An Integrated Method for Improving Risk Analysis Using Human Factors Methods and Virtual Reality

Dissertation

zur Erlangung des akademischen Grades

Doktoringenieurin oder Doktoringenieur (Dr.-Ing.)

angenommen durch die Fakultät für Informatik
der Otto-von-Guericke-Universität Magdeburg

von: M. Sc. Waleed Salem
geb. am: 02.09.1974 in: Ramtha

Gutachterinnen/Gutachter:

Prof. Dr. Andreas Nürnberger
Prof. Dr. Tom Kontogiannis
Prof. Dr. Teodor Winkler

Ort und Datum des Promotionskolloquiums: Magdeburg, 19.05.2009

Abstract

Increasing accident rates and system losses in different industrial sectors endanger safety, threaten economic growth and cause pollution damages. A major cause for these accidents and losses in the chemical process industry is the human error which contributes with a range of 60-90% in the development of these accidents. Conventional safety and risk analysis methods focus mainly on describing technological malfunctions and lack a systematic consideration of the human impact, i.e., the human error, on the process under consideration. These methods lack also a systematic utilisation of existing supporting and enabling technologies, e.g. virtual reality.

In this thesis, an integrated method for improving risk analysis is introduced. This method is developed by utilising human factors knowledge for a better inclusion of human impact in the risk analysis. It also utilises virtual reality as enabling technology that can be used as a medium for running relevant safety scenarios. The utilisation of human factors methods and virtual reality is based on an end user oriented approach of data collection, review and validation from the selected industrial domain (Chemical Process Industry).

Zusammenfassung

Steigende Unfallzahlen und Ausfälle von technischen Systemen in verschiedenen Industriebranchen gefährden die Sicherheit, bedrohen das Wirtschaftswachstum und tragen zur Umweltverschmutzung bei. Eine wesentliche Ursache für diese Unfälle und Verluste in der chemischen Prozessindustrie ist menschliches Versagen, das mit einem Anteil von 60-90% zu Entwicklung dieser Unfälle beiträgt. Konventionelle Methoden der Sicherheits- und Risikoanalyse fokussieren hauptsächlich auf die Beschreibung technischer Störungen und Abweichungen und ihnen fehlt eine systematische Berücksichtigung der menschlichen Einflüsse (d. h., der menschliche Fehler) im betrachteten Prozess. Des Weiteren fehlt diesen Methoden eine gezielte Nutzung vorhandener unterstützender Technologien, z. B., Virtual Reality.

In dieser Dissertation wird eine integrierte Methode zur Verbesserung der Risikoanalyse eingeführt. Diese Methode basiert auf eine Nutzung der Erkenntnisse der menschlichen Faktoren (Human Factors) zur verbesserten Einbeziehung der menschlichen Einflüsse in der Risikoanalyse. Die Methode nutzt auch die virtuelle Realität als technologische Umgebung zur Durchführung und Erprobung relevanter Sicherheitsszenarien. Die Nutzung der menschlichen Faktoren und die virtuelle Realität basieren auf einem Endnutzer-orientierten Verfahren zur Datenerhebung, Revision und Validierung aus der ausgewählten Industriebranche (chemische Prozessindustrie).

Table of contents

List of abbreviations

API	Application Programming Interface
ATHEANA	A Technique for Human Error Analysis
BD	Blow down
CREAM	Cognitive and Reliability Analysis Method
CPI	Chemical Process Industry
CPU	Central Processing Unit
EDM	Engineering Data Management
ESD	Emergency Shut Down
ET	Event Tree
EU	European Union
FT	Fault Tree
GPU	Graphical Processing Unit
HEI	Human Error Identification
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HR, HRA	Human Reliability, Human Reliability Analysis
HTA	Hierarchical Task Analysis
IEC Standard	International Electrotechnical Commission Standard
ITA	Initial Task Analysis
MARS	Major Accidents Reporting System
PDM	Product Data Management
P&ID	Piping & Instrumentation Diagram
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Analysis (Assessment)
PSFs/PIFs	Performance Shaping Factors/ Performance Influencing Factors
QRA	Quantitative Risk Assessment
RA	Risk Analysis
RCA	Root Cause Analysis
TA	Task Analysis
THERP	Technique for Human Error Rate Prediction
VE	Virtual Environment
VR	Virtual Reality

List of figures

List of tables

1 Introduction

This chapter provides an introduction to the underlying research by describing the motivation behind it (based on the current situation), goal definition and scope of the work, research domain and the reasons for selecting this particular domain. The chapter concludes by providing an overview of the contents of this thesis.

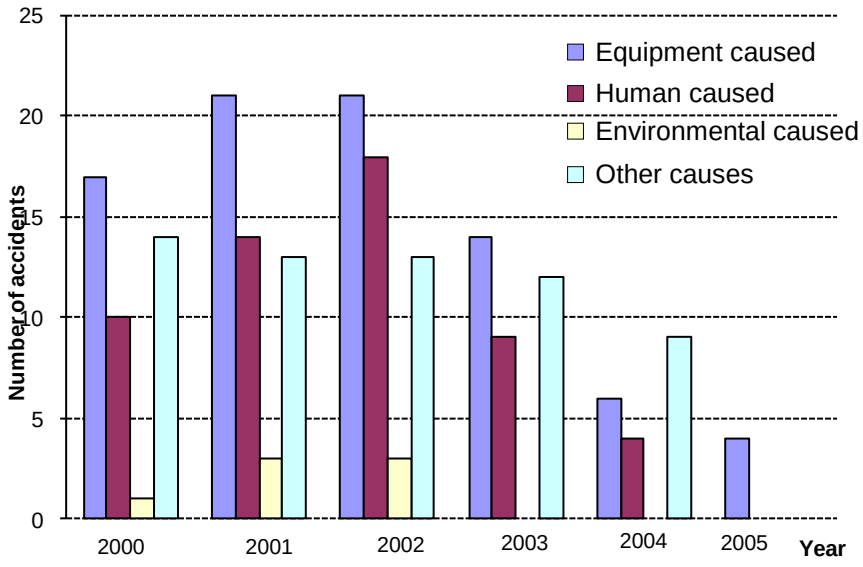
1.1 Motivation and current situation

After many years of continuous improvements in system design and safety methods and techniques, the technical and safety communities have realised that accident rates and system losses have reached limits which can be hardly reduced by improvements in system design or introducing new technical features to these systems. Even in organisations with good general safety records and risks awareness, occasional disasters do occur and shake public confidence in modern technological systems. The terrible explosion of ammonium nitrate which occurred in Toulouse on 21st September 2001 in AZF plant belonging to Grande Paroisse Company, TotalFinaElf Group represents an example of such disasters and major accidents. The accident led to the death of 30 people, 242 were injured (officially), 27,000 homes and 1,300 companies were damaged and the financial losses were in the range of 1,500 million Euros. This disaster has upset the public, traumatised an industrial city and led the politicians to close down the AZF plant which lead to cutting 450 direct jobs and the SNPE phosgene related activities which had the impact of cutting 492 direct jobs and 600 sub-contracting jobs (Dechy et al. 2004).

The common factor in both of these areas, i.e., system design and safety methods is the human error, which – according to recent studies on risk and safety analyses – contributes with a range of 60-90% in the development of accidents and losses in high risk production processes such as chemical and petrochemical industries (Hollnagel 1993; Rankin/Kirchbaum 1998). CCPS (2004) examined the magnitude of the human error problem and provided results of studies on the contribution of human error in chemical process industry (CPI). Below are some facts and figures according to (CCPS 2004):

- Human error accounted for 73% and 67% of total damage for boiler start-up and on-line explosions in oil industries;
- 58% of fire accidents in refineries are caused by human errors;
- The most common human errors include: improper repair, improper inspection, inadequate procedures, using improper material and misoperation.

In addition to that, a recent extraction from the MARS database (Major Accidents Reporting System) which classifies accidents into equipment caused, human caused and environment caused was also performed. The result is illustrated in Fig. **1.1** below. Knowing that some "equipment caused" accidents and the "other causes" accidents are highly probable to be originally caused by erroneous human actions, the aforementioned ranges of human contribution to accidents can be confirmed here.



Source[1] of data: JRC (2006)

Fig. 1.1: Causes of accidents reported in the MARS database until November 2006

As consequences of these human failures, 7.6 million accidents were recorded at work in 2001 in EU-15 countries where 4.9 million of these accidents resulted in more than three days absence from work and a total of 4,900 fatal accidents. The cost of accidents at work and occupational diseases in EU-15 for most countries ranges from 2.6 to 3.8% of Gross National Product (European Communities 2004).

According to (Cacciabue 2000) there are two reasons for this trend of higher human contribution in erroneous actions:

1. The very high reliability and refinement of mechanical and electronic components which enabled a reduction in the mechanical faults and also to manage all plant critical processes, even in the presence of system faults and malfunctions. This high reliability of hardware components has a direct impact on the statistical contribution

[1] No data entries were found for the years 2006, 2007 and 2008. Date: August 2008.

to accident of human errors, which become more and more visible in numerical importance.

2. The complexity of the system (automated systems) and the shift in the role assigned to human operator from the "pure manual operator" into the "supervisor" of plant operations, that are performed by computerised systems. Thus, the working environments are much more demanding in terms of cognitive-reasoning abilities rather than sensory-motor skills. These systems behave and respond via the automation and interfaces, which follow the rules and principles provided by their designers. These rules and principles are not always totally known or familiar to operators.

Risks and safety analysis methods have been (and are still being) traditionally conducted in a static and paper-based way based on a sequential accident model that describes accidents as the outcome of a chain of events that may even be assumed to occur in some fixed and imaginable order. In other words, these methods are based on domain experts' imaginations and their capability of defining as many risky situations as possible and then identifying the possible consequences of these risks.

An accident is thereby described as a series of linked cause-effect pairs, where the analysis begins from the last effect – the "accident" – and proceeds backwards until it finds the first – or "root" – cause. This procedure of analysing possible risk causes (also called root-cause analysis) and consequences is used in most common safety and risk analysis methods which include (among others):

- HAZOP (Hazards and Operability Study) (Cacciabue 2001; Shell 1995d)
- FMEA (Failure Modes and Effect Analysis) (Stamatis 2003; McDermott et al. 2008)
- FT (Fault Tree), ET (Event Tree) (Dhilon 2004; Shell 1995a)
- PHA (Preliminary Hazards Analysis) (Banerjee 2003; Vincoli 2006)

A closer examination of conventional risk and safety analysis methods identifies four major disadvantages of these methods:

1. They predominantly describe technological (mal)functions, which makes it difficult to adequately account for the impact of human – and organisational – factors. In other words, these methods do not incorporate models of human performance (e.g., CREAM: Cognitive Reliability and Error Analysis Method (Hollnagel 1998), ATHEANA: a Technique for Human Error Analysis (USNRC 2000), etc.) which can

be used to analyse the causes of the aforementioned accidents and risks as previously indicated, i.e., the "human error".

2. They cannot represent the outcome of events that have not already been included in the formal representation, i.e., unexpected conjunctions or confluences are excluded from analysis.

3. Risks are associated with identifiable components or functions (events), but not with coincidences and functional dependencies.

4. Their high dependency on experts' imagination which has its limitation apart from experience and skills.

In an attempt to overcome the first difficulty (which is the focus of the underlying thesis), some risk and safety analysis methods have rather straightforwardly added the human factor (HF)[2] – typically in the form of "human error" – hoping that this would make the analysis complete. Including the human error in risks and safety analyses is necessary for providing comprehensive analyses, but it is not sufficient for an integrated inclusion of human factors due to the following facts:

- Firstly, this solution of representing the human's impact on a process in the form of "error" has an embedded implication that humans can be treated as machines which is not true, since humans are not manipulable and disposable components of a system who can be adjusted and modified whenever needed;

- Secondly it ignores the concept of integrated human factors, i.e., modelling operator's behaviour, including performance conditions, considering the dynamic interaction between work context and human behaviour, including a recovery model for error detection and correction, etc. It is clear that the concept of integrated human factors comprises more than a minor individual element in an analysis, i.e., they should not be limited only to one component called "human error";

- Thirdly, this solution disregards the fact that human and organisational performances are not just possible sources of failures but are also an essential resource for system safety.

Based on that, it is evident now that sensible human actions and reactions provide the basic foundation for a system's stability throughout its life-cycle. Rather than simply

[2] Human Factors (simple definition): the study of how humans behave physically and psychologically in relation to particular environments, products, or services. A more contextual definition is provided in Chapter 2.

adding a human factors component to existing methods, e. g., "human error", human factors must therefore become an integral part of the foundations of risk and safety analysis methods. Today, to perform real *integrated risk analyses*[3], i.e., those including HF and provide sensible human actions and reactions, it is needed to have (Colombo 2006):

- Mock-ups of physical space in which operators work and
- Perform detailed on-job simulation and experimentation of the process: reactions, flows, process upsets, delays, etc.

Despite the fact that both of these pre-requisites are expensive and not feasible for long term planning, the former one is not flexible at all since every time the layout changes a new mock-up has to be built and the latter is time and effort consuming (and to some extent might be dangerous, if the experiment need to be performed using real interactions with risky situations). Even with the availability of these pre-requisites, they do not offer the possibility of visualising the consequences of an operational risk or an accident which limits the positive impact on operators' mind. Finally it is a further challenge to communicate and understand human factor issues due to their complex nature as they mostly deal with covert aspects of human behaviour, e.g., problem diagnosis, response and decision making, which is difficult to imagine or analyse in advance.

The illustrated difficulties stress the need to change from static and linear to more dynamic and systematic risk and accident analysis methods. These methods should be flexible and support utilising existing enabling technological media, e.g., Multimedia, Virtual Reality (VR), Process Simulators, etc.

1.2 Goal definition

As described in the "motivation and current situation" under Section 1.1, there is a need for introducing and implementing integrated methods for improving risk analysis for the purpose of reducing operational risks and hazards as well as to improve safety production. These integrated methods should take into consideration the aforementioned limitations and difficulties, i.e., the high dependency of risk analysis on experts' judgement, absence of the "human factor" in these analyses, difficulty of communicating and understanding HF issues, etc. In other words, an integrated method

[3] Risk analysis and its integration in the risk management process are explained in Chapter 2

should enable experimenting with risky situations by utilising HF methods in a way that enables an elaborate consideration of consequences and procedures to avoid these operational risks or reduce the losses associated with them.

A solution to this problematic "human caused operational risks and accidents" is introduced within the framework of this thesis and is based on experiencing safety critical situations in an environment which allows exploiting HF methods and concepts for reducing these risks and accidents. The ability of a Virtual Reality (VR) environment to represent objects and situations in a 3D interactive way makes it a suitable enabling environment (enabler) for this purpose.

Based on that, the goal of this thesis is to introduce an integrated method for improving risk analysis by using relevant HF methods and knowledge in a VR environment. In this context, the term *method* is defined to be "a way, technique, or process of or for doing something" (Merriam-Webster (2009)). An improved risk analysis plays a key role in reducing operational process risks and enhancing operational safety. This allows moving from the current static analysis of process risks and hazards (e.g., HAZOP, ET and FT methods (Cacciabue 2001; Shell 1995d; Dhilon 2004; Shell 1995a; Dien et al. 2004)) into a more dynamic analysis method. The integrated method consists of two main building blocks:

- The first block is the development of end user scenarios and requirements from the domain industry;

- The second block is applying a HF methodology for supporting risk analysis on the end users scenarios and requirements to identify functional specifications and requirements for supporting risk analysis using a VR environment.

The development of this integrated method is based on a HF methodology for supporting risk analysis that takes the human behaviour and performance into consideration. This methodology is developed within the framework of the underlying thesis and considered to be the first step in the work approach[4] used to produce the integrated method. This structure is illustrated in Fig. **1.2** by separating the HF methodology (the upper box in the figure) from the rest of the integrated method.

In addition to the development of these two blocks as main elements of the integrated method, a VR environment design is introduced as an implementation proposal. The

[4] To avoid terminology conflicts, the term "work approach" refers here to the way applied in developing the integrated method in the underlying thesis. The term "integrated method" refers to the resulting method itself as an output that can be further used by target users.

proposed VR environment design is based on standard VR components as well as additional software modules that are required to support particular functional requirements and specifications. Fig. **1.2** illustrates the approach applied in developing the proposed integrated method. The large green bounding box illustrates the integrated method itself whereas the small green bounding box illustrates the proposed VR environment design.

