adequate BFW with high-quality water without impurities that can cause corrosion. This system consists of three types of equipment: a deaerator, a BFW pump, and a preheater, as shown in Figures 27 and 28. The recovered condensate and demineralized water pass the stripping section of a deaerator, in which they are mixed with low-pressure steam to strip out non-condensable gases from the water. The type of deaerator is a spray tray, and the downstream of the deaerator is dosed with a chemical[19] to prevent BFW corrosion and oxygen scavengers.

[19] This is outside the scope of this study.

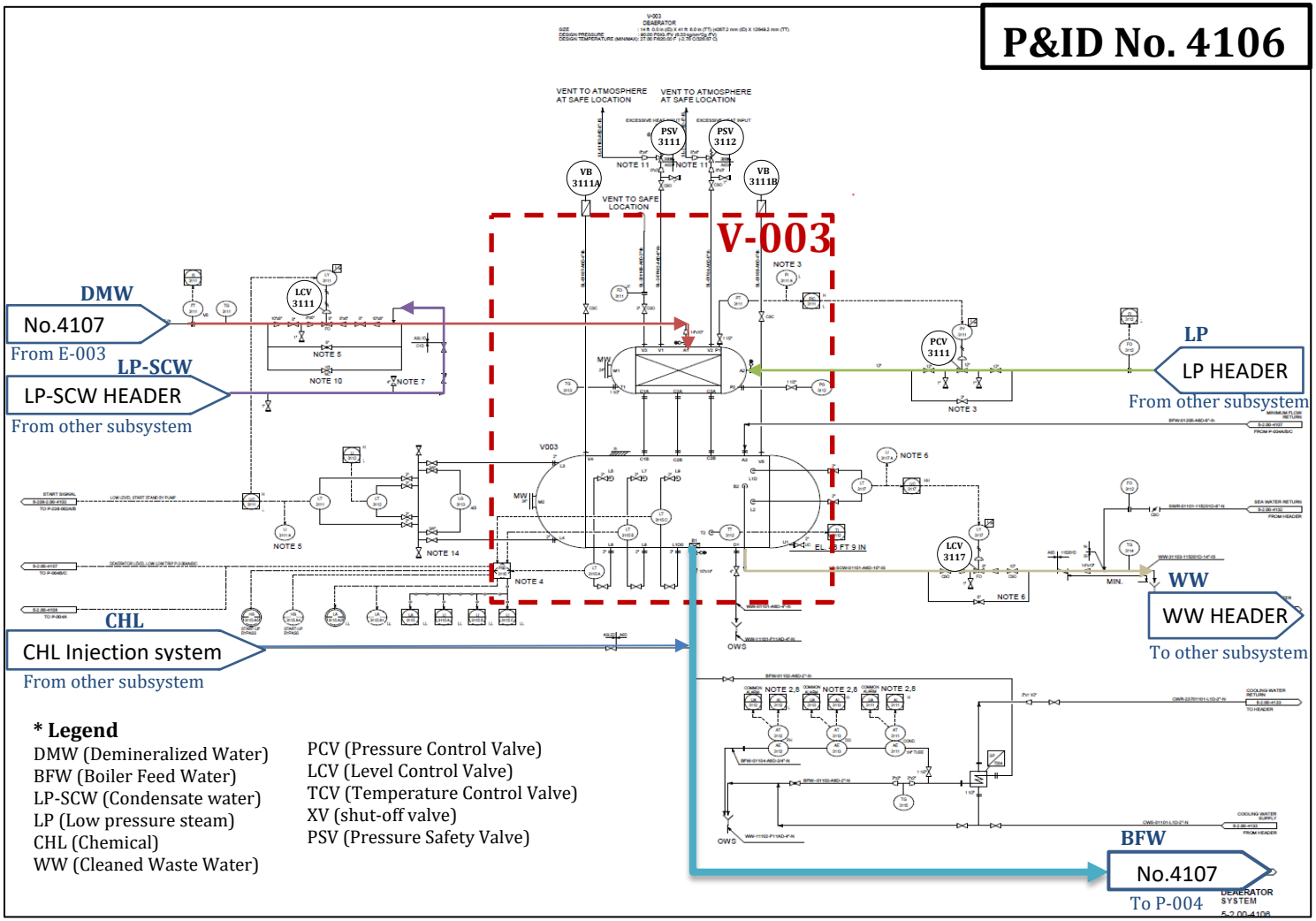


Figure 27. SP P&ID® figure for case study (BFW supply system) (1/2)

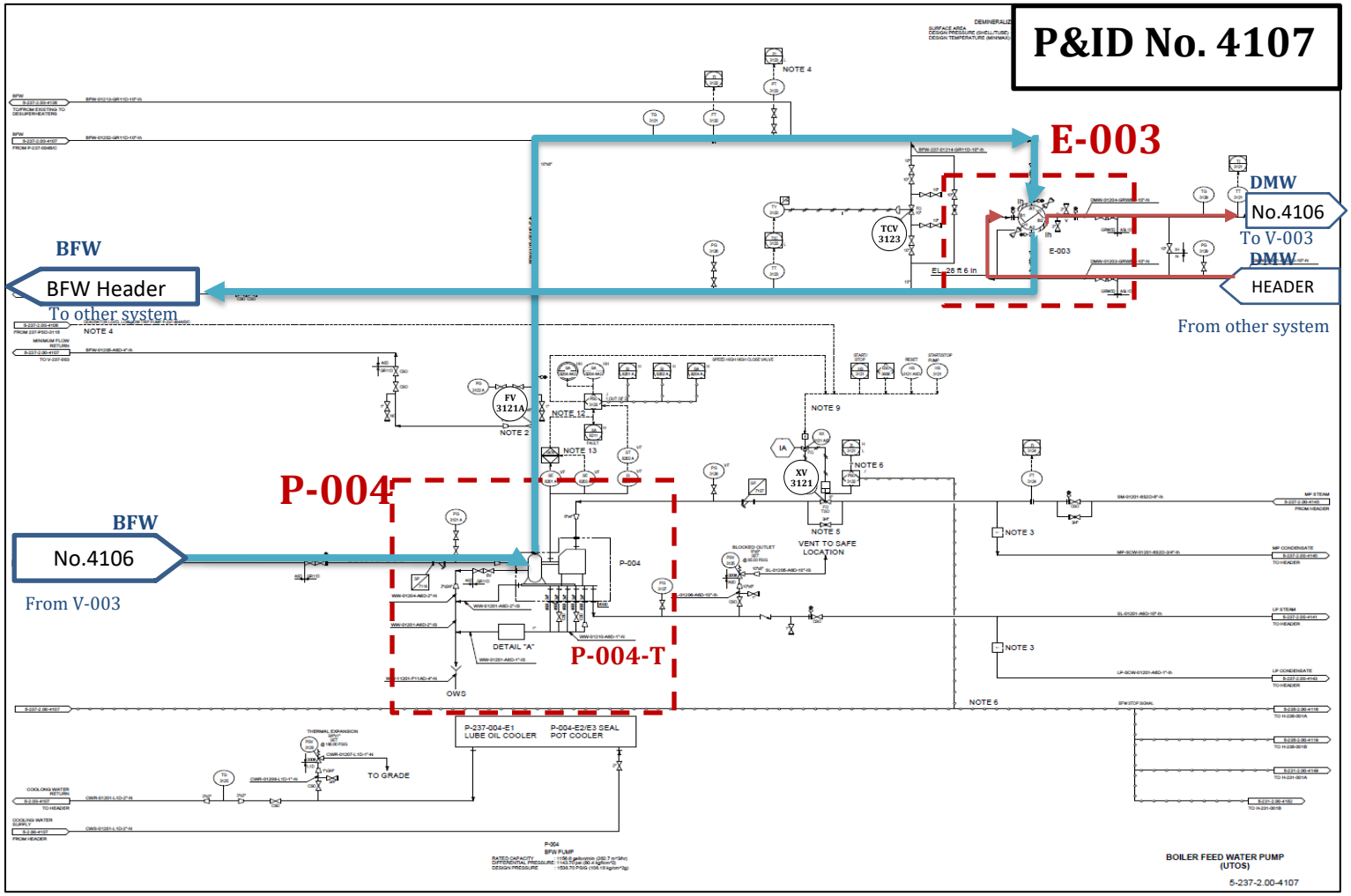


Figure 28. SP P&ID® figure for case study (BFW supply system) (2/2)

5.2 Step 1: Application of HAZOP attributes in DAHAZID

To set up the new HAZID system, a semi-automated preparation stage is needed. Without explanation it might be difficult to understand and follow how the complete preparation stage evolves. Figure 29 serves to elucidate the process with a flowchart taking the current BFW system as an example. In this figure there are three partial preparation step categories: 1) Ref. EQ., 2) Fault Scenarios, and 3) the HAZOP attribute study. *Ref. EQ* means selecting one of the four existing types of equipment as reference equipment (vessel, valve, pump, heat exchanger), *Fault scenarios* means developing proper SQL codes for possible failure scenarios, and *HAZOP attribute study* means preparing prepopulated HAZOP-attribute worksheets. Figure 29 shows that that there are sixteen combinations, so that sixteen worksheets shall be prepared for this case study. For instance, E-003 (of Ref. EQ.) matches with SQL HAZOP-path 1 outcome (of Fault scenarios) and No/Less flow as possible causes (of HAZOP attribute study). This shall be done for all sixteen combinations. This progress is continually maintained until the end of all sixteen combinations.

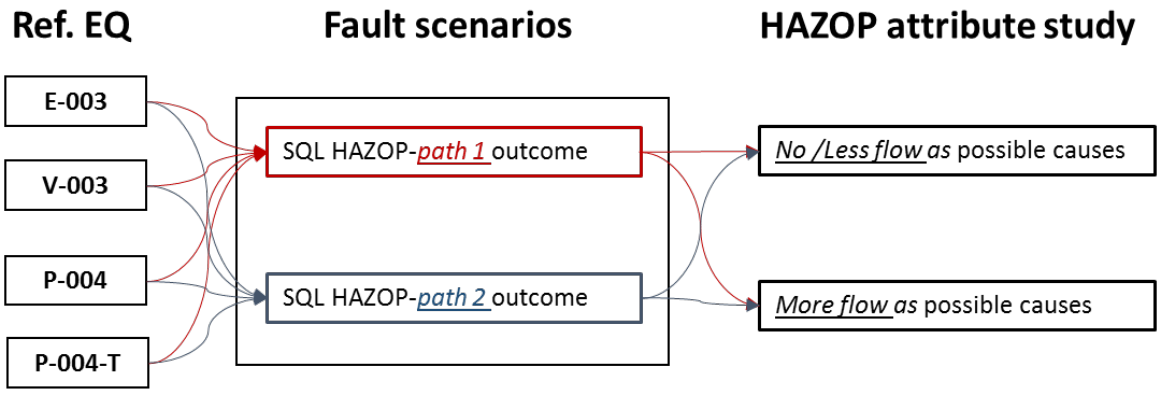


Figure 29. HAZOP-attribute progress for prepopulated worksheet (BFW System)

5.2.1 Case of reference equipment : Heat Exchanger

Once the SQL language codes are ready for HAZOP path 1 and path 2, we can equally and promptly apply these codes to all equipment in the process system. As an example, Figures 30 and 31 represent the current SQL codes and their results for paths 1 and 2, respectively, when the heat exchanger, E-003 in Figure 28, is selected as reference equipment. The other types of equipment will also perform this function in the study on the SQL codes so that we can acquire different corresponding results. Once we input one selected equipment item tag in the system concerned, we can readily encounter equipment or other units that are connected to the selected equipment. Afterward, the outcomes are employed for creating a prepopulated work sheet, such as that presented in Table 13.

Example of the SQL language and its outcomes for HAZOP attributes

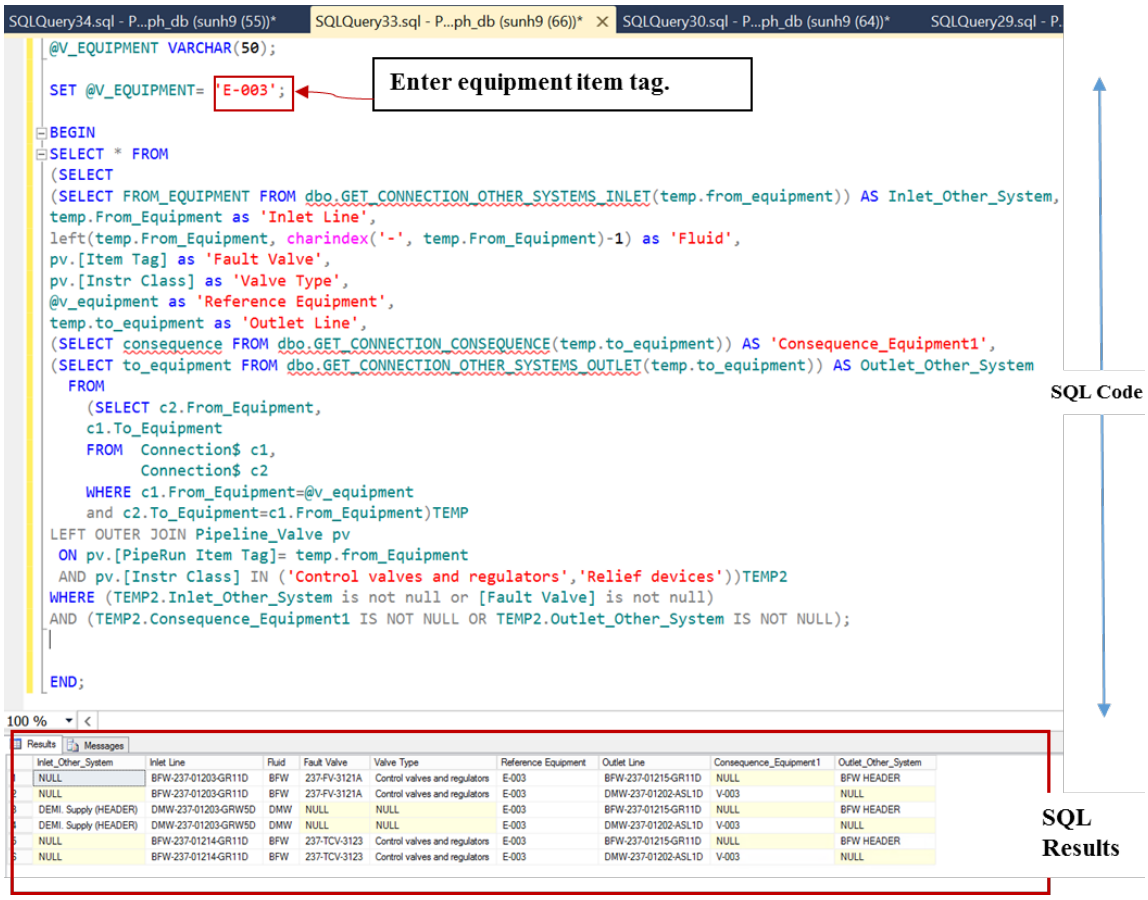


Figure 30. SQL Coding of heat exchanger, E-003, for HAZOP *path 1* and its result