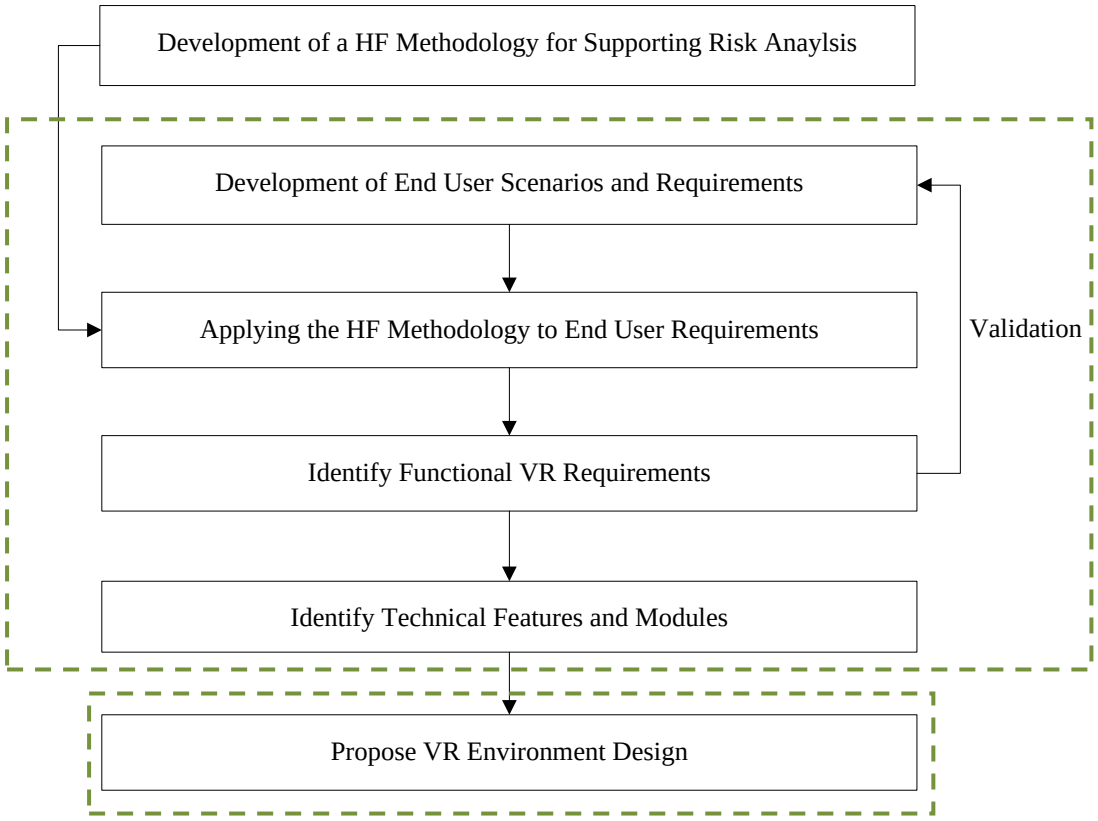


Fig. 1.2: The proposed integrated method for improving risk analysis (the large green bounding box) and the proposed VR environment design (the small green bounding box)

Since the global goal of this thesis is a human factors driven improvement of safety, it does not aim at introducing improvements or innovations in the VR technology: neither software nor hardware related. In this regard VR is considered as a communication process between human beings, mediated by computer systems, which uses interaction, visualisation and other sensory stimulation to convey information. Based on that, this thesis intends to introduce an enhanced usability of VR as an enabling technology for solving problems with high industrial and social impacts. This usability is moulded into a set of functional requirements and specifications as retrieved from field observations, i.e., application-oriented and end-user driven.

Fig. **1.3** illustrates the role of VR in the underlying work by acting as a bridge (representation medium) for bringing together the three key components that influence safety within the framework of this thesis: industrial needs (end user needs), risk

analysis and human factors. The double sided arrows in Fig. **1.3** illustrate that the aforementioned three components do not only influence the design of the VR environment (provide input), but also utilise this environment by acquiring knowledge and information regarding possible improvements (receive output). The Virtual Reality box in the figure has been assigned a brighter colour to emphasise the fact that virtual reality represents a medium of representation (enabler) here and not a point of research which is the case for the remaining dark coloured boxes of the figure.

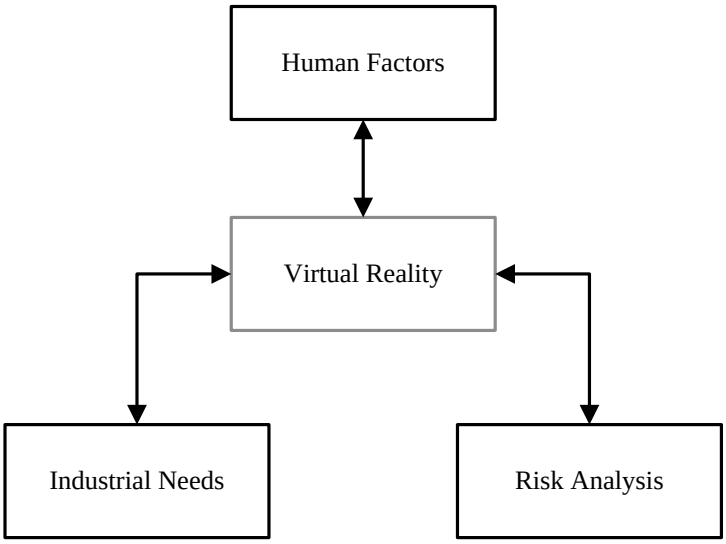


Fig. 1.3: The role of virtual reality as a representation medium among industrial needs, human factors and risk analysis

1.3 Description of the integrated method

It has been mentioned under "Goal definition" that the integrated method consists of two main building blocks, i.e., the development of end user scenarios and requirements and applying a HF methodology on the end users scenarios and requirements to identify functional specifications and requirements for supporting risk analysis using a VR environment.

The starting point (Fig. **1.2**) for the development of the integrated method was an analysis of existing HF methodologies regarding their support to risk analysis. This analysis concentrates on a justified selection of certain HF methodologies as shown in Chapter 2. Based on major limitations of the selected HF methodologies, an integrated methodology for supporting risk analysis is developed as shown in Chapter 3. The methodology is validated by applying it to a case study from the chemical process industry as shown in Chapter 6. Despite the fact, that this step is not considered as part

of the resulting integrated method, it has been mentioned here due to its elementary role for building the integrated method.

After the development of the HF methodology, a definition of end user requirements based on representative end user scenarios is carried out as shown in Chapter 4.

After having developed the HF methodology for supporting risk analysis and the definition of end user requirements, the HF methodology is applied to the end user requirements. This process requires three intermediate steps: clustering the HF methodology in terms of modelling nature (i.e., error modelling or performance modelling), definition of the functions covered by the clusters and mapping the end user requirements to the HF methodology as shown in Chapter 4. The identified functional VR requirements are validated (reviewed) against the end user requirements as shown in Chapter 6. By producing the final list of functional VR requirements, all the elements of the integrated method for improving risk analysis have been defined and can be utilised to propose a VR environment design that supports risk analysis.

To propose a VR environment design, an intermediate stage between the VR design and the functional requirements is required. In this intermediate stage a mapping of functional VR requirements to technical features and modules and the definition of a functional model that describes the interplays and information flow among the components of the VR environment takes place. This intermediate stage has been assigned to Chapter 4 and considered as the concluding part of identifying the functional VR requirements.

For the purpose of completion, a proposal for a VR environment design that supports risk analysis is introduced in Chapter 5. Despite the fact, that this VR environment design is not part of the integrated method introduced in this thesis, it utilises the information gained from the components of the method. The proposed VR environment design is not unique by its nature as it resembles existing VR systems in several components and aspects. Additional components that do not exist in standard VR systems distinguish the proposed design from other VR system designs as illustrated in Chapter 5.

The validation of the results is mainly based on the two building blocks of the method, i.e., validating the HF methodology and validating (reviewing) the end user requirements. A third validation block is dedicated to the proposed VR environment design as shown in Chapter 6.

1.4 Contributions

Introducing an integrated HF methodology for supporting risk analysis by considering the limitations of existing methodologies represents a major contribution from the human factors and industrial safety perspectives. The introduced methodology has been broken down into guidelines and taxonomies that facilitate applying it by safety analysts and consequently including human factors aspects in the analysis without being a HF expert. This represents a second important contribution that is lacking in existing human factors methodologies. A third contribution is the ability of the methodology to consider error recovery possibilities in the analysis and providing the analyst with feasible alternatives for error correction. A systematic consideration of error recovery is not supported in existing HF methodologies.

A fourth contribution is the end-user-driven definition of functional software requirements, i.e., functional VR requirements. The applied process of defining end users scenarios, extracting requirements out of these scenarios, applying a human factors methodology to the end user requirements and consequently identifying functional VR requirements is a unique process that ensures a high level of end user involvement in designing a software solution.

A fifth contribution is provided by the proposed VR environment design. Despite the standard components that constitute the core part of the design, some non-standard components and modules (e.g., process dynamics and analysis modules) have been included to cover specific aspects and functions. These functions have been highlighted by end users and are not supported in existing VR systems.

The sixth contribution is enhancing the usability of VR as a communication and representation medium by utilising it as enabler to solve problems with high industrial, human and social impacts.

1.5 Research domain

Due to the nature of the work in the “process industry” which is characterised by being risky through manufacturing and transporting dangerous, high-temperature and chemically reactive materials, the research domain is the “process industry”. By definition, a process industry is an industry in which raw materials are treated or prepared in a series of stages, e.g. using chemical processes. A more descriptive definition is provided by (Lager (2002), pp. 108) and (Chronéer (2005), pp. 6) which states:

"Process Industry is a part of Manufacturing Industry using (raw) materials to manufacture non-assembled products in a production process where the (raw) materials are processes in a production plant where different unit operations often take place in a fluid form and the different processes are connected in a continuous flow. The concept of Process Industry is also used regarding the whole industry in general, though it should be noted that many different types of process industries dealing with different products/material properties exist in Process Industry, e.g. steel, paper, chemical, etc." Typical industries which fall into the category of process industry include:

- Oil and gas refining
- Petrochemicals
- Water and sewage treatment
- Food processing, and
- Pharmaceuticals

Based on that, all collected data which are used to reach the goals of this thesis stem from the process industry domain. Further clarifications to the origin of the data are provided accordingly in the subsequent chapters and sections.

1.6 Structure of the document

For each chapter and some longer sections of this document, an introductory part and a definition of the major related terms are provided at the beginning of that particular chapter or section. Each chapter and some long sections are concluded by a summary.

In Chapter 2, a comprehensive literature review regarding the building blocks of the underlying thesis (as shown in Fig. **1.3**) is given. This literature review represents a state-of-the-art and review of related works on:

- Process Risks: overview, risk management process, risk analysis (assessment) methods, operational phase of the production (or process) life cycle, etc.
- Human Reliability and Human Factors: overview, screening of most popular and widely used human factors methods, generations and shortcomings of Human Reliability Analysis (HRA) methods, etc.

- Virtual Reality: overview, reasons for selecting VR as enabling technology in the underlying thesis, surveys on selected VR systems and solutions: their areas of applications, their shortcomings, etc.

In Chapter 3, a HF methodology for supporting risk analysis is introduced. This methodology is based on an analysis of peculiarities and limitations of selected methods which could be applied for risk analysis and covers the methods THERP, CREAM and ATHEANA which belong to the well established and widely applied first and second generation methods of human reliability analysis (Kim 2001; Konstandinidou et al. 2006; Kim et al. 2006; USNRC 2005). In Chapter 4, the functional specifications and requirements for supporting the performance of risk analysis in a VR environment are developed. In a similar way to Chapter 3, the results and findings of this chapter are end-user driven and based on field observations and dedicated workshops with end users and safety analysts from the industrial domain.

In Chapter 5, a proposal for a VR environment design which can be used as a medium (tool) for supporting the performance of risk assessment and analysis based on the findings in Chapter 3 and 4 is introduced. In Chapter 6, a validation of the findings is carried out and structured in three parts: validation of the HF methodology by applying it to a case study from the research domain (i.e., validation of the results of Chapter 3), validation (review) of the end user requirements and the functional VR requirements (i.e., validation of the results of Chapter 4) and validation of the proposed VR environment design (i.e., validation of the results of Chapter 5).

Finally, a summary of the results together with future developments based on these results are provided in Chapter 7.

2
State-of-the-art and related work

This chapter provides an overview of works that are related to the underlying thesis and serves as a review on state-of-the-art on the three major components of this work (as defined in Fig. **1.3**) which are: safety (risks), human factors and virtual reality.

Section 2.1 introduces process risks and current methods of performing risk analysis (assessment). In Section 2.2, human factors methods and techniques are presented and discussed and linked to risk analysis. Finally, Section 2.3 provides an overview on virtual reality: state-of-the-art in relation to the topics of this thesis, features, shortcomings of available VR systems, etc.

Before proceeding into the definition of risk and the subsequent necessary explanations in Section 2.1, it is necessary to mention that the term "risk" is being used here within the global context of "safety", i.e., "risks" represent dangers to safety and should be minimised. However, since the expression "reducing risks" within the context of safety implies "improving safety", both of these terms have the same implication within the framework of this thesis. Based on that, in the next chapters and sections, the focus is on the expression "reducing risks" for the purpose of consistency with the title and the goal of this thesis.

2.1 Risks, risk management and risk analysis

Since the term "risks" together with some other related terms are frequently used in this section and the entire document, a definition of these terms is provided in the next subsection to avoid any confusion in the interpretation of these terms.

2.1.1 Definitions

Within the area of system reliability and dependability management, the International Electrotechnical Commission (IEC) introduced the standard IEC 60300-3-9[5] which provides guidelines for selecting and implementing risk analysis techniques, primarily for risk assessment of technological systems. This standard defines the term "risks" and some related terms as follows (IEC (2006), pp. 9):

- *Risk* is defined as "a combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event".

[5] The International Organisation for Standardisation (ISO) and IEC work on developing joint standards in the area of risk management, e.g., ISO/IEC Guide 51 and ISO/IEC Guide 73.

- *Risk analysis* is “the systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment”.

- *Risk management* is “the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk”. Related to this definition and according to (Harms-Ringdahl (2004), pp. 14), risk management and safety management are used in varied ways and are often seen as identical.

In several types of industries, e.g., process industry, the word *safety management* is preferred and defined to be the aspect of the overall management function that determines and implements the safety policy. This involves a whole range of activities, initiatives, programs, etc., focused on technical, human and organisational aspects and referring to all the individual activities within the organisation, which tend to be formalised as Safety Management Systems (Papadakis/Amendola 1997).

Based on that a more specific definition of *risk analysis* is adopted in the chemical process industry and described to be “a systematic procedure for analysing systems to identify and evaluate hazards and safety characteristics” (Harms-Ringdahl (2004), pp. 14).

2.1.2 Types of risks

The wide diversity of types of risks makes it impossible to cover all of them within the framework of this thesis. A closer literature review (Sadgrove 2005; Fragniere/Sullivan 2006; Streffer et al. 2004) on main types of risks (or risk families) can be summarised below:

- Compliance risks, e.g. the risk of failing to meet government standards or laws and regulations, or failing to meet international treaties.

- External risks, e.g. risks from economic shocks, changing public attitudes or EU legislation.

- Financial risks, e.g. risks arising from spending on capital projects or fraud or impropriety; risks from failed resource bids and insufficient resources.

- Foresight risks, e.g. risks arising from insufficient forward planning or horizon-scanning.

- Operational risks[6], e.g. risks arising during the operation phase of a process or a product.
- Project risks, e.g. risks of equipment exceeding budgets or projects missing key deadlines.
- Reputation risks, e.g. risks from damage to the organisation's credibility (reputation).
- Strategic risks, e.g. risks arising from policy decisions or major decisions affecting organisational priorities; risks arising from senior-level decisions on priorities.

It is necessary to mention that the operational risks under consideration in this thesis represent risks with direct impact on human, environment or the technical system (safety related risks) during the operational phase of the process lifecycle. These risks should not be confused with other operational risks like risks or security issues in IT infrastructure, risks associated with the delivery of a particular service, banking or operational financial risks which are out of the scope of this thesis. This focus on operational risks is due to the following reasons:

- The operation phase represents the "productive phase" in the chemical process industry in which an outcome, e.g., liquefied natural gas, liquefied petroleum gas, etc. is being generated and a major return on investment can be achieved by selling this outcome to the customers.
- The operation phase represents the long-lasting phase among the other phases of the process life cycle and consequently represents a permanent source of risks.
- The largest portion of workforce is allocated to the operation phase which consequently raises the risks' opportunities compared to other phases in which lower workforce rates are allocated.
- To enhance a precise goal definition and illustrate the boundaries of this thesis.

Focusing on the risks in the operation phase of the process life cycle does not imply that the remaining phases are free of risks. It is only an indication that risks during the remaining phases are not a subject of research in this thesis. Fig. **2.1** shows the process life cycle with the operation phase in bold text to address the aforementioned focus on risks during this phase.

[6] Basel II provides a definition of operational risks which is widely accepted in banking industries: "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Chorafas (2004), pp. 3).