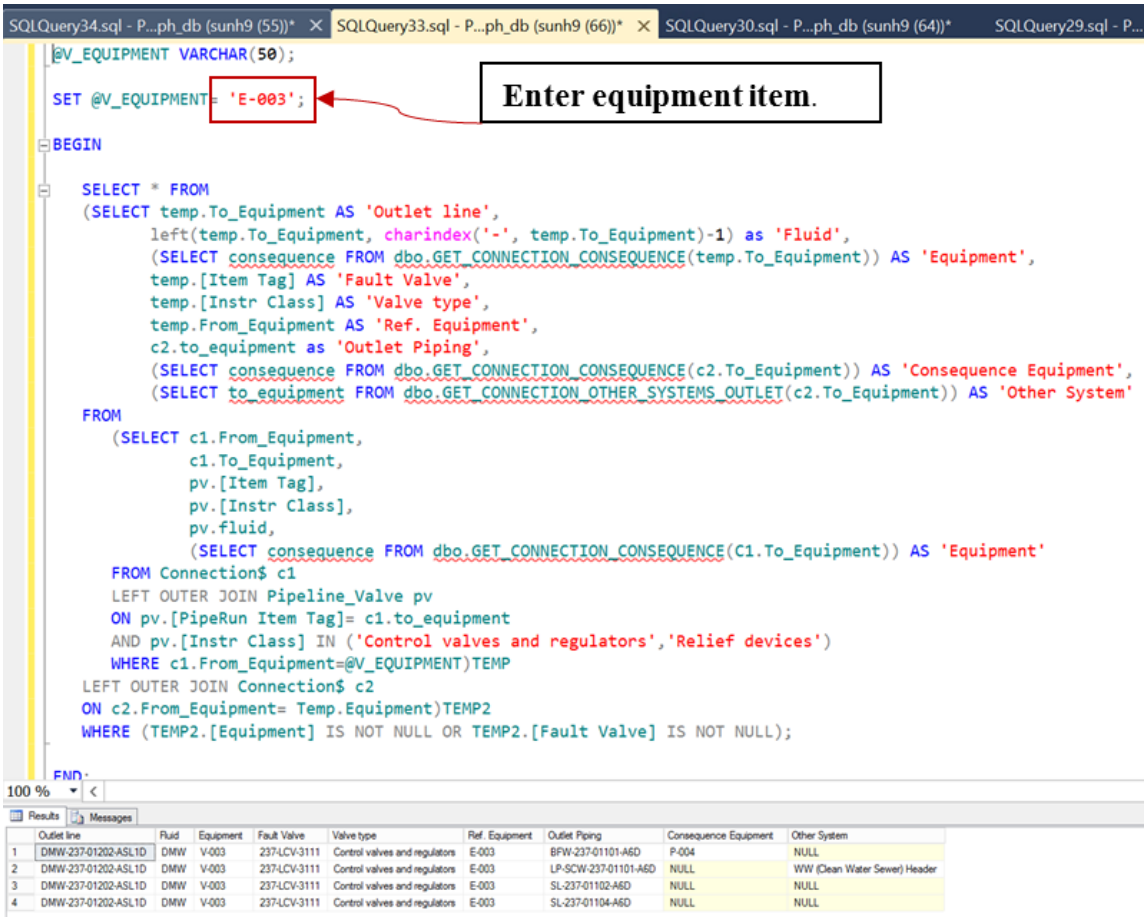
The SQL outcomes for path 1 consist of the following nine types, each represented in an Excel sheet column:

1) **Other inlet system:** Starting from a reference item, if its inlet lines connect with other sub-unit systems, these upstream systems (e.g., HEADER or supply system) are shown in the SQL output. Then, a *possible cause* of unintended process

flowrate events is considered. This step is followed to examine fault-propagated impacts in the concerned system.

2) **Inlet line:** Based on a reference item, its inlet pipeline numbers are extracted to designate the pipeline as a *possible cause* of unintended process flowrate events, e.g., by leakage.
3) **Fluid:** From point 2) inlet line numbers, the fluid type that passes through the pipeline is extracted as a *possible cause* of unintended process flowrate events.
4) **Faulty valve:** Valves on the inlet lines of reference items might disturb the flowrate against the design intention, so faulty valve is regarded as a *possible cause* of unintended process flowrate events.
5) **Valve type:** To review design adequacy, the types of previous point 4) faulty valves are extracted as a *possible cause* of unintended process flowrate events.
6) **Reference equipment**: Following the identification of potential scenarios due to previous possible causes, *possible consequences* (or impacts) on reference equipment can be explored. Regarding possible consequences, the type of process variable to consider, e.g., flow, level, or temperature, is not restricted.
7) **Outlet line:** Similar to point 6) Reference equipment, this is extracted to review the *possible consequences* (or impacts) on outlet lines of the reference equipment.
8) **Downstream equipment**: Similar to point 6) Reference equipment, this is extracted to review the *possible consequences* (or impacts) on equipment downstream of the reference equipment. In other words, this step is followed to examine fault propagation.

9) **Other outlet system:** Similar to point 6) Reference equipment, this is extracted to review the possible consequences (or impacts) on other downstream (sub-) systems that link to the reference equipment. This step is also followed to examine fault propagation to those other downstream systems.




```
@V_EQUIPMENT VARCHAR(50);

SET @V_EQUIPMENT= 'E-003';

BEGIN

   SELECT * FROM
   (SELECT temp.To_Equipment AS 'Outlet line',
          left(temp.To_Equipment, charindex('-', temp.To_Equipment)-1) as 'Fluid',
          (SELECT consequence FROM dbo.GET_CONNECTION_CONSEQUENCE(temp.To_Equipment)) AS 'Equipment',
          temp.[Item Tag] AS 'Fault Valve',
          temp.[Instr Class] AS 'Valve type',
          temp.From_Equipment AS 'Ref. Equipment',
          c2.to_equipment as 'Outlet Piping',
          (SELECT consequence FROM dbo.GET_CONNECTION_CONSEQUENCE(c2.To_Equipment)) AS 'Consequence Equipment',
          (SELECT to_equipment FROM dbo.GET_CONNECTION_OTHER_SYSTEMS_OUTLET(c2.To_Equipment)) AS 'Other System'
   FROM
      (SELECT c1.From_Equipment,
              c1.To_Equipment,
              pv.[Item Tag],
              pv.[Instr Class],
              pv.fluid,
              (SELECT consequence FROM dbo.GET_CONNECTION_CONSEQUENCE(C1.To_Equipment)) AS 'Equipment'
      FROM Connection$ c1
      LEFT OUTER JOIN Pipeline_Valve pv
      ON pv.[PipeRun Item Tag]= c1.to_equipment
      AND pv.[Instr Class] IN ('Control valves and regulators','Relief devices')
      WHERE c1.From_Equipment=@V_EQUIPMENT)TEMP
   LEFT OUTER JOIN Connection$ c2
   ON c2.From_Equipment= Temp.Equipment)TEMP2
   WHERE (TEMP2.[Equipment] IS NOT NULL OR TEMP2.[Fault Valve] IS NOT NULL);

END;
```

	Outlet line	Fluid	Equipment	Fault Valve	Valve type	Ref. Equipment	Outlet Piping	Consequence Equipment	Other System
1	DMW-237-01202-ASL1D	DMW	V-003	237-LCV-3111	Control valves and regulators	E-003	BFW-237-01101-A6D	P-004	NULL
2	DMW-237-01202-ASL1D	DMW	V-003	237-LCV-3111	Control valves and regulators	E-003	LP-SCW-237-01101-A6D	NULL	WW (Clean Water Sewer) Header
3	DMW-237-01202-ASL1D	DMW	V-003	237-LCV-3111	Control valves and regulators	E-003	SL-237-01102-A6D	NULL	NULL
4	DMW-237-01202-ASL1D	DMW	V-003	237-LCV-3111	Control valves and regulators	E-003	SL-237-01104-A6D	NULL	NULL

Figure 31. SQL coding of heat exchanger, E-003, for HAZOP *path 2* and its result

As before in Figure 30, Figure 31 represents how the SQL code retrieves data for HAZOP-path 2[20] in case the heat exchanger, E-003, is a reference item. The SQL outcomes for path 2 consist of the following nine classifications:

1) **Outlet line:** If outlet lines of the reference equipment generate unintended process flowrate events, any undesired consequence could have occurred on the reference equipment. Therefore, outlet line is regarded as *a possible cause item*.
2) **Fluid:** From point 1) outlet line numbers, the fluid type that passes through the pipeline is extracted as a *possible cause* of unintended process flowrate events.
3) **Downstream Equipment:** This represents the equipment downstream of the reference equipment. If downstream equipment generates unintended process flowrate events, any undesired consequences can directly involve the reference equipment. Therefore, equipment is regarded as *a possible cause item*.
4) **Faulty valve:** This represents the downstream control valves of the reference equipment. If unintended process flowrate events occur because of the downstream valves, any undesired consequences can directly involve the reference equipment. Therefore, faulty valve is regarded as *a possible cause item*.
5) **Valve type:** To review design adequacy, the types of valves in outlet lines as in previous point 4) are extracted as a *possible cause* of unintended process flowrate events.

[20] The primary function of the path 2 in the HAZOP attribute is to guide 'backward thinking.'

6) **Reference equipment**: Following the identification of potential scenarios due to previous possible causes, *possible consequences* (or impacts) on reference equipment can be explored. Regarding possible consequences, types of process variables to consider, e.g., flow, level, or temperature, are not restricted.
7) **Other outlet pipe line**: This is extracted to review *possible consequences* (or impacts) on the outlet lines due to events at point 3) equipment (not reference equipment). This column is prepared to analyze further propagated fault impacts.
8) **Other downstream equipment**: This is extracted to review *possible consequences* (or impacts) due to events at point 3) equipment (not reference equipment) on other equipment downstream. This column is prepared to analyze further propagated fault effects on downstream equipment in series linked with the reference piece of equipment.
9) **Other systems:** If other subsystems link to the downstream equipment of point 8), those other systems are extracted to review *possible consequences* (or impacts). As an expected ultimate propagated state, a column would be helpful to guide possible fault propagations.

Conducted HAZOP paths 1 and 2 (Reference EQ: Heat exchanger, E-003)

Following the preparation of prepopulated worksheets as output from previous SQL coding[21], the next step is to conduct an HAZOP-attribute study, as shown in Table 13 (Ref.

[21] The used SQL code listings will be displayed in Appendix D.

EQ: heat exchanger, No/less flow, HAZOP-attribute-path 1 study). Under the “Check” column, the red letters indicate possible causes or consequences associated with undesired failure conditions. Regarding “verification” or “safeguards,” relevant recommendations of these are taken and possibly adapted from CCPS (1998), while the bold letters emphasize the existing safeguards in accordance with the recommended ones. Furthermore, the blue letters show a case where there is room to modify the recommendations from CCPS (1998).