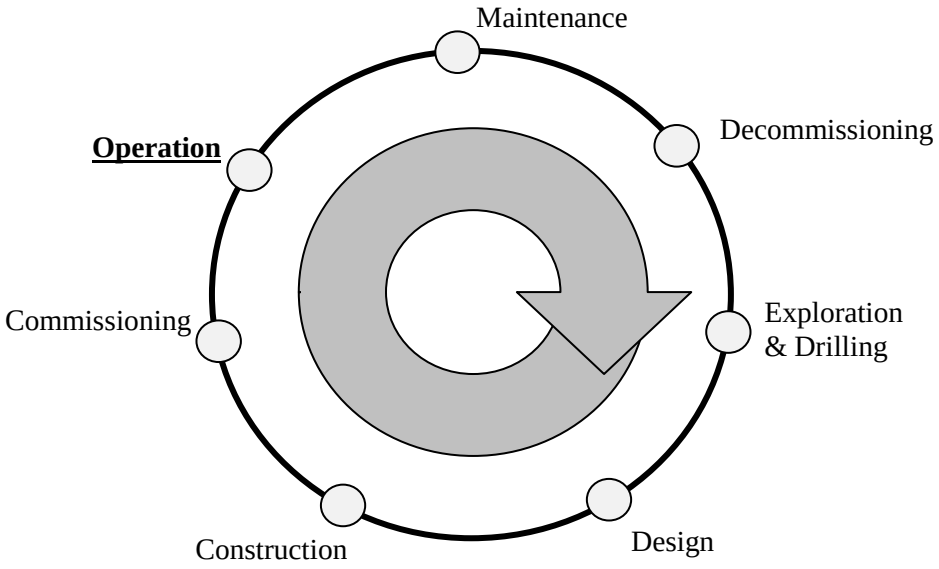


Fig. 2.1: The process life cycle and the focus on the operation phase (bold underlined text)

2.1.3 Risk management process

A continuous risk management process helps organisations to understand, manage, and communicate risks so that their negative impacts and the associated losses can be kept as low as possible. A typical risk management process can be divided into four phases (TBCS 2004) as listed below:

1. Risk Identification
2. Risk Analysis
3. Risk Response
4. Risk Evaluation and Monitoring

Fig. **2.2** below illustrates that the four phases cannot be separately considered since their continuation represents an integrated risk management cycle which is necessary for a complete understanding, managing and communicating the identified risks as described above.

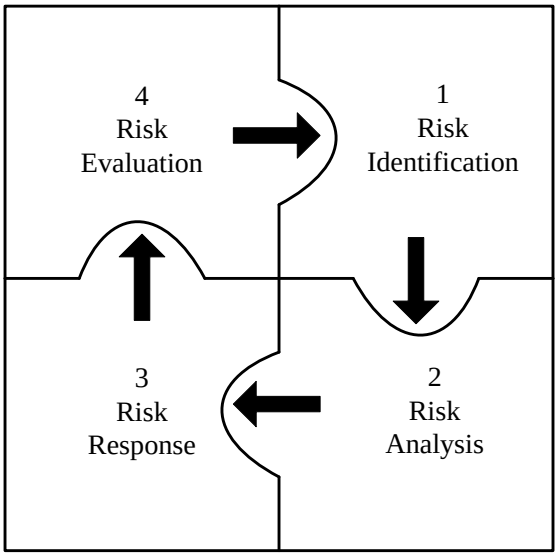


Fig. 2.2: The risk management process

A further goal for dividing the risk management process into four phases, as shown in Fig. **2.2**, is also to illustrate the role of "risk analysis"- which constitutes to the first building block of this thesis as described in Chapter 1 and Fig. **1.3** - within the global context of risk management. This confirms the fact that risk analysis is a step in the risk management process, which is further illustrated in the subsequent sections by addressing this phase in more details and whenever it becomes necessary to include information about the remaining three phases for the purpose of clarification and completion.

2.1.4 Risk analysis

In Section 2.1.1 "risk analysis" was defined to be the systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment. In this section a deeper look into risk analysis is provided: stages of risk analysis, methods and techniques of risk analysis as well as the drawbacks of these methods and techniques.

The risk analysis process in the process industry domain can be decomposed into the following main phases:

- Hazard identification, i.e., identify hazards and potential hazardous events (top events, Section 2.1.6.1)
- Hazards analysis, i.e., analyse hazards and potential hazardous events using:

- Event analysis (likelihood per event, Section 2.1.6.2)
- Consequence analysis (to people, environment and assets, Section 2.1.6.3)
- Exposure analysis (likelihood of exposure, Section 2.1.6.3)

Once the hazards have been analysed, an assessment of these hazards can take place for the purpose of interpreting the results and recommending corrective actions. The process of analysing and assessing risks is called risk assessment. Since only a thin barrier exists between "risk analysis" and "risk assessment", both terms are used widely in the literature to imply the same meaning. Based on that and for the purpose of consistency, the term "risk analysis" is used further in the remaining part of this document and includes the assessment part as described above.

2.1.5 Risk analysis methods (RA methods)

Risk analysis methods and techniques vary widely in complexity, from simple, qualitative approaches to fully quantitative approaches. Once hazards and hazardous events have been identified, their causes, consequences and probability can be estimated and the risk determined by applying the same procedure. Qualitative methods may be adequate for risk assessments of simple facilities or operations where the exposure of the workforce, public, environment or the asset is low and a more accurate determination of likelihoods is not relevant. However, the application of quantitative methods (QRA) is considered to be desirable when (Shell 1995a):

- several risk reduction options have been identified whose relative effectiveness is not obvious;
- the exposure to the workforce, public, environment or the strategic value of the asset is high, and reduction measures are to be evaluated;
- equipment spacing allows significant risk of escalation;
- novel technology is involved resulting in a perceived high level of risk for which no historical data is available (e.g., deep water developments in hostile environments);
- demonstration of relative risk levels and their causes to the workforce is needed to make them more conscious of the risks.

The application of QRA should not be limited to large complex expensive studies. It is a technique which can be used to help structure the solution to problems for which the solutions are not intuitively obvious.

Since the HF methodology for supporting risk analysis, which is developed within the framework of this thesis, aims at supporting the performance of quantitative risk analysis, the examination in the next sections and subsections focuses on quantitative risk analysis methods and techniques.

2.1.6 Quantitative risk analysis (QRA)

Quantitative risk analysis (QRA) - which is also called probabilistic risk analysis (PRA), probabilistic safety analysis (PSA) or quantitative safety analysis (QSA) (Harms-Ringdahl 2004; Cacciabue 2000) - provides a structured approach for assessing the potential for incidents and expressing this potential numerically. In QRA statistical values are derived for potential loss of life and damage to resources and environment. These values should not be interpreted as unavoidable and acceptable losses resulting from the operations considered, but as a guideline to measure safety, to raise awareness for the potential of accidents and thereby developing measures to prevent lives and assets.

Since different methods and techniques are applied for each step in the QRA, it is necessary to zoom into the RA phase which was introduced in Section 2.1.3 (Fig. **2.2**) and investigate the methods and techniques which are currently used so that the weaknesses and shortcomings of these methods and techniques in supporting risk analysis can be identified.

2.1.6.1 Identify hazards and potential hazardous events

The potentially hazardous event is usually called the “top event”. Examples of such top events in the process industry include:

- Gas leakage from process equipment, risers or pipelines
- Extreme environmental loads
- Escalation of fire
- Explosions in buildings

- Outdoors explosions

Many approaches and techniques exist to identify hazards and top events, e.g., Hazard Identification (HAZID), Hazard and Operability studies (HAZOP), Fire and Explosion Analysis (FEA), Job Hazard Analysis (JHA), etc. Due to their wide diversity, the examination in this section is limited to the HAZID and HAZOP methods which are most established and being widely used in the process industry as formal techniques (Shell 1995a). Annex A describes the layout of the HAZID and HAZOP techniques together with an example on each of them.

Limitations and shortcomings of HAZID and HAZOP methods:

Despite that the HAZID and HAZOP methods represent systematic methods for identifying hazards or hazardous events (deviations) and are widely used in industrial domains characterised by risky environments, these methods suffer from several shortcomings. These shortcomings are mainly due to the imaginative and brainstorming nature of both methods and include:

- A main weakness of both methods is that the same group of experts identifies both hazards and mitigating measures or controls, whereas a different group of experts may better serve the latter function.

- It is difficult to assign to each guide word (the first column of the HAZID or HAZOP sheet as shown in Table **A.1** and Table **A.2**) a well-delineated portion of the system and failure causes.

- Errors can be made in the analysis, in particular if the group becomes tired or fatigued. Consequently hazards may be overlooked and the study may become incomplete or erroneous.

- Their success heavily depends on the facilitation of the team leader as well as the knowledge, experience and degree of co-operation and commitment of the team.

- Difficulty in dealing with multiple failures (hazardous events or deviations) due to the inability of both methods in representing dependency between failures which might be a hidden risk factor.

- Both methods analyse single events or deviations without investigating interrelationships between events or linking them.

- The HAZOP method is optimised for process hazards, and needs modification to cover other types of hazards, e.g., hygiene and occupational hazards.

- Both methods require the existence or development of procedural descriptions, which are often not available in appropriate detail or not updated to reflect the current way of performing operations.

- Documentation of results is a manual and time consuming process which might negatively affect the comprehensiveness and completion of the study.

- Both methods analyse causes and effects with respect to deviations from expected system behaviour, but they do not analyse whether the design, under normal operating conditions, yields expected behaviour or if the expected behaviour is what is desired.

- Both methods represent stand alone and qualitative tools for identifying hazards and deviations. For a complete and quantified risk analysis, the methods either need to be modified or additional methods should be used.

- Both methods assess the hazard potential of technological malfunctions and mal-operations and the consequential effects. They provide no assessment of the hazard potential as a result of faulty human action or interaction, i.e., no incorporation of human factors models or methods is considered in both methods (more about human factors in Section 2.2).

2.1.6.2 Development of top events into incident scenarios and estimation of frequencies

Hazardous events themselves do not necessarily cause loss of life or damage; it is their development into incidents which lead to losses. The development of the top event into a serious incident depends on the effect of mitigating factors, e.g., availability of an ignition source close to leakage, wrong intervention by operator, fail in the emergency shutdown system (ESD), etc.

The most known technique to project the development of top events into incidents is Event Tree technique (ET) (Dien et al. 2004). An ET provides a diagrammatic and systematic presentation of this development and makes it possible to include opinions of experienced personnel. A brief description and an example on ET are provided in Annex B.

Limitations and shortcomings of ET method:

- A time consuming method as for each top event from the HAZID or HAZOP, an event tree needs to be created and analysed.
- The need for making assumptions regarding the ways in which equipments and facilities are operated and maintained during the construction and analysis of event trees, makes the production of event trees only possible if experienced persons are involved.
- The major source of data for obtaining the probabilities in this method is historical data which contributes to a major uncertainty of this method since the operating conditions in which the event happened in the past might change and consequently the probability is no more valid.
- The alternative source of data when historical data is not available by relying on experts' opinions and estimation is subjective and could not be validated which adds a further uncertainty to this method.
- Numerous pitfalls might happen, particularly for inexperienced users. For example, focusing on extracting the required probability from a fault tree and ignoring the dependence between events in fault and event trees can lead to errors of several orders of magnitude. In an analogous manner, the effect of events' overlapping from different trees is not considered in an event tree and might lead to unpredicted problems or incidents.
- Human interventions could be taken into account in an event tree either as an extra branch or by updating the actual probability assigned to each branch to reflect this manual intervention. In the first case, a complex event tree is created which complicates the analysis. In the latter case, the uncertainty of the entered value increases since the original failure probability is merged with a probability of human intervention.
- The action or inaction of people during an emergency can have a profound effect on how the incident scenarios may develop and on the resulting consequences. In other words, the event tree might have a different "end event" than the assumed one because people behaved or acted in an unpredicted manner.
- Some component failure probabilities depend on process variables during operation, e.g., pressure, temperature, liquid concentration, etc. which calls for a simultaneous inclusion of these variables in the event tree so that a comprehensive evaluation of

the event tree is possible. The same considerations apply to human interventions (see previous point on human intervention).

2.1.6.3 Assessment of consequences and calculation of potential loss from incident scenarios

Since the focus of the underlying thesis is on improving the way of performing the first two steps of risk analysis which were detailed under 2.1.6.1 and 2.1.6.2, the assessment of consequences and calculation of potential loss from incident scenarios are considered to be out of the scope of this thesis and were mentioned here for the purpose of completing the risk analysis cycle. It is also worth mentioning that the assessment of consequences is context and application dependant, i.e., depends on the type of "end event" which is adequately documented in the literature ((IChemE 2008; Robson/Toscano 2007; Nivolianitou/Kefalas 2005).

2.1.7 Summary of Section 2.1

Besides providing definitions of terms which are widely used in risk and safety analysis community and are necessary for this thesis, this section provided an overview of the risk management process and explained how the risk analysis is integrated into this process. A clarification regarding types of risks and operational process risks – which are the focus of the underlying thesis – was also given.

After this introductory part, a deeper look into risk analysis was made: its phases, methods and techniques applied as well as examples on these methods. A special attention was paid to QRA due to its wide use in the process industry for quantifying and analysing risks.

It was clear from the review of QRA techniques and methods in Sections 2.1.5 and 2.1.6 that these methods are time consuming and highly dependent on expert's imaginations and judgments to reach their intended goal which represents a subjective and inflexible way of conducting risk analysis work. Furthermore it was also shown that QRA provides a crude analysis of barrier performance, emphasising mostly technological and process aspects rather than other risk influencing factors such as human and organisational aspects. These shortcomings represent requirements for the methodology and the definition of functional VR requirements which is introduced in Chapter 3 and 4. A further analysis of the human-related aspects and the influencing factors is discussed and analysed in Section 2.2.

2.2 Human Reliability (HR) and Human Factors (HF)

This section provides an overview about human reliability and human factors: methods & techniques, their link to risk analysis (Section 2.1) as well as the link between human factors (HF) and human reliability analysis (HRA). The section focuses on the methods[7] which are relevant for the underlying thesis and also introduces their limitations as a preliminary step for introducing the methodology in Chapter 3.

Since the terms human factors (HF), human reliability (HR), human error, together with some other related terms are frequently used in this section and the entire document, a definition of these terms is provided in the next subsection to avoid any confusion in the interpretation of these terms.

2.2.1 Definitions

According to (Cacciabue (2004), pp. 12) *human factors* are "the technology concerned with the analysis and optimisation of the relationship between people and their activities, by the integration of human sciences and engineering in systematic applications, in consideration for cognitive aspects and socio-technical working contexts".

By this definition human factors science extends the concept of "ergonomics" - as the science of humans at work - beyond the workplace by including cognitive and social aspects involved in human activity (Edwards 1988).

According to (cf. Cacciabue (2004), pp. 13) in the definition of human factors, they are conceived as "technology" to emphasise their practical nature rather than their disciplinary character. He considers the difference between human factors and human sciences as the same that exists between engineering and physics. Physics and human sciences look at the basic principles and fundamental criteria that govern their locus of interest, while engineering and human factors concentrate on the implementation of these principles and criteria in the real world and working environment.

Human reliability is defined as "the probability that a person will correctly perform some system-required activity during a given time period (if time is a limiting factor)

[7] The term "methods", "techniques" and "approaches" of HF and HRA will imply the same contextual meaning in this document.

without performing any extraneous activity that can degrade the system" (Karwowski (2006), pp. 753).

Human reliability analysis is the identification of human error opportunities that may affect system risks, the quantification of their likelihoods and determination of how to reduce those likelihoods if needed (cf. Kirwan (1996), pp. 360 et seqq.; Karwowski (2006), pp. 753 et seqq.).

Human error is defined to be "the post-hoc attribution of a cause to an observed outcome, where the cause refers to a human action or performance characteristic" (Hollnagel (1998), pp. 160). Hollnagel (1993) uses the terms "erroneous actions" and "performance failures" instead of "error" since the word "error" does not have a unique meaning and it has been historically used to denote either the cause of something, the action or the outcome of the action. In this context, the term "*cognitive errors"* is also used to refer to errors resulting from cognition.

Human error probability is the number of times a human error occurs divided by the number of opportunities for that error (cf. Kirwan (1996), pp. 360).

Performance shaping factors are the aspects of the operational system that influence human performance (negatively or positively), e.g., adequate training, stress, time pressure, managerial attitudes, organisational factors, cultural differences, etc.

2.2.2 Human Reliability Analysis (HRA)

Human reliability analysis can be seen as a specialised scientific sub-field or a kind of hybrid between psychology, human factors and engineering reliability analysis (risk analysis) (Hollnagel 1998). From the viewpoint of the underlying thesis, HRA is considered as an intermediate link between quantitative risk analysis and human factors as shown in Fig. **2.3**[8]. Furthermore and in order to stress the role of the human in the HRA rather than its analytical approaches and quantification of errors, HRA was not discussed in Section 2.1 (Risk Analysis) and alternatively is discussed in this section (Human Factors). In other words, within the framework of this thesis, methods of HRA are considered as human factors methods rather than methods of quantitative risk analysis.

[8] This representation does not aim at eliminating the role of psychology in HRA. It will not be considered here since it represents a science in itself which is beyond the scope of this thesis.

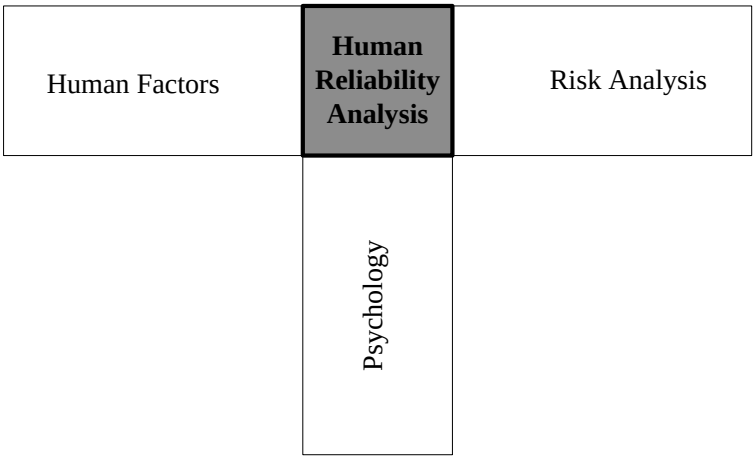


Fig. 2.3: Human Reliability Analysis as a hybrid between Human Factors, Psychology and Risk Analysis

Due to the subjectivity of the methods used to evaluate human reliability and the uncertainty of data concerning human factors, HRA has always been a serious concern for safety experts and risk analysts. Nevertheless, all HRA methods and approaches share the need to develop ways of estimating human error probabilities. As a result, many studies have been performed to produce data sets or databases which can be used as a reference for determining or extracting human error probabilities (HEP) (26: Fujita/Hollnagel 2004).

Since the introduction of the first HRA methods in mid seventies, HRA methods were classified into first generation methods and second generation methods[9] (Swain 1990). The methods of the first generation, e.g., THERP, were highly influenced by the QRA approach (Kim 2001), i.e., aimed at quantifying human errors in order to establish an integrated assessment of plant risk. The methods of the second generation, e.g., ATHEANA, CREAM, account explicitly for how the performance conditions affect performance, i.e., modelling errors and error mechanisms into the risk analysis process (Kontogiannis 1997).

Sections 2.2.3 and 2.2.4 provide a closer look into characteristics and shortcomings of the methods of each generation. It provides also examples on the best known and most used methods of both generations.

[9] Due to their focus on the task itself and the information processing related to perform task, first generation methods are also called Information Processing Approaches (IPA) whereas second generation methods are referred to as Contextual Approaches (CA) due to their focus on the context of performing a particular task.

2.2.3 1st Generation of HRA methods and techniques

1st generation HRA methods have been established and developed until early-1990s. These methods share the following characteristics:

- Focus on human error during performance of a task;
- Emphasise on quantification, i.e., assign probabilities of failure of an operator in performing a task;
- Each method was developed to serve a specific need;
- Provide reference data on human error probability, e.g., databases on human error probabilities (THERP).

According to surveys and analyses provided by (Kirwan 1994; Gertman/Blackman 1994; Spurgin/Moieni 1991; Swain 1989; Haney et al. 1989), more than 30 distinguishable HRA approaches have been classified to belong to the first generation. Annex C provides a list of the most known methods of 1st generation HRA and an example on these methods.

1st generation methods – represented by THERP as shown in Annex C – attempted to account for the complexity of interaction between humans and machines in order to extract HEP which can be integrated in the overall RA process. Since all of the methods have been developed to solve a specific need, most of them were (and are still) used. The THERP method belongs to these widely used approaches not only due to its rich database of human error probabilities that is used as data reference for many safety analysts, but also to its way of describing how events should be modelled (event tree) and quantified.

2.2.3.1 Limitations and shortcomings of 1st generation methods

All limitations of 1st generation methods are based on the central concept around which these methods were built, namely the concept of human error in performing a task. In other words, the task characteristics – captured quantitatively as HEP – are regarded as the most influential element for the estimation of human failure whereas the environment in which the task is performed (context) - represented by the performance shaping factors (PSFs) - is considered as a minor corrective factor (Marseguerra et al. 2006). Based on that, the following limitations and shortcomings of 1st generation HRA

methods were also identified (Hollnagel 1998; Leveson 1995; Kirwan 1996; Swain 1990; Kim 2001; Dougherty 1990):

- The methods do not have a well developed theoretical basis in terms of a model of human cognition and/or a corresponding classification scheme of human errors. In other words the methods lack an adequate theoretical treatment and categorisation of cognitive errors.
- The methods attempt to model human and environmental factors, but they fail to link them with failures in the technical systems.
- The methods which include PSF suffer from relatively unstructured and very flexible process of considering PSFs which depends on subjective assessor's evaluation. Many assessors rarely use the PSF, and tend to use the "stress" PSF as a generic one influencing the HEP.
- Inadequate treatment of some important PSFs in the methods, e.g., managerial attitudes, organisational factors, cultural differences, etc.
- Demonstrations of the accuracy of the methods for real world predictions are almost non-existent, particularly for non-routine tasks.
- Inadequate realism in many methods due to questionable assumptions about human behaviour.
- Some of the methods base their quantification process on the assumption that a human reliability can be described as equipment reliability, i.e., binary representation of human actions, which is no more applicable, particularly in a cognitively demanding task environment such as a chemical plant.
- Highly influenced by QRA, i.e., the HRA is performed within the envelope of QRA (also called PSA-cum-HRA (cf. Kim (2001), pp. 1070 et seqq.) which does not support the larger perspective where humans are involved in the design, construction, operation, maintenance and management of a system. As a result the HRA only considers the human actions that are only included in the QRA event trees. Consequently, the quality of the HRA depends on the completeness and accuracy of QRA modelling which adds a restriction on a successful implementation of the HRA.
- Many domain experts consider first generation methods as inadequate for HRA modelling and can lead to increased risk or wasted risk management.

The development of 2nd generation HRA methods took into consideration many of the listed shortcomings and weaknesses of 1st generation methods into account as described in the next section.

2.2.4 2nd Generation of HRA methods and techniques

To overcome the shortcomings of the 1st generation methods, 2nd generation methods of HRA have been (and are still being) developed. Unlike 1st generation methods which focused on the task rather than the context, the 2nd generation methods pay special attention to the contextual conditions in which the task is performed which is considered to be of greater importance than the task itself (Marseguerra et al. 2006).

Methods of this generation are characterised by being based on a multidisciplinary framework (cf. Konstandinidou et al. (2006), pp. 706 et seqq.) which considers both the performance shaping factors and the conditions of the plant as the factors that give rise to the need of actions and create the operational causes for human system interactions. Dougherty (1990) and Hollnagel/Wreathall (1996) described an important need in second generation HRA methods which is the need to go beyond the PSA-cum-HRA construct that represented a constraint in first generation methods (refer also to the previous section). This is because the PSA-cum-HRA is not capable of modelling characteristics of the plant beyond the "as-built" or "as-operated" concept.

Compared to 1st generation methods, 2nd generation methods provide – with different degrees of complexity and applicability – the following features to support human reliability analysis (Hollnagel 1998):

- Enhanced QRA event trees compared to those of first generation, e.g., by combining the results of more than one event tree or introducing a feedback loop from the human reliability analysis to the event tree (cf. Hollnagel, pp. 148);
- Diversified and extended treatment of errors by definition of error modes;
- Expanded treatment of performance shaping factors by integrating their influence at an early stage of the analysis rather than in the form of adjusting HEP as done in 1st generation methods.

Among the wide variety of HRA methods which can be classified as 2nd generation HRA methods, a list of some of these methods is provided in Annex D. CREAM and ATHEANA are considered to be the best known methods of this generation (cf. Kim 2001, pp. 1069 et seqq.; cf. Konstandinidou et al. 2006, pp. 706 et seqq.; cf. Kim et al.

2006, pp. 191 et seqq.; cf. USNRC 2005, pp. 2-2). These two methods are presented here as representative methods of second generation HRA for the purpose of comparing with methods of 1st generation HRA and completing this literature review. This serves also as a base for the HF methodology which is developed in Chapter 3.

2.2.4.1 Limitations and shortcomings of 2nd generation methods

2nd generation methods emphasise that the likelihood of something being done incorrectly is determined by the performance conditions and not by an inherent human error probability as described in 1st generation methods. However, methods of this generation are still under development to account for several limitations and shortcomings as described below (Pyy 2000; Kim 2001; Hollnagel 1998; Forester et al. 2004; Kim 2006):

- The methods provide systematic methodological frameworks but still suffer from subjectivity due to lack of information needed to apply the methods, i.e., dependence on expert's judgments and qualitative estimations. The developer of CREAM (Hollnagel 1998) confirms this fact as a shortcoming of 2nd generation HRA methods which requires further developments and improvements in the methods.

- The methods try to model causal mechanisms of events and actions that include a considerable amount of randomness. This calls for a wider application of these methods in industrial domains to provide practical basis for additional improvements in these methods to find practical solutions of the randomness effect.

- The methods provide detailed procedures which are very useful in retrospective analysis of a small number of human failure events. For a predictive analysis, a large number of human actions or failure events should be analysed. Consequently these methods should be accompanied with a very detailed analysis – which is not always available or possible for the situations to be analysed – to achieve the envisaged goals and results in risk analysis.

- ATHEANA and CREAM do not provide explicit consideration of recovering human erroneous actions which is extremely necessary in analysing human reliability.

- With an exception to CREAM, methods of this generation provide no clear distinction between phenotypes (manifestation) and genotypes (causes).

- ATHEANA lacks the availability of an accepted model of human behaviour suitable for supporting the quantification of human actions. ATHEANA suggests in its final

steps of the quantification process (as presented in (USNRC 2000)) that analysts translate the important contextual information identified with the search process into human error probabilities (HEPs) using existing HRA methods such as THERP. As a result significant judgment must be exercised by the analysts performing the quantification which contributes to the ATHEANA's subjectivity in quantifying human actions and treating uncertainty.

- ATHEANA's analysis begins with an HFE identified from PSA accident sequence analysis which leads to classifying the method as PSA-oriented. As a consequence, ATHEANA has the PSA-cum-HRA drawback which was presented in Section 2.2.3.1 and thus limits modelling the consequences of human errors only to the pre-identified ones in the PSA accident sequence.

- The theoretical background of ATHEANA seems rather weak for predictive analysis and makes this method more suitable for retrospective analysis (post-accident analysis). This is due to the nature of cognitive engineering models which are used in ATHEANA and assume that most post-accident erroneous actions are cognitive errors. (see also next point).

- CREAM was developed originally for retrospective analysis like ATHEANA and needs further improvements to suit predictive analyses.

- The division of degree of control into four categories in CREAM could affect the accuracy of the results since the degree of control is a continuous process and it is not possible to put fixed contours between different levels of control or account for overlapping among them in an objective manner.

- The complexity of ATHEANA and CREAM makes these methods difficult to apply and use by persons who are not very well trained and familiar with their implementation. There is a need to provide implementation guidelines for both methods to facilitate using them whenever needed which is unavailable and adds an additional limitation to using these methods.

2.2.5 Human factors methods and techniques

This section provides an overview on human factors methods and techniques with focus on the methods that are relevant for the underlying thesis. It also introduces the link between human factors and performance shaping factors which are essential components in HF studies.

According to (Stanton et al. 2005) Human Factors methods and techniques can be classified into:

- Task analysis methods
- Data collection methods
- Charting methods
- Human error identification (HEI) methods
- Mental workload assessment methods
- Situation awareness measurement methods
- Interface analysis methods
- Design methods
- Performance time prediction/assessment methods
- Team performance analysis methods
- Root cause analysis methods

This wide diversity of human factors methods and techniques makes it impossible to list and analyse all these methods and techniques within the framework of this thesis. Alternatively, the methods which are relevant to this thesis are considered. These methods fulfil the following criteria:

- Well established and widely used methods according to literature reviews;
- Relevant to the applications of process industry;
- Can be used within the context of risk analysis and HRA, e.g., task analysis method which is used in most HRA methods.

Based on a screening of most common HF methods, the following set of methods is considered to fulfil the aforementioned criteria:

- Task Analysis methods (Section 2.2.5.1), e.g., initial task analysis, hierarchical task analysis, cognitive task analysis, etc.
- Root-Cause Analyses (Section 2.2.5.2), e.g., event trees and fault trees

It should be mentioned here that these methods are not the focus of this thesis and represent only "a means to an end", i.e., they are used as supporting tools for developing a methodology and improving the way of performing tasks and activities. Based on that, they are presented here as introductory work for the HF methodology (Chapter 3), i.e., characteristics of these methods, how they are used, aims of using them, etc.

2.2.5.1 Task Analysis (TA)

Task analysis is a way of structuring procedures, actions and contextual information regarding human behaviour in a certain working environment. Kirwan (1992) defines TA to be the study of what a user is required to do in terms of actions and/or cognitive processes to achieve a certain task. Task analysis was first developed in the fifties of the last century with the aim of formally describing human behaviour by a series of simple and elementary components (Skinner 1957). It was originally applied to language learning and then was extended to the wider context of operations and working processes (Payne/Green 1986).

TA aims at providing a better understanding of what is exactly involved in carrying out the activity so that a better fit between the person and the workplace (working environment) may be achieved. Task analysis is used in many areas of application, e.g., design of training programs and plans, design of interactive systems, design and test of man-machine-interfaces, etc. (Diaper 1989; Johnson 1991).

TA does not involve only collecting data about the operational procedures for performing a particular task, but in many cases also the collection of information about some properties of the tasks such as the job conditions, the required skills and knowledge, safety and environmental factors, references, equipments, job performance measures, etc.

Methods for collecting data for TA

Various methods or techniques could be used to collect data when performing a task analysis. The selection of the method depends on the nature or characteristics of the task under consideration. Based on field work in the area of application of this thesis, i.e., process industry, the following major types of tasks have been identified:

- Cognitive tasks, e.g., office job, control room job, etc.
- Accessible or non accessible tasks, e.g., the task is highly dangerous, the field access is forbidden to the observer, etc.

- Manual or automatic tasks, e.g., a manual maintenance action, automatic distillation process, etc.

Methods for collecting data – which are of particular relevance to chemical process industry – for TA include interviews, observations, analysing existing documents, etc. (Kontogiannis 1997). It is typical that a single method would not give sufficient results, thus a combination of methods is usually applied. Some of these data collection methods have been used to extract necessary data for the methodology (Chapter 3) and functional requirements (Chapter 4).

Approaches of TA

According to the application or case study, for which a task analysis needs to be performed, a certain approach (or approaches) of TA can be used. Among the most well known approaches are (cf. Kirwan 1998, pp. 299 et seqq.):

- Initial Task analysis (ITA): involves a basic level of task analysis to provide at least a minimum understanding level of the task (Kirwan 1994).

- Hierarchical task analysis (HTA): involves exploring tasks through a hierarchy of *goals* indicating what a person is expected to do and *plans* indicating the conditions when subordinate goals should be carried out (Shepherd 1998; Shepherd 1989).

- Cognitive task analysis (CTA): involves analysing the interaction of mental procedures, factual knowledge and task objectives in the process of job performance (Cacciabue 2004; Schraagen et al. 2000) .

- Goals, Operations, Methods and Selection Analysis (GOMS): involves identifying and analysing the rules for selecting methods for organising operators to achieve goals (Card et al. 1983).

- Task Analysis for Knowledge Description (TAKD): involves identifying, analysing and utilising rules for knowledge elicitation against task descriptions (Diaper 1989).

Further approaches have been analysed by (Kirwan 1998) and (Kirwan 1992). Task Analysis is further utilised in Chapter 3 to develop the HF methodology and in Chapter 4 in the process of extracting end users functional requirements.

2.2.5.2 Root-Cause Analysis

Root cause analysis (RCA) is used in predictive and retrospective analysis to study consequences of a risky event (forward analysis, e.g., risk analysis) or to study causes of an accidents (backward analysis, e.g., accident investigation) respectively. The aim of such an analysis from the point of view of a predictive analysis (risk analysis) is:

- To construct an overall incident scenario based on a risky event;
- Link events and consequences in a causal and logical form;
- Identify inappropriate actions which might lead to incidents.

A common approach of RCA which is widely adopted in the process industry for risk analysis is event tree (ET) which was introduced in Section 2.1.6.2. Despite their shortcomings which were introduced in Section 2.1.6.2, ETs are major components of risk analysis documents in chemical process industries and contain major sources of information on dangerous events and their inter-relationships. For this reason, the focus in this thesis is on utilising existing ETs to extract the necessary information for developing the methodology and functional requirements in Chapter 3 and four.

2.2.5.3 Performance shaping factors (PSFs)

Performance shaping factors (PSFs) or performance influencing factors (PIFs) refer to the set of factors that influences the performance and behaviour of the actors (employees, operators, technicians, etc.) who work in a certain environment or on a particular job (task).

PSFs are important elements of any comprehensive HF analysis or HF based methodology as they can be utilised to define hypothetical accidental or dangerous sequences due to human inappropriate behaviour. Examples of the most common PSFs include:

- Training methods, e.g., existing training is inadequate to cope with the underlying task or procedure.
- Rules and regulations, e.g., rules and regulations are complex and sometimes contrasting with each other.
- Communication means, e.g., inadequate or non-reliable communication means between operators.

- Time pressure, stress, level of supervision, comfort of working context, etc.

PSFs are further detailed using the terminology "performance conditions" as explained in Chapter 3.

2.2.6 Summary of Section 2.2

Besides providing definitions of terms which are widely used in HRA and HF and frequently used in this document, this section provided an overview on HF and HRA: the link between them, their methods and approaches as well as the limitations and shortcomings of current HRA methods.

The well known classification of HRA methods into 1st generation and 2nd generation methods was adopted in this section. A deeper look into 1st generation methods represented by THERP resulted in identifying the major limitation of 1st generation methods by being focused on the concept of human error in performing a task, i.e., task characteristics are the most influential elements in the estimation of human failure whereas the environment in which the task is performed (context) was almost ignored or considered as a minor corrective factor. This limitation of 1st generation methods was taken into consideration in 2nd generation methods which paid more attention to the *context* issue. However 2nd generation methods, which were represented by CREAM and ATHEANA, still suffer from subjectivity due to lack of information needed to apply the methods and their dependency on experts' judgments and qualitative estimations which might be critical in high-risk environments such as the process industry. A second major limitation of 2nd generation methods is their complexity and the lack of implementation guidelines that enable using them by safety and risk analysts on field. The by-product of these two limitations is the inability to automate or formalise these methods which deprived them of having the required IT-support. A third limitation is the nature of the methods which is focused on retrospective analysis and the absence of applications in which these methods have been used for predictive analysis, i.e., risk analysis. These limitations are of major focus in the HF methodology for RA which is developed in Chapter 3.