Table 13. (Ref. EQ: heat exchanger, no/less flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_No /Less

Ref. EQ: E-003

Path 1

No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
	Inlet Other system	Check	Inlet line	Fluid	check	fault valve	check	Ref. EQ	check	Pipe line	check	downstream EQ	check	Outlet other system	check		
1	NULL	-	BFW-237-01203-GR11D	BFW	-	237-FV-3121A	None	E-003	None	BFW-237-01215-GR11D	None	NULL	-	BFW HEADER	None	Assumption_ Because of ARV's capacity, the chance of the failure of this ARV is very less regarding blocking its outlet line	-
2	NULL	-	BFW-237-01203-GR11D	BFW	-	237-FV-3121A	None	E-003	None	DMW-237-01202-ASL1D	None	V-003	None	NULL	-	Assumption_ Because of ARV's capacity, the chance of the failure of this ARV is very less regarding blocking its outlet line	-
3	DEMI. Supply (HEADER)	NF (LF)	DMW-237-01203-GRW5D	DMW	NF (LF)	NULL	-	E-003	NF (LF)_ cold (tube)	BFW-237-01215-GR11D	None	NULL	-	BFW HEADER	None	-	-
4	DEMI. Supply (HEADER)	NF (LF)	DMW-237-01203-GRW5D	DMW	NF (LF)	NULL	-	E-003	NF (LF)_ cold (tube)	DMW-237-01202-ASL1D	NF (LF)	V-003	LL	NULL	-	1. V-003 : Low level (LL)_ (T3/No.41) Level control failure	Refer to No.1-1 (HAZOP result of vessel)
5	NULL	-	BFW-237-01214-GR11D	BFW	NF (LF)	237-TCV-3123	NF (LF)	E-003	LP	BFW-237-01215-GR11D	LP	NULL	-	BFW HEADER	LP	1. E-003 : Low Pressure (LP) Adopted from (T3/No.22) Under pressure or Vacuum : Uncontrolled condensation/absorption of vapor phase component_ Active safeguards were deleted	Regarding E-003 1-1) Vessel design to accommodate max. vacuum (full vacuum rating) : **F.V** 1-2) Insulation :**IH** 1-3) Open vent : **Done** 3) Operating procedure for monitoring temperature and addition rate of materials: **TIC-3123(L)** 'Regarding BFW HEADER **The supply header design to accommodate max. vacuum (Full vacuum rating)**

The abbreviations in Table 13 are NF (No Flow), LF (Less Flow), LP (Low pressure), LL (Low Level) BFW (Boiler Feed Water), DMW (Demineralized Water), ARV (Automatic Recirculation Valve), FV (Flowrate Valve), TIC (Temperature Indicate Control), F.V. (Full Vacuum). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 13. Continued

	HAZOP (Flow)_No /Less																	
	Ref. EQ	E-003																
Path 1	No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
		Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	downstream EQ	check	Outlet other system	check		
	6	NULL	-	BFW-237-01214-GR11D	BFW	NF (LF)	237-TCV-3123	NF (LF)	E-003	NF (LF)_ Hot (Shell)	DMW-237-01202-ASL1D	1. LP 2. LT	V-003	1. LP 2. LT	NULL	-	1. V-003: Low Pressure (LP) refer to HAZOP result for Vessel No.3 2. V-003 : Low Temperature (LT) (T3/No.34) Low temperature material fed to vessel	**Regarding V-003** 1) Vessel design to accommodate minimum expected feed temperature 2-1) Low temperature alarm and feed isolation interlock 2-2) Low temperature alarm activates external heating 3) Instructions to isolate feed on low temperature indication
Path 2	No.	Possible Causes							Possible Consequences								Verification Note	Safeguards
		Outlet line	Check	Fluid	downstream EQ	check	faulty valve	check	Ref. EQ	check	Other Outlet pipe line	check	Other downstream EQ	check	Outlet other system	check		
	7	DMW-237-01202-ASL1D	NF (LF)	DMW	V-003	None	237-LCV-3111	NF (LF)	E-003	None	BFW-237-01101-A6D	-	P-004	-	NULL	-	-	
	8	DMW-237-01202-ASL1D	NF (LF)	DMW	V-003	None	237-LCV-3111	NF (LF)	E-003	None	LP-SCW-237-01101-A6D	-	NULL	-	WW (Clean Water Sewer) Header	None	-	

Table 14. (Ref. EQ: heat exchanger, more flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_More

Ref. EQ **E-003**

Path 1

No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	downstream EQ	check	Outlet other system	check		
9	NULL	-	BFW-237-01203-GR11D	BFW	None	237-FV-3121A	None	E-003	None	BFW-237-01215-GR11D	None	NULL	-	BFW HEADER	None		
10	NULL	-	BFW-237-01203-GR11D	BFW	None	237-FV-3121A	None	E-003	None	DMW-237-01202-ASL1D	None	V-003	None	NULL	None		
11	DEMI. Supply (HEADER)	MF	DMW-237-01203-GRW5D	DMW	MF	NULL	-	E-003	None	BFW-237-01215-GR11D	None	NULL	-	BFW HEADER	None	Check : The capacity of E-003 is enough to cover max.flow of DMW	
12	DEMI. Supply (HEADER)	MF	DMW-237-01203-GRW5D	DMW	MF	NULL	-	E-003	None	DMW-237-01202-ASL1D	None	V-003	None	NULL	-	Check : The capacity of V-003 is enough to cover max.flow of DMW (in order to separate Oxygen content)	

Path 2

No.	Possible Causes							Possible Consequences								Verification Note	Safeguards
	Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Ref. EQ	check	Other outlet pipe line	check	other downstream EQ	check	Outlet other system	check		
13	DMW-237-01202-ASL1D	None	DMW	V-003	None	237-LCV-3111	None	E-003	None	BFW-237-01101-A6D	None	P-004	None	NULL	-		
14	DMW-237-01202-ASL1D	None	DMW	V-003	None	237-LCV-3111	None	E-003	None	LP-SCW-237-01101-A6D	None	NULL	-	WW (Clean Water Sewer) Header	None		

The abbreviations in Table 14 are MF (More Flow), FV (Flowrate Valve), and LCV (Level Control Valve).

5.2.2 Case of reference equipment : Vessel

The method for a vessel is identical to the previous approach. Although this chapter introduces the case for a vessel as a second item, it is recommended that vessels (or reactors) are reviewed first. This is because they are mostly connected with other rotating equipment (e.g., pumps or compressors) and associated with rather complex processes that require consideration of various factors. For this reason, the possible scenarios and safeguards of vessels are nearly all associated with other equipment or systems, so the case where vessels are selected first helps to prevent same tasks from being repeated.

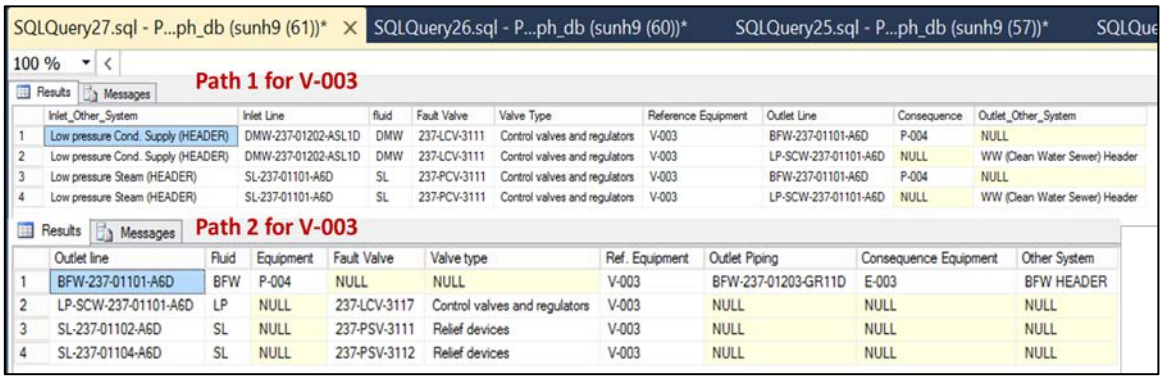


Figure 32. SQL results of vessel, V-003, for HAZOP

Table 15. (Ref. EQ: vessel, no/less flow) HAZOP-attribute-path 1

HAZOP (Flow)_No /Less_Path 1

Ref. EQ V-003

No.	Possible Cause							Possible Consequence								Verification/ Failure Scenarios	Safeguards 1	Safeguards 2
	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	downstream EQ	check	Outlet Other system	check			
1	Low pressure Cond. Supply (HEADER)	NF (LF)	DMW-237-01202-ASL1D	DMW	NF (LF)	237-LCV-3111	None	V-003	None	BFW-237-01101-A6D	None	P-004	None	NULL	-	Assumption_DWM is enough to feed for this BFW system 1. V-003 (T3/No.45) Low of containment_Corrosion from process fluid, DMW (Demineralized Water)	**Regarding V-003** 1-1) Use corrosion resistant materials of construction 1-2) Protective coatings and paints 1-3) Double walled tank design 2) Automatic addition of corrosion inhibitor : **Deaerator chemical injection system (ME-007)** 3-1) Corrosion coupons with periodic withdrawal and analysis : **Manual Sampling (SP-7204)** 3-2) Regular thickness measurements at key points 3-3) On-line corrosion analysis with alarm: **AAH-3111(for Conductivity), AAL-3112 (for PH), and AAH-3113 (for DO)**	
1-1	Low pressure Cond. Supply (HEADER)	None	DMW-237-01202-ASL1D	DMW	NF (LF)	237-LCV-3111	NF (LF)	V-003	LL	BFW-237-01101-A6D	LF	P-004	LF	NULL	-	1) V-003 : Low level (LL)_ (T3/No.41) Level control failure 2) P-004 : Low Flow (LF)_ (T8/No.8) Reduced flow to the inlet of a centrifugal pump causing cavitation, excessive vibration and damage to pump seal	**Regarding V-003** 1) Locate underflow nozzle to maintain a min. liquid level in the vessel 2) Low Level Alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve : **LALL-3155, LAL-3112, LAL-3111** 3) Manual shutoff valve **(or by-pass)** on low level indication : **Manual bass-pass valve of LCV-3111, LI-3111**	**Regarding P-004** 1) Eliminate suction system restrictions 2-1) Low flow shutdown interlock: **PSD-3115 (DEAERATOR LEVEL LOW LOW TRIP P-237-004)** 2-2) High vibration (**or high speed**) shutdown interlock : 2-3) Automation recirculation from discharge to suction side on low flow alarm : **FV-3121** 3) Operator action in response to low flow indication and/or high vibration
2	Low pressure Cond. Supply (HEADER)	None	DMW-237-01202-ASL1D	DMW	None	237-LCV-3111	NF (LF)	V-003	LL	LP-SCW-237-01101-A6D	None	NULL	-	WW (Clean water Sewer) Header	None	Refer to No.1-1 regarding V-003	Refer to No.1-1	None _ LP-SCW line is not a primary line for this process. (just for a drain purpose)

The abbreviations in Tables 15 are NF (No Flow), LF (Less Flow), LP (Low pressure), LL (Low Level) ME (Mechanical Sensor), LAL (Level Alarm Low) LALL (Level Alarm Low Low) LI (Level Indicator), LP-SCW(Condensate Low Pressure Clean) SP (Safety Point), PSD (Pressure Shutdown) AAH (Analysis Alarm High), AAL (Analysis Alarm Low), WC (Wrong Composition). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 15. Continued

HAZOP (Flow)_No /Less_Path 1

Ref. EQ V-003

No.	Possible Cause							Possible Consequence								Verification/ Failure Scenarios	Safeguards 1	Safeguards 2
	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet Other system	check			
3	Low pressure Steam (HEADER)	NF (LF)	SL-237-01101-A6D	SL	NF (LF)	237-PCV-3111	None	V-003	LP	BFW-237-D1101-A6D	None	P-004	None	NULL	-	1) V-003 : Low Pressure (LP)_ (T3/No.22) Under pressure or Vacuum : Uncontrolled condensation/ absorption of vapor phase component	**Regarding V-003** 1-1) Vessel design to accommodate max. vacuum (full vacuum rating) : **its design value is F.V** 1-2) Insulation **:IH** 1-3) Open vent : **Done** 2-1) Use of blanketing gas pressure control system to min. vacuum - **not necessary because is not flammable.** 2-2) Vacuum relief system : **VB-3111A/VB-3111B/FO-3111 (Vent)** 2-3) Feed heater : **Preheater E-003** 3) Operating procedure for monitoring temperature and addition rate of materials : **TG-3113/PAL-3111A**	-
3-1	Low pressure Steam (HEADER)	None	SL-237-01101-A6D	SL	NF (LF)	237-PCV-3111	NF (LF)	V-003	1. LP 2. WC	BFW-237-D1101-A6D	None	P-004	None	NULL	-	1. V-003: Wrong composition (T5/No.17) Insufficient or excessive fractionation leading to compositions outside of metallurgical limits (e.g. Corrosion) 2. Refer to No. 3 (for under pressure)	**2. Regarding V-003 (Wrong composition)** 1) Select metallurgy suitable for worst case composition : **A6D** 2)On-line measurement (e.g., corrosion probes, stream analysis, temperature) and automatic operating adjustment: **AAH-3113 (DO), AAL-3112 (PH), AAH-3111 (Conductivity), FAL-3112, PAL-3111** 3) On-line measurement (e.g. Corrosion probes, stream analysis, temperature) and manual operating adjustment :**Manual sampling (SP-7204) , Manual Bypass valve of PCV-3111, PI-311A**	1. refer to No. 3 Regarding under pressure
4	Low pressure Steam (HEADER)	None	SL-237-01101-A6D	SL	NF (LF)	237-PCV-3111	NF (LF)	V-003	LP	LP-SCW-237-D1101-A6D	-	NULL	-	WW (Clean water Sewer) Header	None	The same with No. 3 None _ LP-SCW line is not a primary line for this process. (just for a drain purpose)	The same with No. 3	-

Table 16. (Ref. EQ: vessel, no/less flow) HAZOP-attribute-path 2

Path 2

HAZOP (Flow)_No /Less																	
	Possible Causes							Possible Consequences								Verification Note	Safeguards
No.	Outlet line	Check	Fluid	Downstream EQ	check	fault valve	check	Ref. EQ	check	other outlet pipe line	Check	Other downstream EQ	Check	Outlet other system	Check		
5	BFW-237-01101-A6D	NF (LF)	BFW	P-004	NF (LF)	NULL	-	V-003	HL	BFW-237-01203-GR11D	NF (LF)	E-003	No (low) supply	BFW HEADER	No (low) supply	1) V-003 : High level (HL)_ (T3/No.37) Over-fill _level control failure causing spill 2) E-003 : Low Temperature (LT)_ No impact expected for physical problems	**Regarding V-003** 1-1) Install open overflow nozzle to containment system 1-2) Closed loop filling 1-3) Diking or drainage to remote impounding 2) High level alarm and automatic feed/cutoff/isolation **:LAHH-3117-automatic drain line to a sewer line, LAH-3111- automatic feed cutoff with LCV-3111** 3) Instruction to stop feed when level reaches a certain point **: with LAH-3112, proper procedure should be provided** **Regarding E-003** No action needed **Regarding BFW HEADER** 1) Making up with other BFW supply line of existing facilities : **BFW-237-01213-GR11D-10"-lh**
6	LP-SCW-237-01101-A6D	NF (LF)	LP	NULL	-	237-LCV-3117	NF (LF)	V-003	HL	NULL	-	NULL	-	NULL	-	Drain line is block-> V-003 : High level (HL) (T3/No.37) Over-fill _level control failure causing spill -> Refer to No. 5	**Regarding V-003** Refer to No. 5
7	SL-237-01102-A6D	NF (LF)	SL	NULL	-	237-PSV-3111	NF (LF)	V-003	HT	NULL	-	NULL	None	VENT TO ATMOSPHERE	None	Because PSV-3111 is installed in case of excessive heat, the temp. of V-003 can be increased when the PSV does not work properly.	**There is the redundant PSV : PSV-3112**
8	SL-237-01104-A6D	NF (LF)	SL	NULL	-	237-PSV-3112	NF (LF)	V-003	HT	NULL	-	NULL	None	VENT TO ATMOSPHERE	None	Because PSV-3112 is installed in case of excessive heat, the temp. of V-003 can be increased when the PSV does not work properly.	**There is the redundant PSV : PSV-3111**