2.3 Virtual Reality (VR)

This section provides an overview of VR as the enabling technology within the framework of this thesis and as the third and last component of the literature review in this chapter. It represents the result of a comprehensive research on state-of-the-art on

using VR: definitions, introduction and features of VR, areas of applications, statistics on use of VR, trends in using VR, etc. It also aims at highlighting shortcomings and limitations of current VR systems (related works) from the viewpoint of this thesis, i.e., whether these systems are used for safety applications, whether they incorporate human factors, whether they target end users from the chemical process industry, etc.

The following points should be mentioned here regarding the scope, content and goals of this review:

- In consistency with the goal of this thesis in which VR is perceived as an enabler, the review focuses on VR systems and applications from a usability point of view, i.e., state-of-the-art on VR applications and products (projects), relevance of these application and products to safety and risk analysis, limitations on using and accepting VR by end users and end user requirements.

- Based on that, this review does not aim at introducing the state-of-the-art on VR technology itself, i.e., visualisation techniques and methods, technical features of the VR products, VR hardware and accessories, etc.

2.3.1 Definitions

Among the many definitions of *Virtual Reality (VR)* (Bohmann 1999; Blümel et al. 2003; Reinhart et al. 2002; Burdea/Coiffet 2003) the following definition provides a comprehensive description of what is meant by VR (Burdea/Coiffet 2003, pp. 3):

"A high-end user-computer interface that involves real-time simulation and interaction through multiple sensorial channels." (vision, sound, touch, smell, taste)

Virtual Environment (VE) is a computer created environment for a 3D visualisation with human-machine interaction. In most cases, a virtual environment is used to imply the same meaning as virtual reality.

I/O devices (VR accessories) are hardware devices that are used to interact with a VR scene to provide a user input or generate a representation of the scene as an output.

Desktop VR is the representation of a VR scene on a conventional PC monitor and performing the manipulation and interaction using mouse and keyboard.

2.3.2 Introduction to Virtual Reality

Virtual Reality (VR) is a breakthrough technology that allows stepping through the computer screen into a 3D simulated world (cf. Pimentel/Teixeira (1995), pp. xvii). Virtual Reality is characterised by its capability of providing Immersivity and Interactivity in one environment (Salem et al. 2006). The immersive characteristic of Virtual Reality can be achieved using the so called "VR-Accessories" which include among others, Head Mounted Displays, Data Gloves, Shutter Glasses, etc. The interactive characteristic of Virtual Reality enhances the engagement of the user in the virtual environment by acting and reacting, and thus enhances integrating the user in the virtual world. The interactivity in the virtual environment can be achieved with the conventional input/output devices including monitor, mouse and keyboard and does not require any special hardware or VR-Accessories. In applications where VR is used to visualise and provide a dynamic behaviour of the involved complements, e.g., interactive maintenance procedure, 3D assembly manuals, operation instructions, etc., a simulation model can be used to represent this behaviour in the virtual environment which is considered to be a further important feature of Virtual Reality (Winkler et al. 2005).

It is becoming clear that VR is a technology that is continually rising and flourishing which is reflected on the interest of the economy in using this technology for training, 3D interactive product lists, simulation of maintenance tasks, entertainment, etc. In some industrial sectors, VR has been integrated in the workflow as a mean of design review, virtual prototyping, functionality test, etc. to save construction and development times and costs. The automotive sector is one of the leading sectors in using VR and integrating it in daily workflows. Several survey researches on applications of VR were conducted or examined within the scope of this work and are introduced in the next subsections.

2.3.2.1 Immersive and Non-Immersive Virtual Reality

Immersive Virtual Reality refers to a high degree of user involvement in the virtual environment. Using a Head Mounted Display (HMD) together with other input devices like data gloves or joysticks supports this immersion by enabling the user to navigate through the 3D environment and to interact with the scene's objects as shown in Fig. **2.4**.

Source: Fraunhofer IFF (Blümel et al. 2005)

Fig. 2.4: An immersive VR environment

The wide spectrum of advantages combined with immersive Virtual Reality, like providing a stereoscopic view of the scene with the possibility of walking around and flying in the scene, were not enough for many end users to outweigh the high costs of implementing such an immersive VR environment. For this reason there was a need for an affordable Virtual Reality solution, which was facilitated by the use of non-immersive Virtual Reality.

Non-immersive Virtual Reality includes a mouse- and keyboard-controlled navigation through a 3D environment on a PC monitor. A stereo view of the contents can be achieved using a stereo projection system together with stereo glasses. Due to its lower complexity and costs, non-immersive Virtual Reality was selected by many firms as the appropriate Virtual Reality form, particularly for providing the contents at each desktop (desktop VR).

2.3.2.2 Layout of a VR system

In its basic and synthetic structure, a VR system is composed of the following components as shown in Fig. **2.5**:

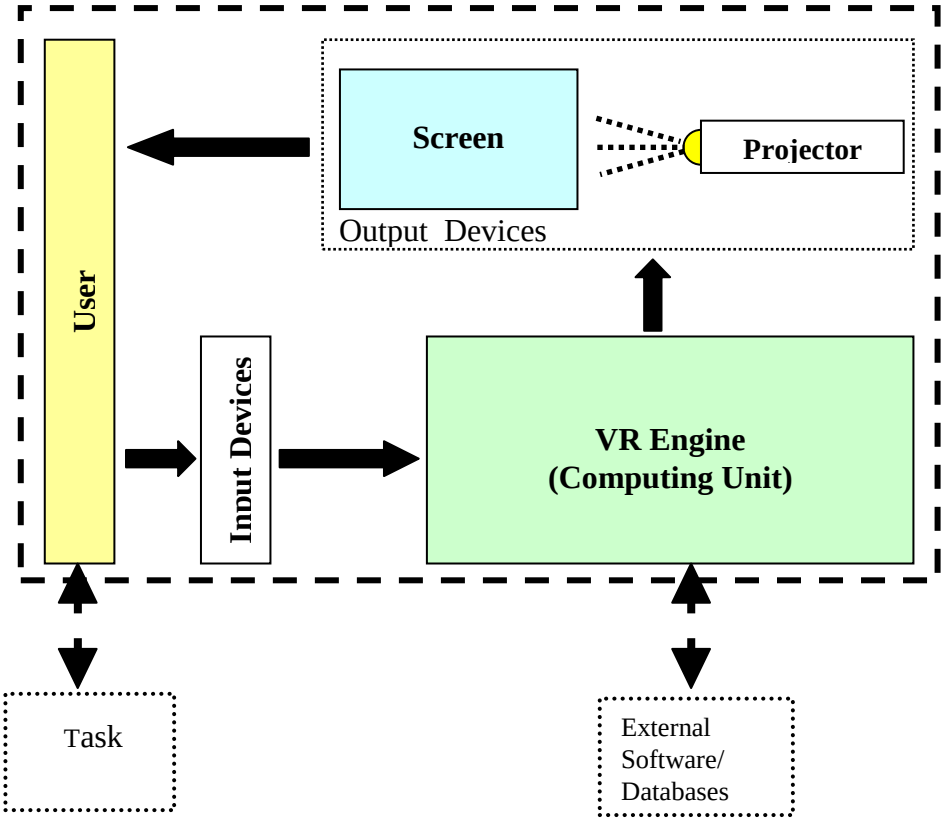


Fig. 2.5: An immersive VR environment

- Input devices: also called control devices and represent the system components that the user needs to interact with the VR scene and to enhance immersivity. Examples of input devices include joysticks, 3D mouse, data-gloves, trackball, etc.

- VR engine (computing unit): represents the heart of a VR system which can be a single PC or a complete multi central processing unit system (CPU) with single or multi graphics processing unit (GPU) and local/shared or distributed memory. This unit (device) controls the whole VR system by:

  - Interfacing with I/O devices

  - Performing graphical calculations and scene rendering

  - Managing and synchronising the devices involved in producing the VR scene, e.g., PC-components, tracking, the optional units, etc.

- Output devices: represent the devices where the virtual environment is presented or displayed. There are various implementations for presenting the output, ranging from a simple PC monitor to a single/multi-wall, curved screens, front/back projected, active and passive, each of them offering greater or slighter immersion. Based on the type of projection system used, the output can be in monoscopic or stereoscopic

form. In simple desktop VR applications, no separate projection device is used since the output is directly presented on the PC monitor.

- Optional units: represent interfaces and devices which might be incorporated in a VR system based on the nature of the application. Since these optional units are used as input or output facilitators, they were not presented separately in Fig. **2.5** and assumed to be an integral part of the input and/or output devices. These optional units are being further developed to involve the remaining human senses apart from the sense of vision which is an essential part of the VR system and belong to the core of the VR system, i.e., the VR engine in Fig. **2.5**.

Examples of optional units include:

- Audio interface for providing audio facilities in the VR scene which might enhance immersion (hear sense)
- Haptic interface for providing force feedback (touch sense)
- Gustation interface (taste sense)
- Olfaction interface (smell sense)

A considerable research has been dedicated to audio and haptic interfaces which resulted in reasonable developments in terms of hardware devices and commercial products in these areas. The gustation and olfaction interfaces are still in early research and development phases (Salem/Kissner 2007) with few prototypes and implementations (Yanagida et al. 2004; Yu et al. 2003; Iwata 2003). The historical evolution of VR towards ultimate interfaces which incorporate all human senses is presented in Fig. **2.6**.

2.3.2.3 Reasons for selecting VR as enabler to support RA

It has been mentioned in the introduction (Chapter 1) that VR is conceived here as an enabler which facilitates performing activities in a close-to-real manner, i.e., VR is conceived as a medium to extend human potentials for producing the desired safety improvements. In most cases, performing these activities in reality might be technically impossible, dangerous to humans or equipment or connected with high costs which cannot be justified. However, since there are other technologies and media which can be seen as enablers, e.g., multimedia, CAD representations, videos, etc. the major reasons

for choosing VR in this thesis are its capability to support (Salem 2003; Blümel et al. 2005):

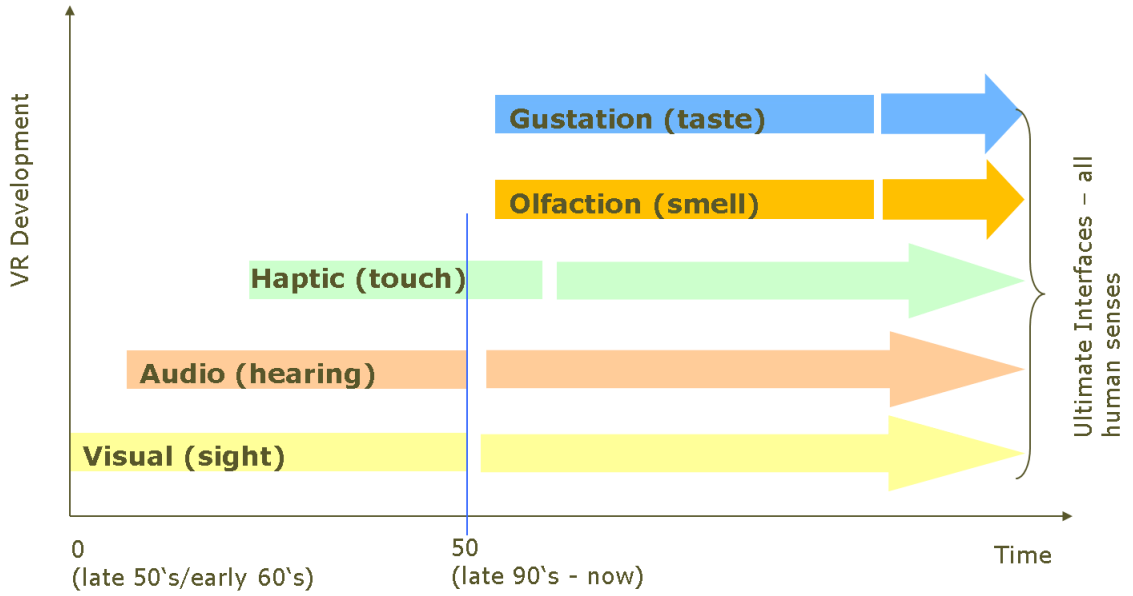


Fig. 2.6: Historical evolution of VR

- Providing High quality 3D graphics and not only simple images which are used in multimedia and video applications;
- Enabling a high level of interactivity and involvement which can be achieved with or without using VR accessories;
- 3D Visual interactive adaptation of the content to user needs or requirements;
- Performing activities in a "close to real" environment with a high recognition level of the components of the virtual environment, e.g., objects, equipments, surroundings, etc. compared to the physical one;
- A flexible provision of contents, e.g., for design, safety analysis, training, etc. which can be accessed independent of time, location and availability of an internet connection and specific resources or equipment.

VR potential in supporting risk analysis is illustrated in Chapter 4 upon defining the VR functional requirements and specifications.

2.3.2.4 Areas of application of Virtual Reality

VR is being used in different areas of application with varying levels of implementation depending on the degree of maturity of VR applications in each particular area.

According to recent studies and surveys on VR (Klocke et al. 2003; RTO-NATO 2005; Burdea/Coiffet 2003; Grau/Broszio 1999; Woods et al. 1987; Salem 2004) the most known areas of application include:

- Production and manufacturing: product design and construction, facility planning, maintenance (assembly/disassembly of products), design reviews, functionality tests, virtual prototyping, product marketing, etc.
- Education and training: training on virtual products and processes, learning complex procedures, group learning, training on products before their physical existence, etc.
- Medicine: virtual operations (new operation techniques), 3D visualisation of tumours and cancers, virtual laboratories, etc.
- Entertainment: interactive 3D games (adventure and strategy games), 3D amusement parks (Disney Quest and Disney Virtual Jungle Cruise), 3D cinema applications, etc.
- Architecture: city visualisation, urban planning, 3D interior design of buildings and facilities, etc
- Ergonomics: virtual human models, accessibility of objects, maintainability of products and objects, etc.
- Heritage: virtual museums, virtual story-telling, 3D exploration for art historians, etc.
- Military: 3D simulators (aircrafts, tanks, battle-field, ship, etc.), visualisation of enemy weapon capabilities, crew training, etc.

The following two facts can be derived from the aforementioned list of VR applications:

1. It is noticeable that VR applications for safety and risk analysis do not belong to the current application areas of VR. The rarity and inadequacy of available VR systems and applications to fulfil the requirements and needs in these areas is the reason behind that. It is also the absence of distinct end user requirements, methodologies and needs which stands behind this lack. This is further illustrated in the remaining part of this section based on results of survey and studies.

2. It is also noticeable that from a HF point of view, the VR systems and applications have been (and are being) used for the purpose of providing ergonomic results and validations, i.e., testing the reachability of product or machine parts, design verification, verifying the maintainability of a product, designing workplaces to be ergonomic and human friendly, etc. However, since ergonomic analysis and studies are elements of HF science, current VR applications lack a comprehensive consideration of HF methods and techniques, e.g., predictive analyses, recovery from a human error, identification of human caused hazards, interdisciplinary collaboration of plant teams (field operators, control room operators, fire brigade, emergency response team, etc.), working under stressful situations, etc.

2.3.3 Results of surveys on VR

As mentioned in the previous section, the rarity or inadequacy of available VR solutions which deal with safety and risk analysis as well as the absence of an integrated consideration of HF aspects have been investigated within the framework of this thesis. This investigation is based on survey results on VR systems in terms of features, areas of application, their use within the production life cycle (Fig. **2.1**), incorporation of HF aspects, etc.

For the purpose of integrity and completion, two types of surveys are considered here:

1. Surveys conducted in the past by commercial or research institutions (the term "external surveys" is used for this type).

2. Surveys that have been conducted as part of this thesis within the framework of a multinational research project on using technology to improve safety (the term "internal surveys" is used for this type).

The analysis provided under point 1 (external surveys) focuses on the industrial trends in using VR, areas of application and limitations behind a wider use of VR in the industry as shown in Section 2.3.3.1. The analysis provided under point 2 focuses on survey results that are directly related to the elements of the underlying thesis topic as shown in Section 2.3.3.2

2.3.3.1 External surveys

The development of VR applications, which had its revolutionary period in the last decade in terms of visualisation techniques and methods, interfacing to external systems (e.g., CAD), support to human machine interface, using VR devices (projection, tracking, haptic, etc.) and wider integration in workflows (e.g., in design review, virtual prototyping, functional tests, training, etc.). This development was accompanied by studies and surveys on the use of VR systems, e.g., industrial applications, acceptance by users, obstacles for using VR solutions, socio-economical impacts, etc.