The abbreviations in Table 16 are NF (No Flow), LF (Less Flow), LP (Low pressure), HL (High Level), LAL (Level Alarm Low), LALL (Level Alarm Low Low) LCV (Level Control Valve), and HT (High Temperature). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 17. (Ref. EQ: vessel, more flow) HAZOP-attribute-paths 1 & 2

Path 1

HAZOP (Flow)_More

Ref. EQ **V-003**

No.	Possible Cause							Possible Consequence								Verification/ Failure Scenarios	Safeguards
	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet other System	check		
9	Low pressure Cond. Supply (HEADER)	MF	DMW-237-01202-ASL1D	DMW	MF	237-LCV-3111	-	V-003	HL	BFW-237-01101-A6D	None	P-004	None	NULL	-	Refer to No. 5	
9-1	Low pressure Cond. Supply (HEADER)	None	DMW-237-01202-ASL1D	DMW	MF	237-LCV-3111	MF	V-003	1. HL 2. Wrong composition	BFW-237-01101-A6D	None	P-004	None	NULL	-	1. V-003 : High level (HL)_ (T3/No.37) Over-fill _level control failure causing spill->Refer to No. 5 2. V-003: wrong component (T5/No.17) Insufficient or excessive fractionation leading to compositions outside of metallurgical limits (e.g. Corrosion) ->Refer to No.3-1	-
10	Low pressure Cond. Supply (HEADER)	MF	DMW-237-01202-ASL1D	DMW	MF	237-LCV-3111	-	V-003	HL	LP-SCW-237-01101-A6D	None	NULL	None	WW (Clean water Sewer) Header	None	Refer to No. 5	

The abbreviations in Table 17 are MF (More Flow) and HL (High Level). The abbreviations in Table 20 are MF (More Flow), HL (High Level), HP (High Pressure), PCV (Pressure Control Valve), FO (Flow Orifice), PSV (Pressure Safety Valve), and PAH (Pressure Alarm High). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 17. Continued

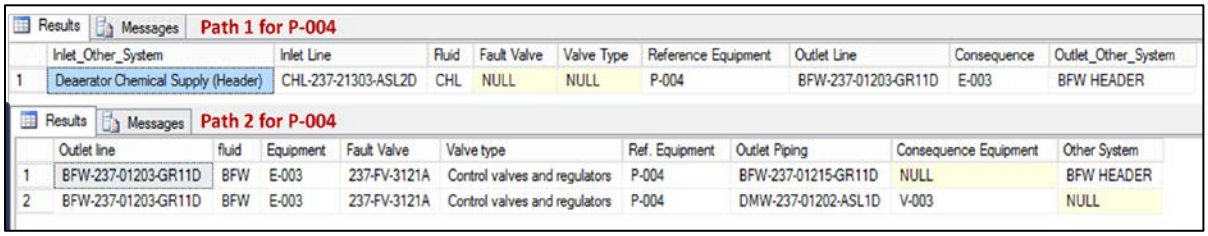
HAZOP (Flow)_More

Ref. EQ **V-003**

No.	Possible Cause: Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Possible Consequence: Ref. EQ	check	Pipe line	check	downstream EQ	check	Outlet other System	check	Verification/ Failure Scenarios	Safeguards 1	Safeguards 2
11	Low pressure Steam (HEADER)	-	SL-237-01101-A6D	SL	MF	237-PCV-3111	MF	V-003	1. HL 2.HP	BFW-237-01101-A6D	None	P-004	None	NULL	-	1. V-003 : High Level (HL) Modified No.5 2. V-003 : High pressure (HP)_ (T3/No.13) Overpressure Failure of upstream process controls, resulting in vapor or flashing liquid feed	**Regarding V-003 (High Level)** 2) High level alarm and automatic feed/cutoff/isolation **: (Recommended)** 3) Instruction to stop feed when level reaches a certain point **: with LAH-3112 , proper procedure should be provided**	**Regarding V-003 (for over pressure)** 1-1) Vessel design accommodating maximum expected or upstream pressure 1-2) Ensure control valves are not oversized **: Check the size of PCV-3111** 2-1) Emergency relief device **: PSV-3111/ PSV-3112, FO-3111 (vent)** 2-2) High pressure alarm and interlock which isolates the inlet flow(s) **:PAH-3111** 3) Operator activation of flow isolation on high pressure indication:
12	Low pressure Steam (HEADER)	-	SL-237-01101-A6D	SL	MF	237-PCV-3111	MF	V-003	HP	LP-SCW-237-01101-A6D	None	NULL	None	WW (Clean water Sewer) Header	None	Refer to No. 11 Wasted stream	Refer to No. 11	

No.	Possible Causes: Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Possible Consequences: Ref. EQ	check	Outlet piping	check	Other downstream EQ	Check	Outlet other System	Check	Verification Note	Safeguards 1	Safeguards 2
13	BFW-237-01101-A6D	-	BFW	P-004	-	NULL	-	V-003	None	BFW-237-01203-GR11D	None	E-003	None	BFW HEADER	None	-		
14	LP-SCW-237-01101-A6D	MF	LP	NULL	MF	237-LCV-3117	Mf	V-003	1. LL 2. LP	NULL	-	NULL	-	NULL	-	1. V-003 Low Level (LL) Refer to No.1-1 2. V-003 Low pressure (LP) Refer to No. 3		

5.2.3 Case of reference equipment : Pump



Results | Messages | Path 1 for P-004

	Inlet_Other_System	Inlet Line	Fluid	Fault Valve	Valve Type	Reference Equipment	Outlet Line	Consequence	Outlet_Other_System
1	Deaerator Chemical Supply (Header)	CHL-237-21303-ASL2D	CHL	NULL	NULL	P-004	BFW-237-01203-GR11D	E-003	BFW HEADER

Results | Messages | Path 2 for P-004

	Outlet line	fluid	Equipment	Fault Valve	Valve type	Ref. Equipment	Outlet Piping	Consequence Equipment	Other System
1	BFW-237-01203-GR11D	BFW	E-003	237-FV-3121A	Control valves and regulators	P-004	BFW-237-01215-GR11D	NULL	BFW HEADER
2	BFW-237-01203-GR11D	BFW	E-003	237-FV-3121A	Control valves and regulators	P-004	DMW-237-01202-ASL1D	V-003	NULL

Figure 33. SQL results of pump, P-004, for HAZOP

This section has an exclusive case study for a pump, except for the pump turbine, the case study of which will follow.

Table 18. (Ref. EQ: pump, no/less flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_No /Less

Ref. EQ **P-004**

Path 1

No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet other system	check		
1	Deaerator Chemical Supply (Header)	NF (LF)	CHL-237-21303-ASL2D	CHL	NF (LF)	NULL	-	P-004	corrosion	BFW-237-01203-GR11D	corrosion	E-003	corrosion	BFW HEADER	corrosion	**The function of this chemical injection line is to feed one corrosion inhibitor.** So, corrosive fluid can be fed into outlet lines without proper chemical injection -> **(Additional one to T12/No.22) Wrong composition_No proper Injection**	**Regarding V-003** **1) Use resistant materials of construction for the worst case** **2) Automatic shutoff downstream (recommendation)** **3-1) Sample with periodic withdrawal and analysis : Manual Sampling (SP-7204), pump inlet line (SP-7116)** **3-2) On-line corrosion analysis with alarm: AAH-3111(for Conductivity), AAL-3112 (for PH), and AAH-3113 (for DO)**

Path 2

No.	Possible Causes							Possible Consequences								Verification Note	Safeguards
	Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Ref. EQ	check	Other outlet pipe line	check	Other downstream EQ	check	Outlet other system	check		
2	BFW-237-01203-GR11D	NF (LF)	BFW	E-003	NF (LF)	237-FV-3121A	None	P-004	None	BFW-237-01215-GR11D	NF (LF)	NULL	-	BFW HEADER	NF (LF)	Assumption _There is no case to block the main stream because of ARV (FV- 3121A) fault	**Regarding BFW HEADER** Refer to Vessel HAZOP No.5
3	BFW-237-01203-GR11D	NF (LF)	BFW	E-003	NF (LF)	237-FV-3121A	None	P-004	None	DMW-237-01202-ASL1D	MF	V-003	HL	NULL	-		**Regarding V-003** Refer to Vessel HAZOP No.5

The abbreviations in Table 18 are NF (No Flow), SP (Safety Point), AAH (Analysis Alarm High), and AAL (Analysis Alarm Low). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 19. (Ref. EQ: pump, more flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_More

Ref. EQ **P-004**

Path	No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
		Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet other system	check		
Path 1	4	Deaerator Chemical Supply (Header)	MF	CHL-237-21303-ASL2D	CHL	MF	NULL	-	P-004	None	BFW-237-01203-GR11D	None	E-003	None	BFW HEADER	None		
		Possible Causes							**Possible Consequences**								**Verification Note**	**Safeguards**
	No.	**Outlet line**	**Check**	**Fluid**	**Downstream EQ**	**check**	**faulty valve**	**check**	**Ref. EQ**	**check**	**Other outlet pipe line**	**check**	**Other downstream EQ**	**check**	**Outlet other system**	**check**		
Path 2	5	BFW-237-01203-GR11D	None	BFW	E-003	None	237-FV-3121A	None	P-004	None	BFW-237-01215-GR11D	None	NULL	-	BFW HEADER	None		
	6	BFW-237-01203-GR11D	None	BFW	E-003	None	237-FV-3121A	None	P-004	None	DMW-237-01202-ASL1D	-	V-003	None	NULL			

The abbreviation in Table 19 is MF (More Flow).

5.2.4 Case of reference equipment : Pump Turbine

Results | Messages — Path 1 for P-004-T

	Inlet_Other_System	Inlet Line	fluid	Fault Valve	Valve Type	Reference Equipment	Outlet Line	Consequence	Outlet_Other_System
1	MP steam supply (HEADER)	SM-237-01201-6S2D	SM	237-XV-3121	Control valves and regulators	P-004-T	SL-237-01201-A6D	NULL	LP Steam Return (HEADER)

Results | Messages — Path 2 for P-004-T

	Outlet line	fluid	Equipment	Fault Valve	Valve type	Ref. Equipment	Outlet Piping	Consequence Equipment	Other System
1	SL-237-01201-A6D	SL	NULL	237-PSV-3125	Relief devices	P-004-T	NULL	NULL	NULL

Figure 34. SQL results of pump turbine, P-004-T, for HAZOP

Table 20. (Ref. EQ: pump turbine, no/less flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_No /Less

Ref. EQ **P-004-T** Steam Turbine

	No.	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
		Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet other system	check		
Path 1	1	MP steam supply (HEADER)	NF (LF)	SM-237-01201-6S2D	SM	NF (LF)	237-XV-3121	-	P-004-T	Stop	SL-237-01201-A6D	NF (LF)	NULL	-	LP Steam Return (HEADER)	NF (LF)	1) P-004-T (centrifugal compressor) : Low Flow->Stop -> No supply BFW 2) LP steam Return : Low Flow -> No impact	Regarding P-004-T 1) Install spare pumps : Motor driven compressor (Spare), STAND BY PUMP, P-237-004A,B or C. 2-1) Automatic change : PAL-3123 (PSD-3115 STOPS P-237-004C AND A/B BY CLOSE OF XV-3122/3121. PAL-3123 STARTS ANY OF) 2-2) Monitoring to action in response to low flow or pressure indication : FI-3124, HS-3121 -> FAL-3124 (recommendation) 3) Operator action in response to low flow or pressure indication : PG-3126, START/STOP PUMP with HS-3121 (manual)
	1-1	MP steam supply (HEADER)	-	SM-237-01201-6S2D	SM	NF (LF)	237-XV-3121	NF (LF)	P-004-T	Stop	SL-237-01201-A6D	NF (LF)	NULL	-	LP Steam Return (HEADER)	NF (LF)		

	No.	Possible Causes							Possible Consequences								Verification Note	Safeguards
		Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Ref. EQ	check	Other outlet pipe line	check	Other downstream EQ	check	Outlet other system	check		
Path 2	2	SL-237-01201-A6D	NF (LF)	SL	NULL	-	237-PSV-3125	NF (LF)	P-004-T	Over speed	NULL	-	NULL	-	NULL	-	1) P-004-T : Over speed (T8/No.12) Compressor over speed leading to equipment damage due to speed control system failure and loss of containment	Regarding P-004-T 1) Use solid versus built-up rotor 2) High speed alarm and compressor over speed shutdown system : PSD-3123 (for high speed)

The abbreviations in Table 20 are NF (No Flow), SP (Safety Point), AAH (Analysis Alarm High), and AAL (Analysis Alarm Low). Regarding safeguards, different types of safeguards were assigned with different numbers: 1) Inherently Safer/Passive, 2) Active, and 3) Procedural.

Table 21. (Ref. EQ: pump turbine, more flow) HAZOP-attribute-paths 1 & 2

HAZOP (Flow)_More

Ref. EQ P-004-T

Path 1	Possible Causes							Possible Consequences								Verification/ Failure Scenarios	Safeguards
No.	Inlet Other system	Check	Inlet line	Fluid	check	faulty valve	check	Ref. EQ	check	Pipe line	check	Downstream EQ	check	Outlet other system	check		
4	MP steam supply (HEADER)	None	SM-237-01201-6S2D	SM	None	237-XV-3121	None	P-004-T	None	SL-237-01201-A6D	None	NULL	None	LP Steam Return (HEADER)	None	-	

Path 2	Possible Causes							Possible Consequences								Verification Note	Safeguards
No.	Outlet line	Check	Fluid	Downstream EQ	check	faulty valve	check	Ref. EQ	check	Other outlet pipe line	check	Other downstream EQ	check	Outlet other system	check		
5	SL-237-01201-A6D	None	SL	NULL	None	237-PSV-3125	-	P-004-T		NULL	-	NULL	-	NULL	-	-	

The abbreviations in Table 21 are SM (Steam Medium Pressure), and SL (Steam Low Pressure).

5.3 Step 2: Application of FMECA attributes in DAHAZID

The FMECA attributes in the DAHAZID analysis require two types of data; 1) process design data by using SQL code with an EXCEL file that was made with SP P&ID® and 2) FPFM data from reliable data sources.

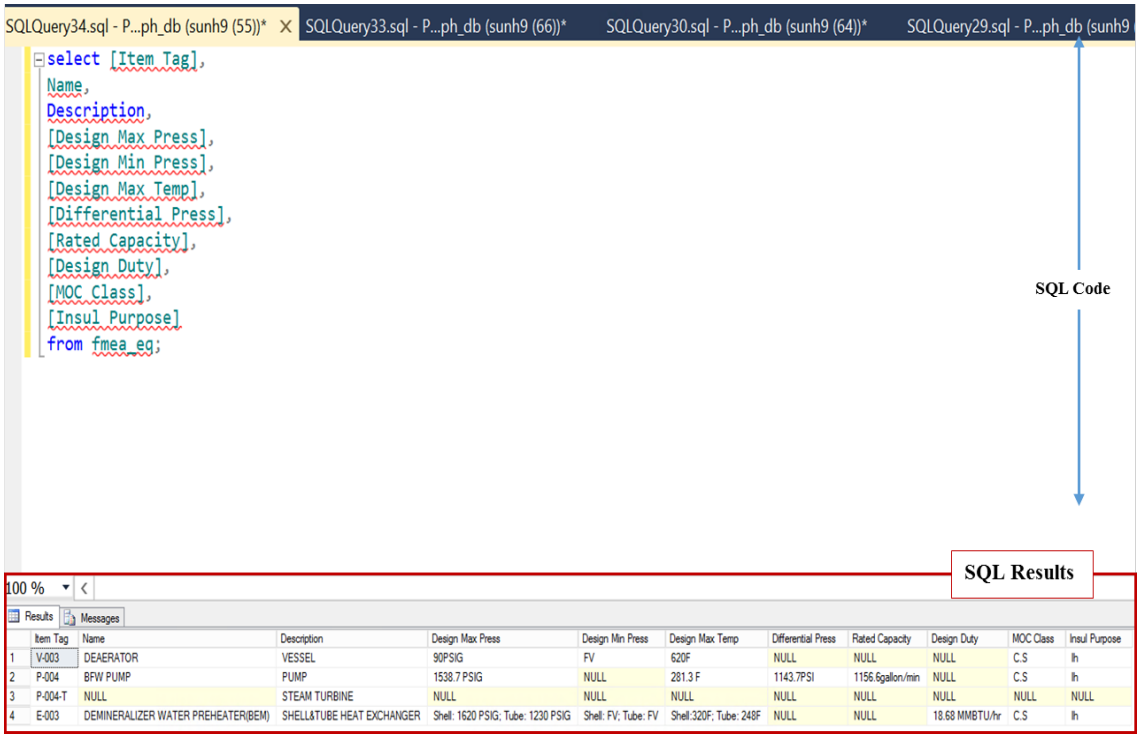


Figure 35. SQL code for FMECA (extraction of data of interest)

The SQL results in Figure 35 show the process design conditions of this BFW system. At this stage, the primary design values are retrieved (design pressures, temperatures, and design duty, etc.) because HAZID-engineers will determine whether proper designs have

been proposed based on this information. Consequently, the process data are integrated with the FPFM data, as shown in Table 22. For reference, the used SQL coding will be displayed clearly in Appendix E.

Table 22. FMECA-attribute case study in DAHAZID for EQ

FMECA

Subsystem : **BFW system**

Component		Process Conditions			Failure Probability Failure Mode			Operating phase	Consequence				Note
Item Tag	Descrip -tion	Design Pressure [PSIG]	Design Tem. [F]	Check	Reliability [per 10^6 hrs]	Environ.	Human Error		Possible impacts on	Check	Impacts on Environ. [per 10^6 hrs.]	Check	
V-003	Vessel	FV / 90	620		26.85			Normal	P-004	V-001	-		Stripper
P-004	Pump	1538.7	281.3		114.66			Normal	E-003		24.54		
P-004-T	Steam Turbine	-	-		96.93			Normal	BFW supply		5.32		
E-003	Demi. water preheater	Shell : FV / 1620 Tube : FV / 1230	Shell : 320 Tube : 248		76.03			Normal	BFW supply		38.01		

Reliability data are adopted from OREDA (2015). It does not mean that the quoted values will be the ones for the current case under specified conditions. Moreover, reliability values will show spread from one equipment item to another. Therefore in case of a later, more detailed quantitative risk analysis, estimated uncertainties will be included.

Table 23. FMECA-attribute case study in new HAZID for valves

FMECA

Subsystem : BFW system (for control valves)

Component		Process Conditions				Failure Probability Failure Mode				Operating phase	Consequence				Note
Item Tag	Description	Design Pressure [PSIG]	Design Tem. [F]	Fluid	Check	Reliability [1] [per 10^6 hrs]	Fail to open on demand [per 10^6 hrs]	Environ.	Human Error		Possible impacts on	Check	Impacts on Environ. [per 10^6 hrs.]	Check	
LCV-3111	Control valve	180	620	DWM		38.03	19.02			All	1. V-003 2. BFW supply		-		
PCV-3111	Control valve	F.V/ 85	620	LP		38.03	19.02			All	1. V-003 2. BFW supply		-		
LCV-3117	Control valve	90	F.V / 620	WW		38.03	19.02			All	V-003		-		
TCV-3123	Control valve	1600	320	BFW		38.03	19.02			All	1. V-003 2. BFW supply		-		
FV-3121A	Automatic recirculate valve	1600	320	BFW		-	-			Abnormal	1. P-004 2. BFW supply				-
XV-3121	Emergency Shut-off valve	F.V/ 630	775	MP		10.69	-			Abnormal	1. P-004 2. BFW supply		7.12		shut-off valve (ball type)
PSV-3111	Pressure safety valve	90	F.V / 620	LP or DMW		6.10	1.32			Abnormal	V-003		-		

Reliability data are adopted from OREDA (2015)

1) Based on the calendar time, the mean values of all failure modes are selected.

5.4 Comparison of DAHAZID vs. HAZOP

In this chapter, a case study is performed with the actual existing process of a BFW system. To clarify the potential in the DAHAZID analysis, this section compares this analysis to a HAZOP study[22], as shown in Table 24.

Table 24. Comparison between DAHAZID and HAZOP

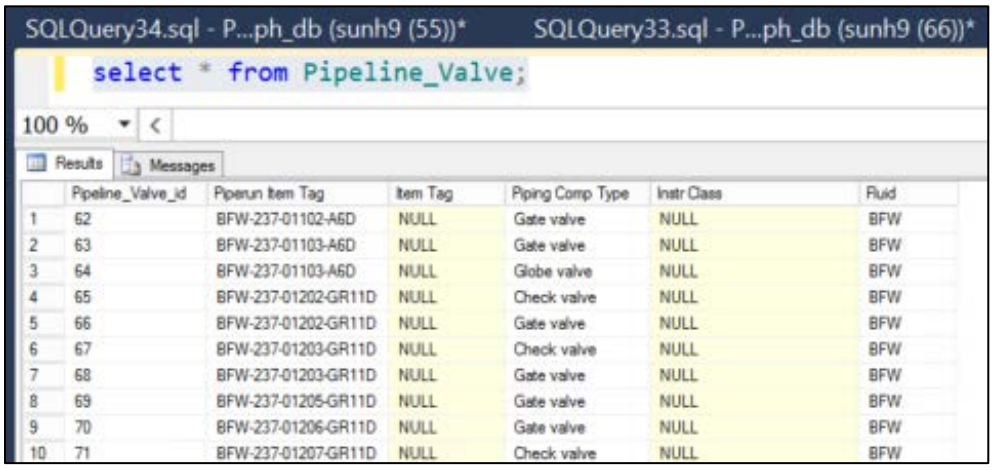
No.	Classification	Type of HAZID	
		DAHAZID	**HAZOP**
1	Required process in advance	Individual participants should review possible fault modes by filling in the prepopulated worksheets of the DAHAZID method	Participants who are in charge should prepare the process documents. In fact, there is no essential requirement
2	Process sequence in the HAZID meeting	Based on the prepared worksheets, participants discuss their opinions and deliberate based on the information	After brief explanations of the process concerned, the participants state their opinions in a brainstorming approach, along with several guidewords and process parameters

[22] Because the system is part of an actual plant and the detailed information is confidential, in this thesis the outcome of the conventional HAZOP study cannot be shown in detail. However, the outcome was almost the same with the result of DAHAZID except for several aspects which are mentioned in this subsection. This table compares the actions occurring in the two approaches.

Table 24. Continued

No.	Classification	Type of HAZID	
		DAHAZID	**HAZOP**
3	Initial point	Consistent mode	Inconsistent mode
		With a prepopulated worksheet after selecting one piece of equipment as reference equipment	Different outcomes occur because of HAZOP facilitator or participants dependencies
4	Fault scenarios	Consistent mode	Inconsistent mode
		After filling in the prepopulated worksheets, equipment failure scenarios are chosen from accumulated data	During the HAZOP study, participants simulate possible scenarios and discuss them together
5	Safeguards	Consistent mode	Inconsistent mode
		Based on equipment failure modes, the DAHAZID method recommends three types of safeguards: 1) inherently safer/passive, 2) active, and 3) procedure	Different outcomes occur dependent on the preferences and experience of HAZOP facilitator or participants
6	Uniqueness	This requires a systematic review of the influence of other systems	Participants can freely suggest any recommendations (e.g., mismanagement of manual valves, impacts on other systems)

In comparison with a conventional HAZOP study, the outcome of the BFW system in the DAHAZID analysis covers all scenarios, except those that are outside the scope of this system (BFW system) and deal with manual valves. However, these issues are solved if the SQL program is manipulated and run again. Firstly, regarding manual valves, the previous prepopulated HAZOP worksheet was designed exclusively for control valves, not manual valves. Based on the fact that SP P&ID® includes all data including manual valves, we can also add manual valve data by using SQL.



	Pipeline_Valve_id	Piperun Item Tag	Item Tag	Piping Comp Type	Instr Class	Fluid
1	62	BFW-237-01102-A6D	NULL	Gate valve	NULL	BFW
2	63	BFW-237-01103-A6D	NULL	Gate valve	NULL	BFW
3	64	BFW-237-01103-A6D	NULL	Globe valve	NULL	BFW
4	65	BFW-237-01202-GR11D	NULL	Check valve	NULL	BFW
5	66	BFW-237-01202-GR11D	NULL	Gate valve	NULL	BFW
6	67	BFW-237-01203-GR11D	NULL	Check valve	NULL	BFW
7	68	BFW-237-01203-GR11D	NULL	Gate valve	NULL	BFW
8	69	BFW-237-01205-GR11D	NULL	Gate valve	NULL	BFW
9	70	BFW-237-01206-GR11D	NULL	Gate valve	NULL	BFW
10	71	BFW-237-01207-GR11D	NULL	Check valve	NULL	BFW

Figure 36. Sorted manual valve list from Microsoft® SQL Server

Figure 36 shows the extracted valve list of the BFW system from the SQL code. Therefore, the manual valve can be considered an intrinsic fault case or a fault case linked to human error. Furthermore, it is expected to identify influences from other systems in the current DAHAZID analysis. In other words, this novel method considers connections with other

subsystems so that we can also predict conditions if these are disconnected. Further communications of units can be reviewed, provided that there are enough data regarding other subsystems.

6. CONCLUSIONS AND FUTURE WORK

This chapter concludes with the key characteristics of this study on Data-based semi-Automatic Hazard Identification (DAHAZID) and opportunities for the application of this methodology, followed by a statement of possible future work.

6.1 Conclusions (Characteristics of the DAHAZID analysis)

This thesis has led to the principle and viability of the DAHAZID analysis and its prepopulated worksheets. Chapter 3 presented the required factors of DAHAZID, and the analysis was developed in compliance with the three main objectives presented in Subsection 1.2. The case studies in Chapters 4 and 5 served to test the possibility of the new semi-automatic tool by taking into account basic projects and existing process plants, respectively. This section elucidates the two main characteristics of the DAHAZID methodology.

6.1.1 The trade-off between sophistication and simplicity

The DAHAZID methodology primarily seeks a simple but deliberately effective approach compared to stand alone HAZOP and FMECA. In this sense, the new DAHAZID method has employed the usefulness of two high-tech computer applications (SP P&ID® and SQL code). By using them, this DAHAZID analysis represents a novel way of increasing the completeness and efficiency of HAZID. Rather than examining each component separately, the combination of components into the functioning plant in DAHAZID enables people to perceive the “bigger picture.” Thus, thanks to the high-tech applications,

the DAHAZID analysis derived this overall insight both from an individual and from a team perspective. Moreover, to achieve a comprehensive understanding with hazard identification by assuming a fault/deviation, it is imperative to follow proper connections between the components of a system in fluid-flow directions, which can be extracted from the SP P&ID®. Through these links, HAZOP and FMECA attributes in DAHAZID are supposed to perform semi-automatically while retaining "human-in-the-loop" to overcome the current limitations of each type of analysis. Consequently, there is room to increase the applications of computerized technologies in the DAHAZID analysis. However, simplicity is are not always correct. For example, even though the tools are employed to enhance simplicity, the usage can have drawbacks due to the intrinsic complexity of new technologies. Consequently, the balance of, "trade-off between sophistication and simplicity" is indispensable to the process of developing the DAHAZID analysis. The representative five trade-offs associated with the DAHAZID analysis are as follows:

1st trade-off: SmartPlant P&ID between strengths and weaknesses

Strengths: The SP P&ID®, commercialized by Intergraph, readily offers various process data inserted in P&ID. Similar to AutoCAD® P&ID, this software produces process system graphs. In addition, SP P&ID® incorporates the process data of the process system graphs simultaneously. For this reason, we do not have to deal with several process documents, so we can save time and obtain highly reliable data that we input with SP P&ID®.