Most of these surveys and studies were focusing on a particular industrial sector due to the nature of the projects for which these studies were performed. In this section an analysis of the results of three comprehensive surveys and studies is presented (Klocke et al. 2003; European Commission 1998; Karaseitanidis et al. 2006). The analysis is based on a classification of the results into one of the following categories:

1. Scope and technical complexity of the VR installations
2. Industrial use of VR and areas of application
3. Benefits of use
4. Limitations on use
5. End user requirements and needs

2.3.3.1.1 Scope and technical complexity of the VR installations

- The trend in using VR systems goes for applying immersive VR solutions with stereoscopic presentations;
- The acceptance of industry for putting higher investments in VR systems is increasing (e.g., investment in HW and SW in values of around 1 Million Euro);
- The industrial trend regarding the technical implementation of a VR system is commissioning to external service providers due to complexity of the installation and maintenance as well as the lack of know-how on operating the VR system. This follows the current outsourcing trends which can be confirmed by comparing recent figures on German outsourcing market as an example. According to (Experton 2009), the German outsourcing market is expected to reach a total turnover of 18.2 Billion Euros which corresponds to a growth rate of 8.2% compared to 2007. Outsourcing of

infrastructure components dominates the outsourcing trends with a total market share of 70% followed by applications (22%) and business processes (8%).

2.3.3.1.2 Industrial use of VR and areas of application

- Chemical and petrochemical applications (process industry) represent a field where VR still have to make a strong penetration due to the limited VR applications which have been considered so far in these areas;

- The current use of VR is highly focused on design, construction, product development, manufacturing and assembly. This can be justified by the nature of the industries in which VR is currently widely used, i.e., automotive and aerospace as previously described;

- Within the focus areas mentioned under the previous point, using VR to support HF approaches was not perceived as a priority which was confirmed in the ranking of applications of VR within these focus areas. Using VR to support "ergonomic studies" – which is an element of HF as previously mentioned under 2.3.3 – occupied the sixth place among 12 prioritised uses of VR;

- Within the framework of the EC-funded project "VIEW of the future" a rating of VR applications by VR experts, end users and HF experts resulted in design review and visualisation as the key VR applications compared to entertainment, advertisement, education and training;

- Another finding was the limited use of VR to improve safety (place number seven out of eight examined uses of VR) which was justified by the low consideration of safety as a VR application due to its dependency on many factors which requires dedicating specialised research work in this field. The limited applications here mainly used in the automotive industry for crash tests, finite element analysis, etc.;

- Among the most known applications of VR in the chemical process industry are: VR for scientific computations, VR for molecular modelling, VR for subsurface applications (visualisation);

- Using VR for safety training represents an area of application in which the acceptance is in the process of being won.

2.3.3.1.3 Benefits of use

- The benefits of using VR were significant in terms of productivity and monetary profits, i.e., reduction of costs and time as well as improving quality (in the part in which VR being used, e.g., design, construction, production, etc.);
- "Increasing productivity" and "enhancing speed to market" were ranked at high positions in all areas of application which confirms the industrial expectation from using VR.

2.3.3.1.4 Limitations on use

- The current integration of VR solutions in process workflow (process and engineering data management systems, PDM/EDM) is weak. Having recognised the potentials of VR, many industries intend to invest in integrating VR in daily workflows;
- A major reason which prevents a wider use of VR in industry is the lack of employees' acceptances. The reasons for this lack of acceptance were found out to be:
    - User-friendliness of the VR system
    - Lack of knowledge on using VR
    - Inadequacy of used VR hardware and devices (low resolution, uncomfortable VR accessories, etc.)
- The reason behind the low rate of VR applications and use in the process industry belongs to the problems encountered by this industry which are less directly amenable to a VR solution than in other industries.

2.3.3.1.5 End user requirements and needs

- A support to the well established CAD systems (e.g., CATIA V5 and ProEngineer) is a pre-requisite for using the VR solution in industrial applications. This finding is not unusual based on the fact that VR has been mostly used in product development and construction where conversion of CAD data represents a pre-requisite. The majority of commercial VR solutions provide this support via direct import or by installing an additional plug-in;

- A ranking of the end user requirements regarding VR software resulted in the need of having flexible conversion pipelines to and from the VR software, e.g., export the VR scene as a video, import objects' data and parameters, extract images for further use in a presentation or on a website, providing necessary data for a web service (spare parts catalogue, eLearning, etc.), etc. The availability of flexible conversion interfaces would also contribute to a better integration of VR solutions in the IT infrastructure;

- The biggest deficits of current VR systems were found to be high costs, insufficient software features and functionalities, lack of standardisations in VR and lack of integration in PDM or EDM systems;

- The future trend is not only to use VR as a tool to support product and process development but also as a communication platform and discussion medium between the employees involved in the construction, design, production and maintenance of the product.

Apart from the results and figures provided by these surveys on using VR and the identified research and application gaps, there is a need to extract a synthesis out of these results from the point of view of the underlying thesis. This synthesis aims at providing guidelines for the definition of the VR functional requirement and specifications which is provided in Chapter 4:

- The most known and widely spread areas of using VR are automotive and aerospace industries.

- There are no comprehensive evaluations on using VR in the process industries since it was not a good candidate for first VR applications as automotive and aerospace industries.

- Using VR to improve safety is an area which has not been evaluated due to the absence of mature VR solutions and applications in this area and consequently very limited results are available in this area.

- Integrating HF components in VR environments does not exist in a systematic and comprehensive way. Only partial consideration of HF aspects (e.g., ergonomic studies, effect of environmental conditions, different lightening conditions, etc.) in such environments was considered to match the particular area of applying the investigated VR system.

- The end users' acceptance of using VR represents a major obstacle for a wider use of VR in industry. This acceptance should be raised by enhancing the usability of VR environments which should take the criteria defined by Rautenstrauch (1997) for enhancing the end user's acceptance as follows:

    - Ergonomic design of the application software with flexible and adequate interaction methods and tools;

    - Problem-oriented provision of software functions based on the task (problem) to be solved by the end user and not on the technical features which can be provided by the software;

    - Moderate strategy for introducing the software application in the company, particularly if the new software application will substitute an older one, on which the end users used to work since a considerable time.

2.3.3.2 Internal surveys

The analysis under internal surveys focuses on survey results that are directly related to the elements of the underlying thesis topic as was described in Section 2.1 and 2.2. This analysis covers:

a. Results related to using the investigated VR systems and applications for safety or risk analysis (refer also to Section 2.1);

b. Results related to VR systems and applications dedicated to support the operational phase of the production life cycle (refer also to Section 2.1);

c. Results related to incorporating HF and HR components in the investigated VR systems and applications (refer also to Section 2.2);

d. Combination of any of the previous three aspects.

2.3.3.2.1 First survey

This first survey covered eight industrial companies that are collaborating in the multinational research project mentioned in Section 2.3.3. A description of the profile of these companies and the data collection method for the survey are provided below:

- Industrial sector to which these companies belong:

- Seven companies belong to the process industry (chemical and petrochemical);
- One company belongs to the nuclear and energy domain.

- Size of the company:
  - 6 of the companies are classified as large scale industries with more than 250 employees;
  - Two of the companies are classified as SMEs (according to EC definition of SMEs (European Commission 2008)).

- Data collection: the data were collected during 2-3 days on-site workshops with experts from these industries (interviews). The interviewed experts have the following competencies or belong to the following departments in their enterprises:
  - Training managers and/or trainers;
  - Safety specialists/analyst with a global view of safety actions in the company and if possible with operational background;
  - HSE managers (project managers/process managers);
  - IT department (IT manager and/or system engineer);
  - Engineering & Design department;
  - Development and planning department.

On average, 2-4 experts with the aforementioned profiles have been involved during the interviews from each company. The following results regarding the use and applications of VR were extracted during the workshops and based on interviews' results:

1. Only one company has a complete VR installation which is being utilised and maintained;
2. The VR applications running in this VR environment do not cover safety or risk analysis. The reason for that is the lack of VR solutions which provide support in these areas;
3. Only three of the interviewed industries have experience with VR based on their participation in research projects or by using VR tools for design and training;

4. Training is still the most popular field of using VR as perceived during the interviews;

5. Even large scale industries were not sure about the potential of VR in supporting daily activities which was the reason behind the uncertainty in investing in VR;

6. The interviewed SMEs mentioned the following obstacles which prevent investing in VR:

    - The unaffordable costs of VR compared to the size and turnover of the company
    - The lack of employees who have the knowledge and competencies in VR
    - The need for customising the VR applications to their needs

7. Only one of the interviewed industries has experience in human factors engineering and using VR to support design and operation from the ergonomics point of view;

8. All large scale industries considered the combination of VR and HF to improve safety and risk analysis as an innovative application in their enterprises and the willingness to invest in a technological solution which could improve the process of performing safety and risk analysis;

9. All the interviewed industries expressed the need of having a flexible VR solution which can run in an immersive environment or on PC (desktop VR).

2.3.3.2.2 Second survey

The second survey was dedicated to software products and solutions which make use of visualisation techniques and animations as core features. A total of 21 products were investigated based on the following criteria:

- Nature of product: commercial or non commercial (e.g., a closed project or under development);
- Target group of the product: military, entertainment industry, aviation industry, process industry, automotive industry, nuclear industry, etc.;
- Phases of the production life cycle for which the product is targeted: exploration, design, construction, operation, etc. (see Fig. **2.1**);

- Availability of advanced VR features in the product: collision detection, reliable CAD support, SDKs/APIs, development guides and documentation, authoring interfaces, etc.;

- Support to HF methods and knowledge;

- Area of application from safety perspective: training, risk analysis, accident investigation, safety management, other (non-safety relevant, e.g., design review, marketing, games, etc.).

The detailed survey results are provided in Annex E. Below is an analysis of the results based on the aforementioned criteria:

Nature of the products:

57% of the investigated products represent non commercial products, i.e., industrial or research projects under development. This confirms the inadequacy of available commercial products to provide feasible solutions to the critical issues in safety and risk analysis as explained in Section 2.3.3.2.1. One of the reasons for this inadequacy is the dependency of "safety" and "risks" on many external and overlapping factors which requires dedicating specialised research work in this field.

Target industries of the products:

The wide range of target groups covered by this survey adds a comprehensive feature to it by not focusing only on the sectors which are popular in using VR solutions as described in the Section 2.3.2.4. 33% of the investigated products target the process industry which is represented here by chemical and petrochemical industries followed by manufacturing and military industries. This result should be further examined based on the relevance of the product applications to safety and risk analysis as well as the inclusion of HF and VR components as illustrated in the next diagrams.

Inclusion of VR and HF:

Most of the investigated products are classified to be pure VR products whereas about 28% of the products provide a mix of VR features and support to HF aspects. In most cases this HF support takes the form of facilitating the performance of ergonomic studies or adding certain effects to the VR environment to address some performance shaping factors (PSFs, see also Section 2.2.5.3), e.g., weather conditions, work conditions, adequacy of training procedures, etc. None of these "HF+VR" products within the 28% category provides the HF support in the form of a systematic HF

methodology which enables extracting the information and parameter for conducting an integrated HF study.

Application areas of the products:

VR training applications has been found to be the first and most popular area of using and applying VR in industrial and research applications. It is also a fact, that almost all VR systems can be (or are currently) used to provide training and learning which was confirmed by the survey result in this regard, i.e., around 71% of the products are dedicated to training applications. The remaining products (29%) are distributed as follows:

- Around 5% of the products are used to provide support for design, marketing, virtual prototyping, etc. which are considered to be less relevant to safety applications;
- 24% of the products are used in safety-related applications which include risk analysis and safety management. It was not possible to investigate the complexity and depth of these products in tackling safety and risk related issues due to unavailability of adequate information and evaluations of these products.

Phases of the production life cycle covered by the products:

Most of the investigated products aim at supporting the operational phase of the production life cycle (38.5%) followed by the maintenance phase (25.5%). This is due to the fact that these two phases represent the phases in which most of the production time is spent, i.e., improving processes inside these phases is expected to enhance productivity, reduce production costs and consequently increase profitability and raise market chances which represent the ultimate goal of industries. The design phase – which plays a stronger role in manufacturing, automotive and aviation industries – occupied the third place with 20%.

Combination of the analysed elements:

Fig. **2.7** combines the different elements of the underlying thesis on the investigated products using the survey results. These elements are:

- Covering the operational phase in the production life cycle (Op)
- Using VR
- Providing support to HF

- Providing support to risk analysis (RA)
- Applied to process industry (PI)

Increasing the degree of complexity by moving from the first element to the last one reduces the number of products that match the defined criteria. Consequently only one non-commercial product (project) was found to match all criteria listed above. Since the only available information about this product is the filled survey template, additional information was requested on this product. Up to the time of producing this thesis, no information was received. Even an internet search resulted in no information on this product. Despite this unavailability of necessary data and information for evaluation, this product was not removed from the list of investigated products for the purpose of scientific neutrality.

A list of the examined products is provided in Table E.1 (Annex E)

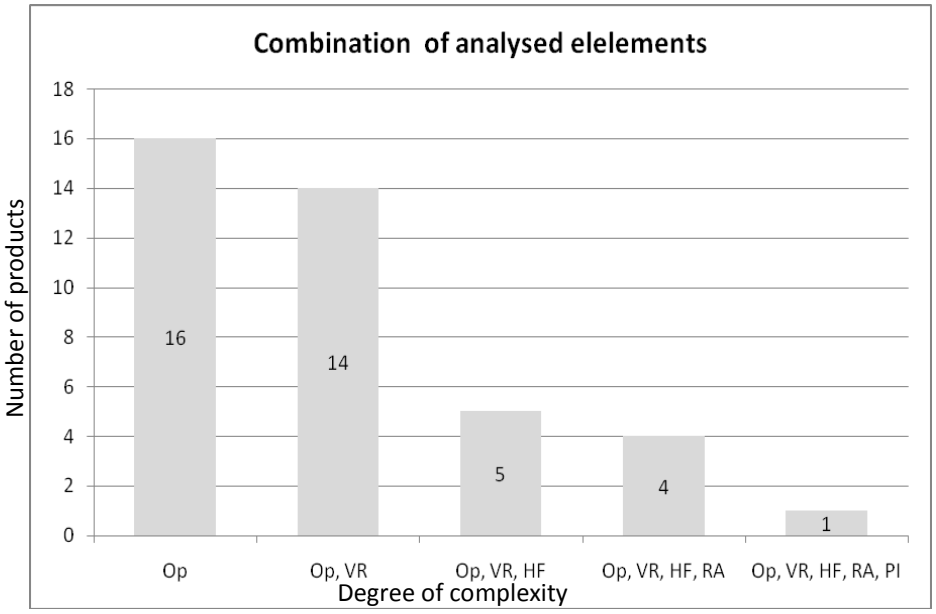


Fig. 2.7: Effect of combining analysed elements on number of matching products

The results of the surveys performed within the framework of this thesis (internal surveys) confirm to a large extent the findings of external surveys as described in Section 2.3.3.1. Below is a synthesis of these results:

- A systematic and methodological incorporation of HF aspects in a VR environment is still a research area with no clear mature commercial products.
- The operational phase of the production life cycle is the major supported phase by VR products due to the fact that most of the production is spent during the operational phase.

- Using VR for training and learning is still dominating the VR applications due to the many research projects in the area of VR training during the 1990s which lead to good advancements in this area. Using VR for safety and risk analysis is still under development due to the nature of these applications which is more complex and demanding than training applications.

2.3.4 Summary of Section 2.3

Besides providing definitions of terms which are widely used in the VR community and are necessary for this thesis, this section provided an overview about Virtual Reality: state-of-the-art on using and applying VR in industrial applications, peculiarities of providing contents in a VR environment as well as a review of previous and related works.

After the introductory part on VR, basic system architecture of a VR environment was introduced together with a description of its components and their interoperability. After that an analysis of surveys which were examined and conducted within the framework of this thesis was introduced with a particular focus on the relevance of the results to the three building blocks of this thesis (safety/risks, human factors and VR applications within the operational phase of the production life cycle).

It was clear from this review that using VR to improve safety (reduce risks) does not belong to the well known VR uses – unlike training and design reviews for example – which confirms the need for further research and exploration in this area. Furthermore, integrating HF components in VR environments does not exist in a systematic and comprehensive way. Only partial consideration of HF aspects (e.g., ergonomic studies, effect of environmental conditions, different lightening conditions, etc.) in such environments was considered to match the particular area of applying the investigated VR system.

2.4 Summary and conclusions

Chapter 2 provided an overview of works that are related to the underlying thesis and served as a review on state-of-the-art on the three major components of this work (as defined in Fig. **1.3**) which are: safety (risks), human factors and virtual reality from the practical (industrial) dimension of use.

Based on this review, the following conclusions with direct relation to the motivation and elements of the underlying thesis have been extracted:

- **Limitations of current methods and techniques for performing risk analysis**

Conventional QRA techniques and tools (e.g., HAZID, HAZOP, event trees, fault trees, etc.) are time consuming and highly dependent on expert's imaginations and personal judgments to reach their intended goal which represents a subjective and inflexible way of conducting risk analysis work. Furthermore, QRA provides a crude analysis of barrier performance, emphasising mostly technological and process aspects rather than other risk influencing factors such as human and organisational aspects.

- **Limitations of 1st and 2nd generation methods and techniques for performing human reliability analysis**

1st generation methods focused on the concept of human error in performing a task, i.e., task characteristics are the most influential elements in the estimation of human failure whereas the environment in which the task is performed (context) was almost ignored or considered as a minor corrective factor. 2nd generation methods paid more attention to the *context* issue but still suffer from subjectivity due to the lack of information needed to apply the methods and their dependency on experts' judgments and qualitative estimations which might be critical in high-risk environments such as the process industry. A second major limitation of these methods is their complexity and the lack of implementation guidelines that enable their usage by safety and risk analysts on field. A third limitation is the nature of the methods which is focused on retrospective analysis and the absence of applications in which these methods have been used for predictive analysis, i.e., risk analysis.

- **Lack of VR applications for safety and risk analysis**

The rarity and inadequacy of available VR systems and applications to fulfil the requirements and needs in these areas is the main reason behind this lack. A second reason is the absence of clear end user requirements, methodologies and needs on safety and risk analysis which can be moulded in a VR environment. A third reason is the complexity of translating the safety context into a task-format unlike the case of training or maintenance tasks where VR has been widely used. This is due to the nature of *safety* and its dependency on many factors, e.g., human, organisational, technological, etc. which are difficult to be modelled in a single task.

- **Incorporation of HF in VR environments**

Current VR solutions and applications lack a comprehensive, systematic and methodological consideration of HF methods and techniques, e.g., predictive analyses, recovery from a human error, identification of human caused hazards, interdisciplinary collaboration of plant teams (field operators, control room operators, fire brigade, emergency response team, etc.), working under stressful situations, etc. The focus in current VR solutions was a partial consideration of HF aspects (e.g., ergonomic studies, design validation and tests, examining effect of environmental conditions, impact of different lightening conditions, etc.) in such environments.

- **VR applications in the process industry**

Chemical and petrochemical applications (process industry) represent a field where VR still have to make a strong penetration due to the limited VR applications which have been considered so far in these areas. The reason behind this limited use is the nature of the working environments which is characterised by being complex, hazards and involves different working teams.

- **End users' acceptance of using VR**

The end users' acceptance of using VR represents a major obstacle for a wider use of VR in industry which is mainly caused by complexity of the VR systems, high costs of introducing a reliable VR solution, the availability of VR specialists for installation and maintenance at the end users' enterprises, the fear of losing workplaces, etc. This acceptance should be raised by enhancing the usability of VR environments through human-cantered design approaches, end-user and problem oriented provision of system functionalities and features, ergonomic design of the application with flexible interaction methods and a moderate strategy for introducing the VR applications in the company to minimise employees' resistance.

These conclusions re-emphasise the need for research on end-user oriented VR applications for improving safety under the consideration of human factors methods and human reliability analyses which is the core of the underlying thesis.

Since they represent scientific findings as well, these conclusions are further considered in the development of the HF methodology (Chapter 3), definition of functional requirements (Chapter 4) and the proposed VR environment design (Chapter 5) to support reaching the goal of this thesis as was introduced in Chapter 1.

3
A HF methodology for supporting risk analysis

This chapter introduces a HF methodology for supporting risk analysis which takes the human behaviour and performance into consideration, i.e., human errors. It assists safety and risk analysts in the qualitative analysis of cognitive reliability upon running and controlling processes on complex production systems, e.g., chemical processing plants, gas plants, oil refineries, etc.

3.1 Definitions

To avoid complication in the definition of the term "methodology" due to the many existing definitions, the following definition has been found to match the intended use of this term in the underlying thesis and is adopted here:

Methodology is "a body of methods, rules, and postulates employed by a discipline" (Merriam-Webster (2008)).

Method is "a way, technique, or process of or for doing something". (Merriam-Webster (2009))

To distinguish between the two terms within the context of this thesis, the term *method* represents a main process to do something whereas a *methodology* consists of different rules and guidelines to model human factors within the integrated method. The difference can be better understood, if we apply it to a mathematical problem. In this regard, the formula for solving the problem would be the method whereas the methodology would be a step in this formula.

Further definitions for the term *Methodology* are provided by (Ritzer 2007, pp. 2967-2970; Wiktionary 2008b; Johnson 2003, pp. 92). These definitions are widely close to the definition provided by Merriam-Webster.

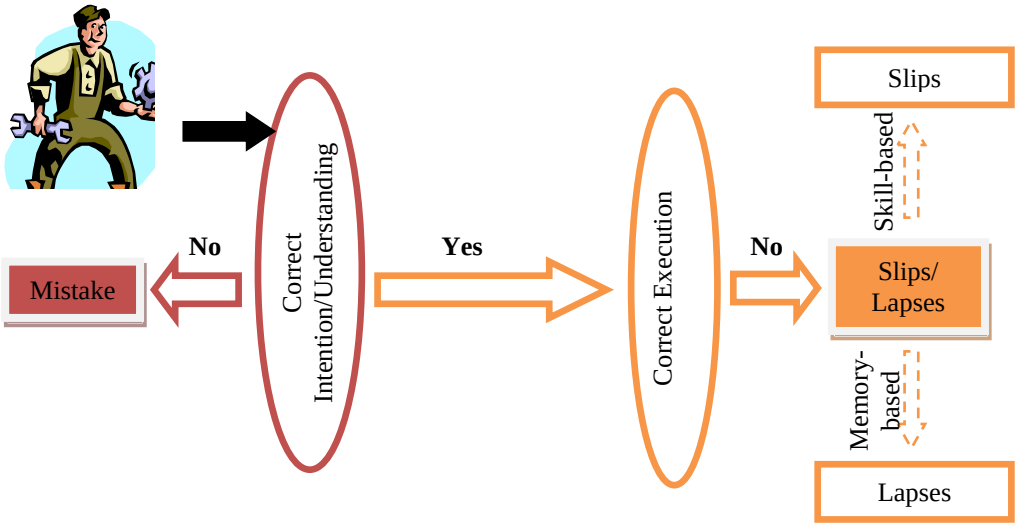
Human error, cognitive error: see *human error* in Section 2.2.1.

Human error is classified into slip, lapses and mistakes. Slips and lapses are failures that occur when the plan is adequate, but the execution is wrong, i.e., wrong execution of a proper intention (cf. Rasmussen et al. (1994), pp. 139).

Slips are "associated with attentional or perceptual failures and result in observable inappropriate actions" (Cacciabue (2004), pp. 19). According to (cf. Salvendy (1997), pp. 120 et seqq.), slip-type errors occur most frequently at the skill-based level.

Lapses are "connected to cognitive events and involve memory failures" (Cacciabue (2004), pp. 19), i.e., lapses are failures that can be directly attributed to the breakdown of memory such as forgetting or confusing material (cf. Salvendy (1997), pp. 120 et seq.).

Mistakes are errors made at high cognitive level (cf. Cacciabue (2004), pp. 19) and occur from a proper execution based on the wrong intention or incorrect understanding of the situation. Fig. **3.1** illustrates this classification of errors.



Based on Hollnagel (1998), pp. 26

Fig. 3.1: Human error classification into slips, lapses and mistakes

Error mode is "a possible way of failing to perform an action correctly given specific conditions" (Hollnagel (1998), pp. 14).

Taxonomy is "the practice and science of classification" (Wiktionary (2008b)), i.e., classification of things that are arranged frequently in a hierarchical structure.

Cognitive tasks are tasks characterised with their high cognitive nature such as control and supervisory tasks in complex industries (e.g., chemical process industry, nuclear industry, aviation industry, etc.).

Problem-solving is a higher-order cognitive process that requires modulating and controlling more routine or fundamental skills (Goldstein/Levin 1987). It forms part of thinking and is considered to be the most complex of all intellectual functions (Wikipedia (2008a)).

Performance mechanisms are aspects of the *problem-solving* behaviour that can be applied to the cognitive functions of identification, interpretation, decision-making and planning. Refer also to Section 3.3 and 3.4.3.

Performance conditions are descriptions of task demands in coping with complex events and include contextual factors such as, available time, availability of plans, simultaneous goals, feedback, working conditions, etc. Refer also to Section 3.3. and 3.4.4.

3.2 Preamble

Recent trends in Quantified Risk Analysis (QRA) and Human Reliability Analysis (HRA) have focused on cognitive tasks, such as situation assessment and decision-making, as we are witnessing a shift of operator jobs from manual control tasks to cognitive and supervisory control tasks. Cognitive errors often result in incorrect diagnosis and inadequate plans that may fail the safety functions needed to mitigate accident scenarios. In this sense, the role of cognitive science is becoming essential in providing frameworks of human performance to help safety analysts to examine cognitive error modes and underlying causes.

An enhanced method for improving predictive analysis of human reliability should include (Hollnagel 1993; Dougherty 1993; Meister 1995):

1. An explicit model of human performance for cognitive tasks:

It has been shown and explained in Chapter 2 that most of the existing HRA methods are classified into 1st or 2nd generation HRA methods. In the former methods - e.g., INTENT (Gertman et al. 1992), TRACER (Shorrock/Kirwan 2002) and THERP (Swain/Guttmann 1983) - explanations of human error are viewed as breakdowns in the natural course of information processing, i.e., employees' failure to follow an established procedure. These methods assume that reliable criteria of optimal performance exist against which deviations can be measured. For tasks, which are well-specified, reliable criteria may be derived from operating procedures; however, this is difficult for unfamiliar tasks. For man-machine interactions high in dynamics and uncertainty, it is not always easy to specify in advance reliable criteria of performance standards since this depends on the context of work. In this respect, 2nd generation HRA methods have attempted to specify operator control strategies that are dependent upon the context of work and task characteristics. These methods - e.g., CREAM (Hollnagel 1998), ATHEANA (Cooper et al. 1996) and IDA (Smidts et al. 1997) -

focused on models of adaptive human behaviour and examined ways in which operators can modify their plans to cope with the demands of the situation.

2. A comprehensible taxonomy of error modes and error causes that can be easily applied by safety analysts:

This requirement addresses the ability of HRA methods to discriminate and classify a comprehensive range of errors. While most methods may score high in terms of comprehensibility, the logic for deriving the proposed error modes and causes is not made clear which may reduce their usability in the hands of safety analysts who are less familiar with the theoretical foundations of human performance and human reliability.

3. A representation of the dynamic interaction between workplace factors and human performance:

This requirement which corresponds to the dynamic interplay between context of work and human cognition is difficult to achieve when the proposed method has been developed to have general application. Methods developed in the context of specific industrial domains appear to offer a more concrete basis for addressing the intricacies of the particular application. In the context of nuclear power industry- e.g., ATHEANA (Cooper et al. 1996) and AGAPE-ET (Kim et al. 2004) - have provided elaborate representations of the interaction between context of work and human performance. However these methods are either still under development or lack instructional guidelines for applying them which makes them unfeasible for safety and risk analysts who are not necessarily human factor experts.

4. A consideration of the error detection and recovery processes:

The large number of errors detected and recovered by operators in complex systems indicates that it is impossible to achieve total error prevention and that an alternative approach to enhancing human reliability could be through error recovery. Relatively fewer methods have addressed systematically this fourth requirement of modelling error detection and recovery (Kontogiannis 1997; Shorrock/Straeter 2006; Trucco & Leva, 2007).

The underlying methodology provides a practical framework for modelling human error and recovery processes in a representation format that is widely used by safety analysts. The theoretical foundation of this methodological framework stems from a model of “performance mechanisms” and “performance conditions” (Kontogiannis 1997). Cognitive error modes and error causes are cast in new forms drawing upon the keywords used in hazard and operability (HAZOP) studies to facilitate using them by

safety experts. A practical model of human error recovery is proposed and presented in a dynamic event tree (DET) that is suitable for representing the changing context of work and the influence on the detection and recovery of errors.

3.3 Error causation model

Before moving into the individual elements of the proposed methodology, Fig. **3.2** shows the error causation model that is applied in the underlying methodology. The model starts by analysing cognitive error causes, error modes and recovery failures that might lead to unsafe human interventions with potential critical safety consequences (boxes 1-5). This model, which takes a chain form, is influenced by performance mechanisms, performance conditions and system defences (boxes 11, 12 and 13). For this reason, these three elements are placed on a parallel level to the five basic components of the error causation model numbered 1-5 (a grey colour has been assigned to these three elements to distinguish them from the remaining elements of the error causation model).

The error causation model starts by analysing causes of an erroneous action (slips, lapses or mistakes). In the underlying methodology emphasis is placed on possible cognitive error causes, e.g., failure to revise assessment, overlooked constraints in searching information, inefficient tests, etc. (box 1). These cognitive error causes are examined in the context of the interaction between performance conditions (box 12) and performance mechanisms (box 11). Having identified the cognitive error causes, the methodology proceeds with an analysis of cognitive error modes, e.g., wrong diagnosis, delayed decision, priority error in planning, etc. (box 2) and recovery failures (box 3) that might lead to an unsafe intervention (box 4). Unsafe interventions are descriptions of error manifestations that could in turn be the result of slips and lapses (i.e., action failures as explained in Section 3.1) or mistakes (i.e., cognitive failures as explained in Section 3.1). The focus in the underlying methodology is on mistakes (cognitive failures), which is also illustrated in the feedback loop in Fig. **3.2**. System defences, e.g., safeguards and limiting functions (box 13), are examined not only as mechanisms for mitigating the error consequences (box 5), but also in their potential to assist operators in detecting errors. The methodology is moulded as a set of taxonomies of error modes and error causes that provide input to a dynamic tree representation of error modes and recovery failures.

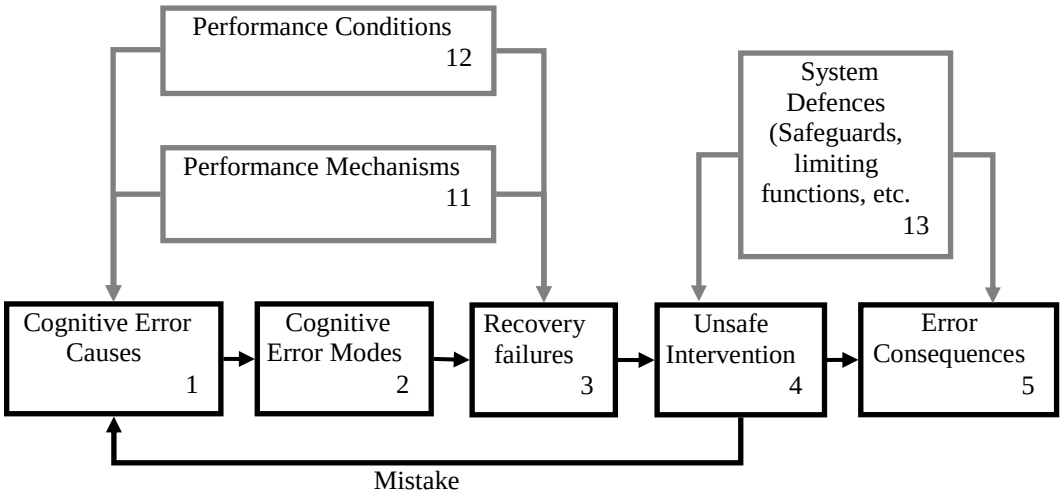


Fig. 3.2: The error causation model applied in the underlying methodology

The concept of performance mechanisms relies on a problem-solving view of the cognitive functions, i.e., identification, interpretation, decision-making and planning, which may fail in certain ways when demands exceed resources. The concept is proposed as a more direct assessment of task demands in coping with complex events and includes contextual factors such as, available time, availability of plans, simultaneous goals, feedback, working conditions and so forth. Possibilities for error recovery are explored by examining how performance conditions and performance mechanisms change in the course of a scenario. The main support in analysing recovery failures is provided in terms of a dynamic cognitive event tree presented in Section 3.5.

3.4 The methodology

It has been mentioned that the proposed methodology will assist safety and risk analysts in the qualitative analysis of cognitive reliability upon running and controlling processes on complex production systems. This is achieved by identifying cognitive error modes and causes behind unsafe interventions and modelling paths of error modes and recovery opportunities as the situation unfolds dynamically and performance conditions change in the course of events.

To reach these goals, the methodology is introduced based on its building elements, which are (refer also to Fig. **3.2**):

- A model of cognitive functions (Section 3.4.1);

- Error modes (external error modes: Section 3.4.2.1 and cognitive error modes: Section 3.4.2.2);
- Performance mechanisms (Section 3.4.3);
- Performance conditions (Section 3.4.4);
- Cognitive error causes (Section 3.4.5);
- Error detection and recovery (Section 3.4.6).

A graphical overview of the methodology and how to apply it to scenarios and case studies is presented in Section 3.5. In Chapter 6, the methodology is validated by applying it to a case study from the chemical process industry.

3.4.1 A model of cognitive functions

In human error analysis, we should be able to identify cognitive functions that have given rise to certain human actions as well as the influences exerted by the context of work. The Simple Model of Cognition (SMoC) (Hollnagel 1998), (Ritter et al. 2001), (Johnsen et al. 2008) has been adopted here to examine the cognitive functions that are brought to bear in carrying out operator tasks. Fig**. 3.3** introduces the model of cognitive functions that is used in the underlying methodology (cognition cycle). This model is used to identify cognitive errors in the four cognitive functions illustrated in Fig**. 3.3**, i.e., the functions of *identification*, *interpretation*, *decision-making* (*choice of goals)* and *planning* as follows:

- ***Identification (recognition):***

When a problem occurs, operators have to identify important changes of system parameters and signify their consequences in terms of system functions that may be threatened in the near future.

- ***Interpretation:***

Upon the recognition of a problem, operators have to interpret and organise the information into a meaningful whole. In this stage, the operator might acquire more specific information in order to understand the causes of the problem since the potential for misunderstanding the situation could be critical at this stage

- ***Decision-making (choice of goals):***

This stage encompasses the process of goal selection to compensate for the problem. It entails an evaluation of alternative problem constraints and/or solutions and whether a decision must be made.