Weakness: By using SP P&ID®, several challenging issues arose, compared to the traditional AutoCAD® P&ID. Most of all, initially it turns out somewhat difficult to use this software. For a computer science novice, in the beginning, nearly every step appears to be demanding, from the installation of the program to understanding its principles and multiple subprograms. Consequently, it takes some time to adapt to the SP P&ID® environment.

2nd trade-off: Data reduction by application of SQL

Strengths: DATA mining, such as the standard query language SQL code in DAHAZID, facilitates dealing with intricate process data and sorting so that we can obtain the needed data quickly. Other methodologies have been struggling to identify connections among process components using different methods to track the causality of faults. The DAHAZID analysis with the aid of the SQL code commences its process with finding the linkages within the process system. Therefore, possible incident scenarios are expected to appear immediately and consistently.

Weakness: Similar to utilizing SP P&ID®, it is initially necessary to become familiar with the SQL software for the preparation of proper SQL coding. Furthermore, the preparation demands overall understanding of chemical plants to select the right data from amongst a significant amount of information. An understanding of the principles of process safety concepts also is required to develop possible scenarios with the SQL code. After gaining the required insight with the aid of SQL, we can adequately frame the hazard identification tools.

3rd trade-off: "Flow" as the main guide for fault propagation

Strengths: DAHAZID adopts a single process variable, *flow*, as the primary guide for fault effect propagation for two main reasons. Firstly, it is believed that nearly all possible faults and failure modes in the chemical process occur due to flow deviation from the normal cause a flow deviation. Physically, flow, temperature, and pressure are related. Moreover, flow can be regarded as the fundamental carrier of cause-effect information downstream or upstream. In the extracted data, flow can be tracked between linked parts of equipment (and not internally a piece of equipment). Secondly, this approach facilitates scenario thinking along flow directions and generates relatively logical outcomes with respect to causality. For these reasons, by focusing only on "flow" at the start the DAHAZID analysis achieves cause-effect chain scenarios in a simpler way than conventional HAZOP.

Weakness: Regarding the use of flow as the fundamental guide variable of fault effect propagation requires discussion. Most of all, this approach might fail to cover all possible scenarios, or it will make it more difficult. For example, a case associated with no flow may still require checking both in normal upstream and downstream directions for possible effects and in case of a process including chemical mixtures, the partial flows of individual mixture constituents should be followed. Additionally, this approach shall not impede the freedom of brainstorming of a HAZOP study that examines all deviations by selecting one or a multiple of process variables. These possible weaknesses shall in be investigated in a continued study.

4th trade-off: From cause to consequence and cure

Potential: The DAHAZID analysis attempts to define the possible scenarios of control faults or equipment failure modes and the safeguards to mitigate possible effects. The idea behind DAHAZID is to develop a "*nonstop service*" automatically from fault diagnosis to a reliable recommendation for enhanced safety management. Even though experts may propose many good recommendations during a HAZOP meeting, important possibilities might still be overlooked. For this reason, the DAHAZID analysis utilizes the accumulated recommendations of the CCPS (1998) guideline, which incorporates in tabulated form nearly all failure cases of chemical plant equipment. Of course, these suggestions can in an actual case be updated. Through this process, the outcomes of the DAHAZID methodology can be maintained consistently without depending only on the ability and experience of an individual expert.

Counter-effect: Relying heavily on well-prepared circumstances regarding fault and failure modes and safeguards, and not questioning an accepted state of affairs sufficiently, can be risky. However, there is no perfect answer. In the light of adverse effects, organizations that might employ this approach should arrange conditions in which people are stimulated and motivated to engage in discussions readily and freely, and update and improve recommendations to their company.

5th trade-off: Automated vs. Semi-automated approach

Automation: As conventional HAZID may be wearing people out, it would be useful indeed to obtain results with less human effort. For this reason, DAHAZID sought

application of automation tools by using new technologies and existing reliable data sources.

***Semi*-automation:** Similar to the reason given in the section 2.4 “From cause to consequence and cure”, adoption of results obtained through “mechanical” processes by just relying on software without any questioning is unacceptable. Process safety analysis deals with the prevention of loss of life, which demands prudence and responsibility regarding its results. Producing cues for the thinking process is good; people should become familiar with all the ins and outs of the process. Consequently, from the beginning of this research, the DAHAZID analysis intentionally pursues a semi-automated (not completely automated) preparation tool to reduce errors and boring work and enable people to engage more effectively in the HAZID process proper. DAHAZID leaves room for proactive approaches. 1) The prepopulated worksheets are designed to stimulate people’s imaginations as a checklist does, but should leave space to insert uncommon cause and effect events emerging from the team deliberations, 2) The two basic sources, possible scenarios and safeguards, of prepopulated worksheets in DAHAZID can be improved continually based on people’s experience.

6.1.2 Opportunities of the DAHAZID methodology

Based on the above-mentioned characteristics of the DAHZID method, the possible opportunities of the DAHAZID analysis in terms of the process safety management aspect are listed:

Boosted discussion with prepopulated-worksheets

Because of their clear guidelines, the suggested prepopulated worksheets enable engineers to examine possible scenarios rigorously in advance. Rather than attending a meeting without any concerns, engineers/analysts can clarify their thinking with aid of the prepopulated worksheets before team discussions take place. Thus, the outcome of the DAHAZID analysis might be more effective.

Unified work process within entire organization

It would be useful to maintain a consistent analysis approach among individuals across their entire organization. Of course, this worksheet needs substantial improvement, but a worksheet that has equivalent formats guides the identical analysis approach regardless of personal experiences. Therefore, we do not have to be solely dependent a minority of experts, and this method can be used for the purpose of training, especially regarding process safety designs. But it will also be of great value to the operational stage in case new potential scenarios are discovered. These new findings can be easily added to the worksheets. However, it will also be of great value to the operational stage in case new potential scenarios are discovered. These new findings can be easily added to the worksheets.

Practicality in any stage projects

Because the possible cause/consequence items are shown readily, the DAHAZID analysis can be exploited for any stage projects (e.g., basic, Front End Engineering Design (FEED), Engineering, Procurement, and Construction (EPC) projects) and even for Management

of Change (MOC) in the operational stage. Consequently, this new method leads to time and hence, cost-saving

6.2 Future work

Several opportunities of the current DAHAZID methodology can be suggested:

Visualization of Causality by Using Bowtie and Bayesian Networks

Based on the current stage (ongoing steps) in Figure 24 in Chapter 3, this research can be taken further by combining the identified scenarios into clusters in a bowtie structure and mapping the bowtie analysis into a Bayesian network. The next steps of the proposal can produce visual causal relationships and quantification to effectively diagnose possible root causes according to their relative probabilities. In addition, this study can be extended to abnormal, start-up, turn-around, or batch operation conditions.

Construction of Database

It is reasonable to assume that "*if you put garbage in, garbage will come out*." To obtain realistic results with the DAHAZID methodology, future studies should construct a valid and reliable computerized database. According Unni Krishnan (2005), one of the main reasons to occur similar or same incidents respectively, it is uncommon for companies to accumulate their knowledge which can be passed to the next generation. For this reason, based on previous incidents, the database should incorporate updated failure scenarios and safeguards for different types of chemical processes or fluids. It can also add other failures

that presumably occur because of the environment, possible domino effects, human and procedural errors, or organizational weaknesses in DAHAZID.

Human Factors

More information on human and organizational factors would help to establish a greater degree of accuracy with the DAHAZID methodology. The information on human factors can be associated with the individual and organizations. Regarding the individual, we should carefully consider process procedures, which are not to be dissociated from other safeguards. Additionally, further research is needed to understand the influence of safety management systems better.

System Approach

Various researchers (Hollnagel, 2012; Leveson, 2011; Perrow, 2011; Rasmussen & Suedung, 2000) have stressed that trying to identify all possible scenarios of what can go wrong by decomposing the system into components and focusing on faults will fail. Events following from a dysfunctional interaction of rightly functioning components will be overlooked. This kind of mishaps has to be identified by a system-theoretic tool as developed by Leveson. Practical inclusion of this in a computerized tool will be a challenge.

6.3 Summary of conclusions

This research proposed the Data-based semi-Automatic Hazard Identification (DAHAZID) analysis to improve on classic HAZID tools. This method enables the determination of possible causes and consequences in a system from the HAZOP functioning perspective, including operational errors, whereas FMECA will check the effects of a system's possible failure modes, including those from its environment, the problems intrinsic to each piece of equipment from loading and material wear, and human errors that occur in construction, operation, and maintenance. This notion in the DAHAZID methodology was realized through prepopulated worksheets with the aid of new technologies, SP P&ID® and the SQL language. Throughout this research, there were many trade-offs between sophisticated and simple modes for a better practical identification tool.

The research makes contributions towards the current HAZID field, in which safeguards are considered separately from fault scenarios and generated in a brainstorming approach, and people tend to rely heavily on individual experts.

REFERENCES

Baybutt, P. (2015a). Competency requirements for process hazard analysis (PHA) teams. *Journal of Loss Prevention in the Process Industries, 33,* 151-158.

Baybutt, P. (2015b). A critique of the Hazard and Operability (HAZOP) study. *Journal of Loss Prevention in the Process Industries, 33,* 52-58.

Baybutt, P. (2016a). Insights into process safety incidents from an analysis of CSB investigations. *Journal of Loss Prevention in the Process Industries*.

Baybutt, P. (2016b). Process design and engineering: A missing process safety element. *Process Safety Progress, 35*(1), 115-115.

Bunge, M. A. (1979). Treatise on Basic Philosophy: Ontology II: A World of Systems. Dordrecht, Holland: D: Reidel Publishing Company.

Cameron, I. T., Mannan, S., Németh, E., Park, S., Pasman, H., Rogers, W., & Seligmann, B. (2017). Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better? *Process Safety and Environmental Protection*.

Cameron, I. T., Seligmann, B., Hangos, K., Lakner, R., & Németh, E. (2007). *The P3 Formalism: A basics for improved diagnosis in complex systems.* Paper presented at the CHEMECA 2007, Melbourne.

CCPS. (1989). *Guidelines for Process Equipment Reliability Data, with Data Tables*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CCPS. (1998). *Guidelines for design solutions for process equipment failures.* (1st ed. Vol. 17). New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CCPS. (2008). *Guidelines for hazard evaluation procedures* (3rd ed.). New York: Center for Chemical Process Safety of the American Instituteof Chemical Engineers.

Crawley, F., & Tyler, B. (2015). *HAZOP: Guide to best practice for the process and chemical industries* (3rd ed.). United States: Elsevier

Crowd, C. (2016). Oil & Gas: Redline, as-built & drafting services for clients in Calgary, Edmonton, Red Deer, Medicine Hat, Grand Prairie & Fort McMurray. Retrieved from http://www.eng-source.com/services/oil-gas-drafting-design-services/

Crowl, D. A., & Louvar, J. F. (2001). *Chemical process safety: fundamentals with applications* (2nd ed.). Upper Saddle River, New Jersey 07458: Pearson Education.

Cui, L., Zhao, J., Qiu, T., & Chen, B. (2008). Layered digraph model for HAZOP analysis of chemical processes. *Process Safety Progress, 27*(4), 293-305.

Cui, L., Zhao, J., & Zhang, R. (2010). The integration of HAZOP expert system and piping and instrumentation diagrams. *Process Safety and Environmental Protection, 88*(5), 327-334.

Duguid, I. (1999). Analysis of past incidents in the oil, chemical and petrochemical industries. *Loss Prevention Bulletin, 144*.

Dunjó, J., Fthenakis, V., Vílchez, J. A., & Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials, 173*(1), 19-32.

Ego, D., & MacGregor, R. (2004). Improve your facility's PHA methodology. *Hydrocarbon processing*, *83*(4), 81-86.

Giardina, M., Castiglia, F., & Tomarchio, E. (2014). Risk assessment of component failure modes and human errors using a new FMECA approach: application in the safety analysis of HDR brachytherapy. *Journal of Radiological Protection, 34*(4), 891.

Giardina, M., & Morale, M. (2015). Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology. *Journal of Loss Prevention in the Process Industries, 35*, 35-45.

Goodson, P. (2016). *Becoming an academic writer: 50 exercises for paced, productive, and powerful writing*: Sage Publications.

Gränfors, A. (2015). Introduction to Intergraphs Smartplant PID. Retrieved from https://www.youtube.com/watch?v=8ejxxz2-ank

Group, I. W. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0. *Final report, April*.

Han, J., Pei, J., & Kamber, M. (2011). *Data mining: concepts and techniques*: Elsevier.

Hendershot, D. (2006). Process safety. *Journal of Chemical Health and Safety*, *13*(2), 30-31.

Hollnagel, E. (2012). *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*: Ashgate Publishing, Ltd.

HSE. (2012). Failure Rate and Event Data for use within Risk Assessments. Retrieved from www.hse.gov.uk/landuseplanning/failure-rates.pdf.

Instone, B. (1989). *Losses in the hydrocarbon process industries.* Paper presented at the Proceedings of 6th Int. Symposium Loss Prevention and Safety Promotion in the Chemical Industries.

ISA The Instrumentation Systems and Automation Society. (1981). ISA–20–1981 *Specification Forms for Process Measurement and Control Instruments, Primary Elements, and Control Valves*. United States of America: the Instrument Society of America.

Kaszniak, M. (2010). Oversights and omissions in process hazard analyses: Lessons learned from CSB investigations. *Process Safety Progress*, *29*(3), 264-269.

Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection*, *98*, 116-147.

Khan, F. I., & Abbasi, S. (1995). HAZEXPT: A comprehensive Knowledge Base system for HAZOP study *Research report number CPCE/R&D 15/95*: Pondicherry University.

Khan, F. I., & Abbasi, S. (1997a). OptHAZOP—an effective and optimum approach for HAZOP study. *Journal of Loss Prevention in the Process Industries, 10*(3), 191-204.

Khan, F. I., & Abbasi, S. (1997b). TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. *Journal of Loss Prevention in the Process Industries, 10*(5-6), 333-343.

Khan, F. I., & Abbasi, S. (2000). Towards automation of HAZOP with a new tool EXPERTOP. *Environmental Modelling & Software, 15*(1), 67-77.

Kidam, K., & Hurme, M. (2012). Design as a contributor to chemical process accidents. *Journal of Loss Prevention in the Process Industries, 25*(4), 655-666.

Kidam, K., & Hurme, M. (2013). Analysis of equipment failures as contributors to chemical process accidents. *Process Safety and Environmental Protection, 91*(1), 61-78.

Kidam, K., Hurme, M., & Hassim, M. H. (2010). Technical analysis of accident in chemical process industry and lessons learnt. *Chemical Engineering Transactions, 19*, 451-456.

Knowlton, R. E. (1987). Introduction to hazard and operability studies: the guide word approach *Introduction to hazard and operability studies: the guide word approach*: Chemetics International Company.

Lawley, H. (1974). Operability studies and hazard analysis. *Chemical Engineering Progress, 70*(4), 45-56.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*: MIT press.

MacGregor, R. J. (2013). Assess Hazards with Process Flow Failure Modes Analysis. *Chemical Engineering Progress, 109*(3), 48-56.

MacGregor, R. J. (2016). *hree Case Studies Comparing and Contrasting PFFM and HazOp PHA Reviews*. Paper presented at the 19th International Annual Symposium, College Station, TX.

Marsh Inc. (1987). A Thirty-Year Review of One Hundred of the Largest Property Damage Losses in the Hydrocarbon-Chemical Industries. Marsh Inc.

McKelvey, T. (1988). How to improve the effectiveness of hazard and operability analysis. *IEEE Transactions on Reliability, 37*(2), 167-170.

Mikulak, R. J., McDermott, R., & Beauregard, M. (2008). *The basics of FMEA*: CRC Press.

Németh, E., Seligmann, B. J., Hockings, K., Oakley, J., O'Brien, C., Hangos, K. M., & Cameron, I. T. (2011). *Generating cause-implication graphs for process systems via blended hazard identification methods.* Paper presented at the 21st European symposium on computer aided process engineering (ESCAPE 21).

Nivolianitou, Z., Konstandinidou, M., & Michalis, C. (2006). Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system (MARS). *Journal of hazardous materials, 137*(1), 1-7.

OREDA. (2015). *Offshore & Onshore Reliability Data* (6 ed. Vol. 1-Topside Equipment). DNV GL: OREDA Participants.

Pasman, H. J. (2015). *Risk Analysis and Control for Industrial Processes-Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-probability, High-consequence Events*: Butterworth-Heinemann.

Perrow, C. (2011). *Normal accidents: Living with high risk technologies*: Princeton University Press.

Prem, K. P., Ng, D., & Mannan, M. S. (2010). Harnessing database resources for understanding the profile of chemical process industry incidents. *Journal of Loss Prevention in the Process Industries, 23*(4), 549-560.

Rahman, S., Khan, F., Veitch, B., & Amyotte, P. (2009). ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis. *Journal of Loss Prevention in the Process Industries, 22*(4), 373-380.

Rasmussen, J., & Suedung, I. (2000). *Proactive risk management in a dynamic society*: Swedish Rescue Services Agency.

Redmill, F., Chudleigh, M., & Catmur, J. (1999). *System safety: HAZOP and software HAZOP*: Wiley Chichester.

Rockoff, L. (2016). *The language of SQL* (2nd ed.): Addison-Wesley Professional.

Seligmann, B. (2011). A Functional Systems Framework and Blended Hazard Identification Methodology to Support Process Diagnosis.

Seligmann, B., Németh, E., Hangos, K. M., & Cameron, I. T. (2012). A blended hazard identification methodology to support process diagnosis. *Journal of Loss Prevention in the Process Industries, 25*(4), 746-759.

Shaw, A. (2016). Stock List 2: Pipelines. Retrieved from https://www.linkedin.com/pulse/stock-list-2-pipelines-amy-shaw

Shell and Tube Exchnager Data sheet-Excel sheet and PDF form. (2016). Retrieved from http://processprinciples.com/2013/12/shell-and-tube-exchanger-data-sheet/

Srinivasan, R., & Venkatasubramanian, V. (1998). Automating HAZOP analysis of batch chemical plants: Part II. Algorithms and application. *Computers & Chemical Engineering, 22*(9), 1357-1370.

Sumathi, S., & Sivanandam, S. (2006). *Introduction to data mining and its applications* (Vol. 29): Springer.

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162-173.

Taylor, J. R. (1975). A Study of Abnormal Occurrence Reports. Report RISØ-M-1837, Risø National Laboratory: Roskilde.

Taylor, J. R. (2007). Statistics of design error in the process industries. *Safety science, 45*(1), 61-73.

Unni Krishnan, G. (2005). What Hazop studies cannot do. *Hydrocarbon processing, 84*(10), 93-95.

US Regulations. (1992). CFR 1910.119,"Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," Department of Labor. *Occupational Safety and Health Administration, Washington, DC*.

Vaidhyanathan, R., & Venkatasubramanian, V. (1995). Digraph-based models for automated HAZOP analysis. *Reliability Engineering & System Safety, 50*(1), 33-49.

Vaidhyanathan, R., & Venkatasubramanian, V. (1996a). Experience with an expert system for automated HAZOP analysis. *Computers & Chemical Engineering, 20*, S1589-S1594.

Vaidhyanathan, R., & Venkatasubramanian, V. (1996b). A semi-quantitative reasoning methodology for filtering and ranking HAZOP results in HAZOPExpert. *Reliability Engineering & System Safety*, *53*(2), 185-203.

Vaidhyanathan, R., Venkatasubramanian, V., & Dyke, F. T. (1996). HAZOPExpert: An expert system for automating HAZOP analysis. *Process Safety Progress, 15*(2), 80-88.

Venkatasubramanian, V., & Vaidhyanathan, R. (1994). A knowledge-based framework for automating HAZOP analysis. *AIChE Journal, 40*(3), 496-505.

Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005a). Phasuite: an automated HAZOP analysis tool for chemical processes: part I: knowledge engineering framework. *Process Safety and Environmental Protection, 83*(6), 509-532.

Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005b). PHASuite: An automated HAZOP analysis tool for chemical processes: Part II: Implementation and Case Study. *Process Safety and Environmental Protection, 83*(6), 533-548.

Zhao, J., Cui, L., Zhao, L., Qiu, T., & Chen, B. (2009). Learning HAZOP expert system by case-based reasoning and ontology. *Computers & Chemical Engineering, 33*(1), 371-378.

APPENDIX A

Regulations associated with PHA

Governmental regulations related to identifying and evaluating process hazards

(CCPS, 2008)

Country or region	Regulation
United States	29 CFR 1910.119, US. Occupational Safety and Health Administration (OSHA) Process Safety Management of Highly Hazardous Chemicals
	40 CFR 68, US. Environmental Protection Agency (EPA) Risk Management Program for Chemical Accident Release Prevention
United Kingdom	U.K. Health, Safety Executive, Control of Major Hazards (COMAH) regulations
South Korea	Industrial Safety and Health Act -Article 20, Preparation of Safety and Health Management Regulations
Australia	National Standard for Control of Major Hazard Facilities [NOHSC:1014 (1996)l
European Union	Seveso II Directive 2003/105/EC
	ATEX 137 Workplace Directive 1999/92/EC
Mexico	NOM-028-STPS-2004, Occupational organization - Safety in the Processes of Chemical Substances
Singapore	National Environment Agency (one-time QRA Report for new chemical plants)

This table represent several countries' regulation lists regarding hazard identification and evaluation.

APPENDIX B

The CSB incidents reviewed by Baybutt (2016a)

No.	Incident	Incident date	Report date	PSM[1]	PHA[2]
1	Sonat Exploration Co. Catastrophic Vessel Over pressurization	3/4/1998	9/21/2000	N	N
2	Morton International Inc. Runaway Chemical Reaction, Explosion and Fire	4/8/1998	8/16/2000	N	Y
3	Concept Sciences Hydroxylamine Explosion	2/19/1999	2/1/2002	Y	Y
4	Tosco Avon Refinery Petroleum Naphtha Fire	2/23/1999	3/21/2001	Y	N
5	Bethlehem Steel Corporation Gas Condensate Fire	2/2/2001	12/6/2001	N	N
6	BP Amoco Thermal Decomposition Incident	3/13/2001	5/20/2002	N	Y
7	Motiva Enterprises Sulfuric Acid Tank Explosion	7/17/2001	8/28/2002	N	Y
8	Georgia-Pacific Corp. Hydrogen Sulfide Leak	1/16/2002	11/20/2002	N	N
9	Third Coast Industries Petroleum Products Facility Fire	5/1/2002	3/6/2003	N	U
10	DPC Enterprises Festus Chlorine Release	8/14/2002	5/1/2003	Y	U
11	First Chemical Corp. Reactive Chemical Explosion and Fire	10/13/2002	10/15/2003	N	N
12	Environmental Enterprises Hydrogen Sulfide Release	12/11/2002	9/17/2003	N	U
13	Catalyst Systems Inc. Reactive Chemical Explosion and Fire	1/2/2003	10/29/2003	N	N
14	BLSR Operating Ltd. Vapor Cloud Deflagration and Fire	1/13/2003	9/17/2003	N	U
15	West Pharmaceutical Services Dust Explosion and Fire	1/29/2003	9/23/2004	N	N

Y -yes, N-No, U-Unknown

No.	Incident	Incident date	Report date	PSM[1]	PHA[2]
16	Technic Inc. Ventilation System Explosion and Fire	2/7/2003	8/20/2004	N	N
17	CTA Acoustics Dust Explosion and Fire	2/20/2003	2/15/2005	N	N
18	D.D. Williamson & Co. Catastrophic Vessel Failure	4/11/2003	3/12/2004	N	N
19	Honeywell Chemical Releases (3 incidents)		8/8/2005		
	a. Chlorine	7/20/2003		Y	Y
	b. Antimony pentachloride	7/29/2003		N	N
	c. Hydrogen fluoride	8/13/2003		Y	N
20	Isotec/Sigma Aldrich Nitric Oxide Explosion	9/21/2003	8/24/2004	Y	Y
21	Hayes Lemmerz Dust Explosions and Fire	10/29/2003	9/27/2005	N	N
22	DPC Enterprises Glendale Chlorine Release	11/17/2003	2/28/2007	Y	Y
23	Giant Industries Oil Refinery Explosion and Fire	4/8/2004	10/26/2005	Y	Y
24	MFG Chemical Inc. Toxic Gas Release	4/12/2004	4/11/2006	Y	N
25	Formosa Plastics Vinyl Chloride Explosion	4/23/2004	3/6/2007	Y	Y
26	Sterigenics Ethylene Oxide Explosion	8/19/2004	3/30/2006	Y	Y
27	Marcus Oil and Chemical Tank Explosion and Fire	12/3/2004	6/6/2006	N	N
28	Acetylene Service Company Gas Explosion	1/25/2005	1/26/2006	Y	Y
29	BP Texas City Refinery Explosion and Fire	3/23/2005	3/20/2007	Y	Y
30	Formosa Plastics Propylene Fire and Explosions	10/6/2005	7/20/2006	Y	Y

Y -yes, N-No, U-Unknown

No.	Incident	Incident date	Report date	PSM[1]	PHA[2]
31	Bethune Point Wastewater Plant Explosion and Fire	1/11/2006	3/13/2007	N	N
32	Synthron Chemical Reaction and Vapor Cloud Explosion	1/31/2006	7/31/2007	Y	N
33	Partridge Raleigh Oilfield Explosion and Fire	6/5/2006	6/12/2007	N	N
34	Universal Form Clamp Co. Explosion and Fire	6/14/2006	4/10/2007	Y	N
35	EQ Hazardous Waste Plant Explosions and Fire	10/5/2006	4/16/2008	N	U
36	CAI/Arnel Chemical Plant Explosion	11/22/2006	5/13/2008	Y	N
37	Valero Refinery Propane Fire	2/16/2007	7/9/2008	Y	Y
38	Barton Solvents Explosions and Fire	7/17/2007	6/26/2008	N	U
39	Xcel Energy Company Hydroelectric Tunnel Fire	10/2/2007	8/25/2010	N	Y
40	Barton Solvents Flammable Liquid Explosion and Fire	10/29/2007	9/18/2008	N	U
41	T2 Laboratories Inc. Reactive Chemical Explosion	12/19/2007	9/15/2009	N	N
42	Imperial Sugar Company Dust Explosion and Fire	2/7/2008	9/24/2009	N	U
43	Goodyear Heat Exchanger Rupture and Ammonia Release	6/11/2008	1/27/2011	Y	U
44	Packaging Corporation Storage Tank Explosion	7/29/2008	3/4/2010	N	N
45	Bayer CropScience Pesticide Waste Tank Explosion	8/28/2008	1/20/2011	Y	Y
46	INDSPEC Chemical Corporation Oleum Release	10/11/2008	9/30/2009	Y	Y
47	Allied Terminals Fertilizer Tank Collapse	11/11/2008	5/26/2009	N	N

Y -yes, N-No, U-Unknown

No.	Incident	Incident date	Report date	PSM[1]	PHA[2]
48	Veolia Environmental Services Flammable Vapor Explosion and Fire	5/4/2009	7/21/2010	Y	N
49	ConAgra Natural Gas Explosion	6/9/2009	2/4/2010	N	U
50	CITGO Refinery Fire and Hydrofluoric Acid Release	7/19/2009	12/9/2009	Y	Y
51	Caribbean Petroleum Refining Tank Explosion and Fire	10/23/2009	10/21/2015	N	N
52	Silver Eagle Refinery Explosion	11/4/2009	4/14/2014	Y	U
53	NDK Crystal Inc. Explosion	12/7/2009	11/14/2013	N	U
54	DuPont Corporation Toxic Chemical Releases (3 incidents)		9/20/2011		
	a. Methyl chloride	1/22/2010		U	U
	b. Oleum	1/23/2010		U	U
	c. Phosgene	1/23/2010		Y	Y
55	Kleen Energy Natural Gas Explosion	2/7/2010	6/28/2010	N	U
56	Tesoro Refinery Explosion and Fire	4/2/2010	5/1/2014	Y	Y
57	Horsehead Holding Company Explosion and Fire	7/22/2010	3/11/2015	N	U
58	Millard Refrigerated Services Ammonia Release	8/23/2010	1/15/2015	U	U
59	E. I. DuPont De Nemours Co. Hotwork Explosion	11/9/2010	4/19/2012	Y	Y
60	AL Solutions Dust Explosion	12/9/2010	7/16/2014	N	U
61	Carbide Industries Fire and Explosion	3/21/2011	2/7/2013	N	U
62	Hoeganaes Corporation Flash Fires and Explosion	5/27/2011	1/5/2012	U	U
63	Chevron Refinery Fire	8/6/2012	1/28/2015	Y	Y
64	US Ink Fire	10/9/2012	1/15/2015	U	U

Y: yes, N: No, U-Unknown

With the table above, the table represents the possible underlying causes based on the analysis of Baybutt (2016a)

Associated Categories for Causes	The number of CBS investigation report in Table A.2	Percentage of the total CSB incident reports
Industry standards and guidelines	9,14,16,25,26,29,36,37,48,51,53,54c,55, 56,63	22%
Design and engineering	1,3,6,15,16,17,18,21,25,29,31,34, 37, 40, 41, 42, 57, 58, 64	28%
Previous incident review	2, 5, 6, 11, 17, 19a, 20, 21, 25, 26, 29, 41, 42, 45, 51, 53, 54a, 54c, 60, 61, 63, 64	32%
Safeguards protection analysis	2, 7, 8, 9, 11, 12, 13, 17,18, 20, 21, 22, 24, 25, 26, 28, 29, 30, 32, 34, 35, 36, 37, 38, 40, 41, 42, 46, 48, 49, 50, 51, 54a,54b, 54c, 60, 62, 64 Specially, 19a, 56 and 63 are non-specific or general cases.	56%

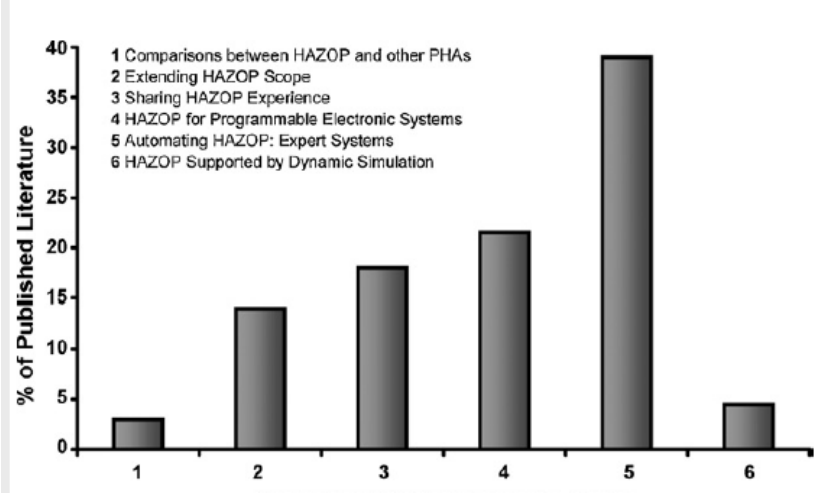
Data from: Baybutt (2016a)

APPENDIX C

BACKDATA FOR HAZOP

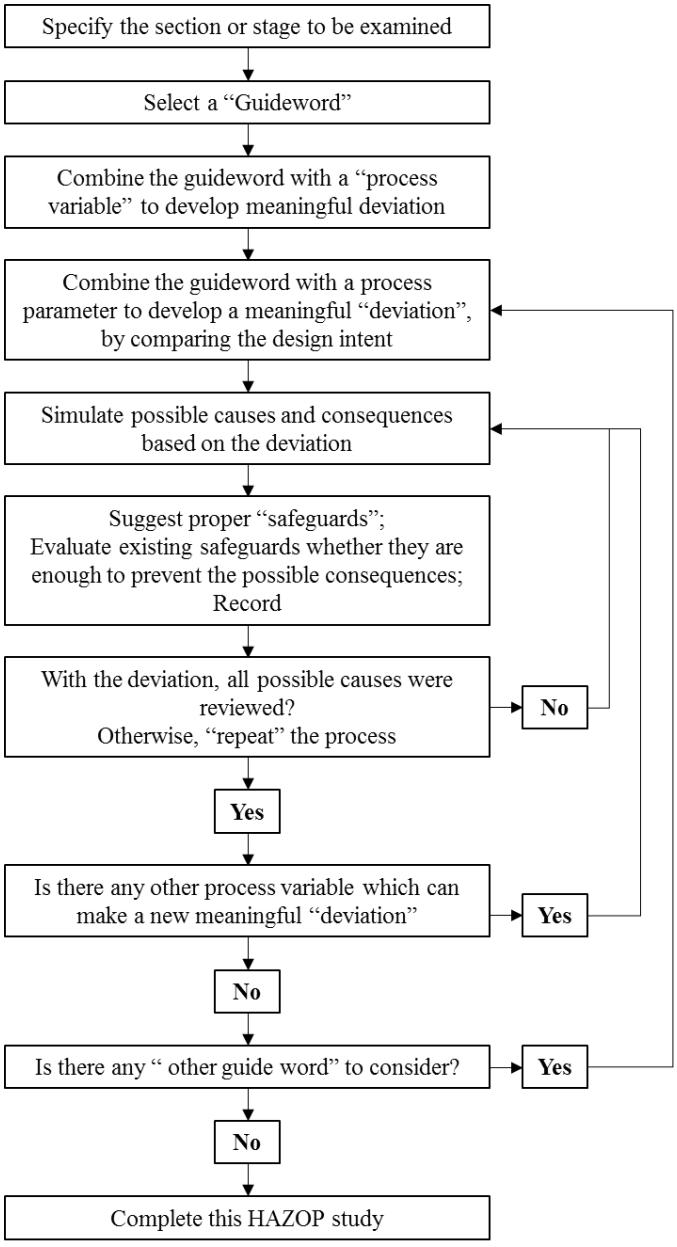
C.1 Brief history of HAZOP

The genesis of HAZOP study was proposed by the Imperial Chemical Industries in the early 1970s (Pasman, 2015). Ever afterward, HAZOP has evolved to overcome its weaknesses. Lawley (1974) carried out the fundamental principles of HAZOP on the paper "Operability Studies and Hazard Analysis," and Chemical Industries Association launched an official guide for the study in 1977. According to Dunjó *et al*., (2010), the HAZOP research areas actively has been conducted, and the majority of tasks (after the1990s) perused automatic HAZOP approaches as follows.



Classifications of HAZOP research areas
(Dunjó, Fthenakis, Vílchez, & Arnaldos, 2010)

C.2 A generic process of HAZOP study



Modified from the book of Crawley and Tyler (2015)

This working diagram represents a relatively systematic approach, whereas it points to how engineers should repeat similar processes during one meeting and participants simulate possible scenarios depending on their gut feeling.

C.3 Useful resources related to a HAZOP study (Dunjó *et al.*, 2010)

Year	Author/ Institution	Title	Paper	Guideline	Book	Standard
1974	Lawley	Operability Studies And Hazard Analysis	■			
1977	CIA	A Guide to Hazard and Operability Studies		■		
1981	Knowlton	Hazards and Operability Studies, The Guideword Approach			■	
1983	Kletz	"HAZOP & HAZAN". Identifying and Assessing Process Industry Hazards (first edition)			■	
1986	Kletz	"HAZOP & HAZAN". Identifying and Assessing Process Industry Hazards (second edition)			■	
1996	Lees	Loss Prevention in Process Industries Hazard Identification, Assessment and Control			■	
1991	HSE	Guidance on HAZOP Procedures for Computer-controlled Plants		■		
1992	Kletz	"HAZOP & HAZAN". Identifying and Assessing Process Industry Hazards (third edition)			■	
1992	CCPS	Guidelines for Hazard Evaluation Procedures			■	
1994	Nolan	Application of HAZOP and What-if Safety Reviews to the Petroleum, Petrochemical and Chemical Industries			■	
1996	Wells	Hazard Identification and Risk Assessment			■	
1999	Kletz	"HAZOP & HAZAN". Identifying and Assessing Process Industry Hazards (fourth edition)			■	
1999	Redmill	System Safety: HAZOP and Software HAZOP			■	
2000	EPSC	HAZOP: Guide to Best Practice. Guidelines to Best Practice for the Process and Chemical Industries			■	
2001	BS IEC 61882	Hazard and Operability studies (HAZOP Studies)— Application Guide				■
2004	McDonald	Practical HAZOPs, Trips and Alarms			■	

APPENDIX D

SYNTAX OF HAZOP ATTRIBUTE

D.1 SQL Code for HAZOP-Path 1 (Microsoft® SQL Server 2012 program)

```
@V_EQUIPMENT VARCHAR(50);
SET @V_EQUIPMENT= 'E-003';
BEGIN
SELECT * FROM
(SELECT
(SELECT FROM_EQUIPMENT FROM
dbo.GET_CONNECTION_OTHER_SYSTEMS_INLET(temp.from_equipment)) AS
Inlet_Other_System,
temp.From_Equipment as 'Inlet Line',
left(temp.From_Equipment, charindex('-', temp.From_Equipment)-1) as 'Fluid',
pv.[Item Tag] as 'Fault Valve',
pv.[Instr Class] as 'Valve Type',
@v_equipment as 'Reference Equipment',
temp.to_equipment as 'Outlet Line',
(SELECT consequence FROM
dbo.GET_CONNECTION_CONSEQUENCE(temp.to_equipment)) AS
'Consequence_Equipment1',
```

```
(SELECT to_equipment FROM
dbo.GET_CONNECTION_OTHER_SYSTEMS_OUTLET(temp.to_equipment)) AS
Outlet_Other_System
  FROM
  (SELECT c2.From_Equipment,
  c1.To_Equipment
  FROM  Connection$ c1,
     Connection$ c2
  WHERE c1.From_Equipment=@v_equipment
  and c2.To_Equipment=c1.From_Equipment)TEMP
LEFT OUTER JOIN Pipeline_Valve pv
 ON pv.[PipeRun Item Tag]= temp.from_Equipment
 AND pv.[Instr Class] IN ('Control valves and regulators','Relief devices'))TEMP2
WHERE (TEMP2.Inlet_Other_System is not null or [Fault Valve] is not null)
AND (TEMP2.Consequence_Equipment1 IS NOT NULL OR
TEMP2.Outlet_Other_System IS NOT NULL);



END;
```

D.2 SQL Code for HAZOP-Path 2 (Microsoft® SQL Server 2012)

```
@V_EQUIPMENT VARCHAR(50);
SET @V_EQUIPMENT= 'E-003';
BEGIN
  SELECT * FROM
  (SELECT temp.To_Equipment AS 'Outlet line',
       left(temp.To_Equipment, charindex('-', temp.To_Equipment)-1) as 'Fluid',
     (SELECT consequence FROM
dbo.GET_CONNECTION_CONSEQUENCE(temp.To_Equipment)) AS 'Equipment',
     temp.[Item Tag] AS 'Fault Valve',
     temp.[Instr Class] AS 'Valve type',
     temp.From_Equipment AS 'Ref. Equipment',
     c2.to_equipment as 'Outlet Piping',
      (SELECT consequence FROM
dbo.GET_CONNECTION_CONSEQUENCE(c2.To_Equipment)) AS 'Consequence
Equipment',
      (SELECT to_equipment FROM
dbo.GET_CONNECTION_OTHER_SYSTEMS_OUTLET(c2.To_Equipment)) AS
'Other System'
  FROM
   (SELECT c1.From_Equipment,
```

```
        c1.To_Equipment,
      pv.[Item Tag],
      pv.[Instr Class],
      pv.fluid,
      (SELECT consequence FROM
dbo.GET_CONNECTION_CONSEQUENCE(C1.To_Equipment)) AS 'Equipment'
   FROM Connection$ c1
   LEFT OUTER JOIN Pipeline_Valve pv
   ON pv.[PipeRun Item Tag]= c1.to_equipment
   AND pv.[Instr Class] IN ('Control valves and regulators','Relief devices')
   WHERE c1.From_Equipment=@V_EQUIPMENT)TEMP
  LEFT OUTER JOIN Connection$ c2
  ON c2.From_Equipment= Temp.Equipment)TEMP2
  WHERE (TEMP2.[Equipment] IS NOT NULL OR TEMP2.[Fault Valve] IS NOT
NULL);
END;
```

APPENDIX E

SQL Code for FMECA (Microsoft® SQL Server 2012)

```
select [Item Tag],

Name,

Description,

[Design Max Press],

[Design Min Press],

[Design Max Temp],

[Differential Press],

[Rated Capacity],

[Design Duty],

[MOC Class],

[Insul Purpose]

from fmea_eq;
```