- ***Task planning or scheduling***

This stage is required to formulate a sequence of actions based on a set of problem constraints and/or solutions identified in the decision-making stage.

The double-sided arrows in Fig**. 3.3** indicate that there is no pre-defined ordering of cognitive functions since task organisation and control depend on the particular context of work. This issue has been addressed by (Roth et al. 1994) who indicates that *decision-making* and *interpretation* are often carried out in parallel when coping with complex events. Some kind of preliminary *decision-making* or solutions can also take place in the *interpretation* stage and influence the assessment of situation. On the other hand, viable goals can also be proposed at an abstract level without having achieved a complete *interpretation* of problem causes.

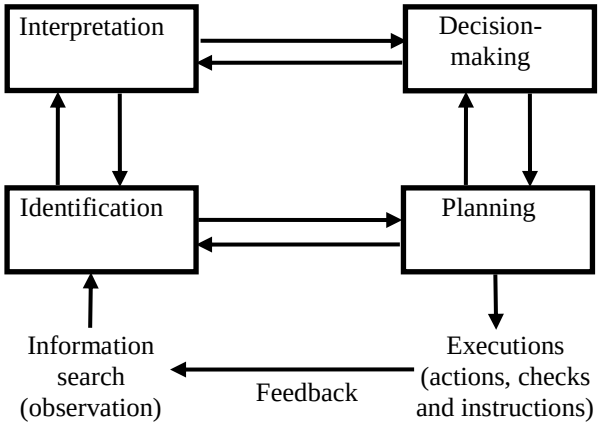


Fig. 3.3: A model of cognitive functions (boxes) underlying information search and execution

The first unboxed element in Fig**. 3.3** refers to the input, i.e., *information search* (observations), that influences the cognition cycle. The second unboxed element refers to the result of the cognition cycle which takes the form of *executions*, i.e., actions, checks, instructions, etc. The feedback loop indicates that the executed actions affect the identification of new problems. To illustrate this aspect in an example, let's assume that for an identified problem, one of the executed actions is "bypass valve X by using valve Y". This fact is taken into consideration in identifying new problems in the same working area, i.e., "valve X" is not seen as a cause of the problem here and new information search is needed to identify the problem.

3.4.2 Error modes

The underlying methodology distinguishes two types of error modes or human malfunctions:

1. External error modes that are observable by safety analysts (i.e., errors in information search and execution);

2. Internal or cognitive error modes (i.e., errors in identification, interpretation, decision-making and planning) that account for the more covert aspects of cognition.

3.4.2.1 External error modes

Several taxonomies of external error modes - that are in general agreement - have been developed (Reason 1990; Embrey et al. 1994). The underlying methodology proposes two taxonomies of error modes for the stages of information search and execution. These taxonomies provide categorisation and classification schemes of external errors to support safety and risk analysts in understanding and explaining how an error occurs. This error classification is used in the next steps of the methodology as explained in the upcoming sections of this chapter.

I) External error modes for the information search stage

Errors in information search could be due to poor "plans of data collection" and hence, could affect the cognitive stages of identification and interpretation. For this reason, information search errors must be considered in advance of cognitive error modes in the underlying methodology. Table **3.1** provides a taxonomy of information search errors based on the application of a HAZOP-style analysis on the available information, data and oral instructions. The table illustrates that information search errors could be due to missing an important piece of information (items 1 and 2), delayed detection of the information (item 3), disregarding a relevant piece of information (item 4), misreading of instruments (item 5), mistrusting the information (item 6) or misunderstanding the observed information (item 7).

The second part of Table **3.1** examines errors in fitting information into patterns to reach an understanding of the situation. In this sense, the collected data could be fewer or greater in number than those required to get at the correct pattern. A fewer number of collected data would mean that the data is insufficient to understand the situation (item 9). On the other hand, a greater number of collected data may imply that some of the information could be irrelevant or redundant (items 8 and 10).

Table 3.1: Taxonomy of external error modes for the information search stage

Number	Keywords	Information search errors
Individual pieces of information		
1	*None (Missing)*	An important piece of information that is not displayed on the control panel because of a faulty sensor or lack of sensor.
2	*Not done (Missed)*	Failure to detect or identify critical information or failure to retrieve data and values from manuals.
3	*Later than (Delayed)*	Cues or data are not identified in time (delayed detection) because of poor visibility, distractions and workload.
4	*Skipped (Discarded)*	Cues or data are identified but ignored because they are not seen as relevant at a certain point in time.
5	*More/less than (Misread)*	Errors in reading instruments, retrieving data from manuals, or receiving oral instructions.
6	*Mistrusted*	Failure to verify instructions or unreliable instruments.
7	*Misunderstood*	An event or cue is mistaken for something else.
Patterns of information collected		
8	*Other than (Irrelevant)*	Collected data are not pertinent to the situation. Cues are wrongly associated to the implications of the situation.
9	*Part of (Insufficient)*	Data are not sufficient to understand situation or make decisions. Failure to associate two or more cues when their combined effects should be noted.
10	*As well as (Redundant)*	Operators spend a lot of time gathering cues or data in excess of what is required to understand the problem.

II) External error modes for the execution stage

For the execution stage, Table **3.2** provides a taxonomy of external error modes for the execution stage (execution errors) cast as a set of keywords used in hazard and operability studies (HAZOP) which does not require a great deal of expertise by the safety analyst. The keywords are applied to several operator activities including manual actions, checks on instruments, retrieval of information from written procedures and communication of information. An analysis of execution errors assumes that there is nothing wrong with the plan or course of action developed by operators (i.e., the *planning* phase in Fig. **3.3**); in this sense, errors are made during the implementation of actions.

Table 3.2: Taxonomy of external error modes for the execution stage

Number	Keywords	Execution errors (actions, checks and instructions)
1	*Not done*	The activity is not performed or the operator is unable to do it.
2	*Part of*	Part of a complex activity has been omitted.
3	*More- less than*	The result of the activity is above or below the required level.
4	*Sooner than*	Performed faster or started earlier than required (overreaction)
5	*Later than*	Performed slower or initiated later than required.
6	*Opposite, too much or too little*	Performed in the opposite direction or way. An action that involves movement, force or rotation exceeds recommended control span.
7	*Other than*	A similar activity is taken on the wrong object or instrument.
8	*As well as*	An additional activity is performed that creates a side-effect.
9	*Repeated or continued*	The same activity is repeated a second time, or it is continued although the results are not in the expected direction.
10	*Out of sequence*	An activity is executed in the wrong sequence. A sequence of steps is stopped but resumed from an earlier or later step.

3.4.2.2 Cognitive (internal) error modes

Cognitive error modes are used in the functions of *identification*, *interpretation*, *decision-making* and *planning*. Table 3.3 provides a taxonomy of cognitive error modes which makes use of previous studies on several application domains (Rouse/Rouse 1983; Meister 1995). We assume that the four cognitive functions entail mental processes where operators make decisions about problem constraints, propose alternatives for solving the problem, perform an evaluation of alternatives, revising assessment, etc. (see also the list of performance mechanisms provided in the next section).

According to Table 3.3, cognitive functions may produce no results either because operators were unable to understand the situation and make a decision (item 1) or because another cognitive function was given priority (item 2). On the other hand, cognitive functions may produce correct but premature or delayed results (items 3 and 4), wrong results (items 5 and 6) and incomplete or insufficient results (items 7 and 8). Furthermore, wrong decisions and interpretations are assigned to two categories which are false acceptance of explanations or options (item 5: assuming that the correct one was not attended by operators) and false rejection of the correct explanation or option (item 6). Finally, Table 3.3 considers the case of interpreting feedback of previous

actions as well as additional information that arrive after operators have reached a decision (items 9-10).

Table 3.3: Taxonomy of cognitive error modes for identification, interpretation, decision-making and planning

Number	Keywords	Cognitive error modes
1	*Unable to understand or make plan/decision (inconclusive)*	Unable to understand causes or specify goals and plans, usually due to a fast evolving situation. It also includes failures to identify system states or monitor the effects of corrective actions.
2	*Priority error in plan/decision (misordered)*	Instead of making a decision or plan how to stabilise the system and maintain safety margin, operators persevere with interpretation.
3	*Premature plan/decision (sooner than)*	Correct but premature interpretation or selection of goals and plans. Premature decisions and hasty plans are vulnerable to new evidence or contingent events. For identification, the system is perceived as reaching a critical point when, in fact, it hasn't.
4	*Delayed plan/decision (later than)*	Correct but delayed interpretation or selection of goals. Plans may be too slow to achieve the goal or may be initiated too late. For identification, it implies delays in realising that the situation has changed as indicated by new information.
5	*Wrong plan/decision (other than, missed)*	Wrong explanations or goals have been accepted without paying attention to the correct ones. The inferred system state does not match the plant status information.
6	*Wrong plan/decision (as well as, unlikely)*	Considered but rejected the correct goal or explanation in favour of others that are sub-optimal or less likely to occur. Salient cues may shift attention to other states less unlikely to occur.
7	*Incomplete plan/ decision (part of)*	Incomplete identification of system state or explanation because some data were overlooked or discarded. An incomplete plan would achieve only part of the selected goal.
8	*Inefficient plan/decision (less than)*	Selected plan may involve errors in the sequence of steps, wrong control actions, or wrong cueing and timing of steps.
9	*Unable to detect or interpret feedback*	Feedback of corrective actions and changes of the situation are not monitored or not interpreted correctly giving rise to fixation.
10	*Unable to recover*	Problems with original interpretation or plan are recognised but operators can't recover errors due to limited time or knowledge.

3.4.3 Performance mechanisms

In the underlying methodology, human performance is seen as the interplay between work context or task demands (performance conditions) and human behaviour (performance mechanisms). In this respect, we cannot be dogmatic that certain forms of problem solving will lead to errors because the context of performance (e.g., available time, feedback, lack of interruptions) may provide opportunities for recovering

inappropriate actions or switching to more efficient strategies. On the other hand, what may constitute an efficient strategy could fail to produce positive outcomes in environments that present excessive task demands, prevent innovation and lack recovery opportunities. Performance mechanisms are aspects of *problem-solving* behaviour that appear to be common to the cognitive functions of *identification*, *interpretation*, *decision-making* and *planning*. Based on research on *problem-solving* behaviour (Klein et al. 1993; Frensch/Funke 1995; Goldstein/Levin 1987; Halpern 2003) a set of performance mechanisms is proposed in Table **3.4.**

Table 3.4: Performance mechanisms

Number	**Performance Mechanism**	**Explanation/Examples**
1	*Setting of problem boundaries and constraints*	To be performed with regard to time (e.g., abort diagnosis and try to stabilise system), human resources (e.g., sending an auxiliary operator on-site), tasks (e.g., interruption to tasks previously performed), procedures (e.g., compliance with operational procedures) and training (e.g., training practices related to the problem under consideration).
2	*Generating alternatives*	Searching and generating alternative explanations (diagnosis) of the situation and plausible goals or problem solutions
3	*Testing/evaluating alternatives*	Carry out an evaluation test to reduce the list of alternatives and converge to one explanation or solution
4	*Assessment of performance*	Establish revision steps to take into account new evidence as the situations deploys (self-assessment of diagnostic performance). This mechanism of self-assessment (see second part of the table) is particularly useful in addressing error recovery.
Self assessment		
4a	*Assess confidence in judgment*	Low confidence can lead to delays whilst over-confidence may lead to premature commitment.
4b	*Assess the "cost of being wrong"*	To be done in terms of delays in getting back to the right course, introducing side-effects and sanctions for inappropriate performance, etc.
4c	*Re-assess the situation*	Based on oncoming evidence from new events and actions previously taken.

These performance mechanisms provide safety analysts with a common framework to analyse human behaviour entailed in the cognitive functions of *identification*, *interpretation*, *choice of goals* and *planning*, i.e., input for defining and analysing cognitive error causes as also illustrated in Fig. **3.2**. The next two sections explain how these performance mechanisms are linked to the four cognitive functions.

3.4.3.1 Identification and Interpretation

It is useful to draw upon a distinction (Rasmussen 1986) between structural (state) identification (e.g. in terms of plant equipment, control room components, etc.) and functional (categorical) identification (e.g. in terms of cooling capacity, inventory functions, etc.). At the structural level, identification of a system state can be useful for matching a pattern of changes to a suitable operator response that can be retrieved from memory or operating procedures. At functional level, the identification can be useful for assigning situations into classes of events requiring a common response (Bainbridge 1989) which is more challenging than structural identification. This functional identification focuses on the situational constraints imposed on the availability of equipment, standby systems and operating personnel. As more evidence accumulates, operators are able to formulate more specific ideas about alternative explanations of problem causes and starting the interpretation phase. The process of (functional) interpretation entails making hypotheses about alternative causes and carrying out diagnosis tests. Criteria for diagnosis tests include replies to the following questions:

- Which is the most likely cause or the most serious cause to start with?
- How long it takes to carry out the test?
- Are there side effects in performing the test?
- How reliable the test may be?

Functional identification and interpretation can be seen as a continuum in our understanding of the situation. In process control industries (e.g., nuclear industry, Woods et al. 1990) and aviation industries (Amalberti/Deblon 1992), functional identification can bring the system to a relatively stable state and this takes precedence over making a precise diagnosis of problem causes. Some researchers (Acosta/Siu 1993; Gertman et al. 1996) refer to functional identification as global diagnosis whilst local diagnosis is reserved for functional interpretation.

The final aspect of “self-assessment of diagnostic performance” is very important in situations of high uncertainty because several subtle criteria are likely to influence operator confidence such as, compliance with procedures and team culture. In addition, the cost of misdiagnosis could be high, e.g., once an emergency response has been initiated, decisive cues arriving after diagnosis are missed since the multiple tasks initiated by the emergency response will capture attention. The financial costs of false emergency actions are sometime comparable with accidents' costs.

3.4.3.2 Decision-making (choice of goals) and Planning

Decision-making (choice of goals) can be seen as a cognitive process that entails thinking of alternative goals and possible goal-conflicts or tradeoffs. Several strategies have been proposed for comparing alternative goals in the decision-making literature (Hammond et al. 1987; Klein et al. 1993). However, justification for a decision may be examined easier on the basis of the criteria used and their perceived importance rather than the actual comparison strategy. It is useful, therefore, to draw attention to this process of criteria generation and prioritisation per se. Evaluation criteria should not be confined to short-term requirements but must include long-term criteria as well. Options must be balanced against future changes since one option may have a more stabilising effect on the system than another option. Other criteria for decision-making may be related to compliance with procedures, team culture and organisational policies; these criteria are likely to affect operator confidence in judgment and, hence, their decisions. A favoured goal that is not supported by the operating procedures and the team members, for instance, can make team leaders reluctant to take this goal or may delay their final decision.

Task planning is also a decision-making process that involves trading-off alternative means and resources how to achieve a particular goal. Other decisions may concern what goals take precedence and how to minimise the risks arising from unsatisfied criteria. More subtle criteria for selecting plans could involve "assessing the risk of being wrong" and "correcting a plan on the fly" and "cost of recovery" from several slips and lapses during the implementation of a plan. Finally, "re-assessing performance" can be seen as an important element of planning. In other words, a plan should incorporate a mental check on the progress made over a course of action to decide whether some modifications may be needed to correct errors or respond to unexpected events.

3.4.4 Performance conditions

The term "performance conditions" is used in the underlying methodology instead of the traditionally used "Performance Shaping Factors" (PSFs). Performance conditions offer some advantages over PSFs, with regard to testing their effects, incorporating them in task analysis and relating them to difficulties involved in situation assessment and decision-making. PSFs (e.g., training quality, operator experience, and operating procedures) are too broad and tend to be defined differently by several analysts. Inadequate training, for instance, can refer to inadequate operator plans, inexperience with multi-tasking, conflicting decision criteria and absence of verification tests to

crosscheck data reliability. All these factors are better stated independently because they have different effects on performance.

To evaluate the context in which human performance takes place, a literature review on performance conditions (Hollnagel 2006; Stanton et al. 2005) resulted in the development of a set of performance conditions as shown in Table **3.5**.

The descriptions in Table **3.5** also avoid "composite factors" (e.g., stress, workload, task complexity, etc.) that are the combined effect of several performance conditions. Stress, for instance, can be caused by time constraints, lack of plans to cope, requirements for multi-tasking, negative feedback of previous actions and personality factors. These composite factors, although strongly related to the context of performance, are rather ill suited for the analysis of human reliability due to the following reasons:

- The complexity of treating them within the work context because of their composite nature.

- The necessity of investigating personal aspects to ensure an adequate consideration of these composite factors in the analysis, e.g., personal data, personal behaviour, social problems of the examined person, etc. Persons' security laws and data security laws imposed many restrictions on analyses of this nature.

- The need to concentrate on measurable components that might influence these composite factors, e.g., availability of time, availability of instructions, accessibility of information, etc. as listed in Table **3.5**. Improving these (measurable) performance conditions will positively influence the composite factors.

It is also important that performance conditions are not evaluated in a "once-and-for-all" fashion but are evaluated throughout an entire analysis because events may evolve dynamically or the situation may exacerbate in cases of delays and errors.

Table 3.5: Performance conditions

Number	Performance Conditions	Explanation/Examples
1	*Availability of time to respond*	The time within which a task must be completed in order to avoid adverse consequences; it affects the depth of problem solving.
2	*Availability of plans and instructions*	Plans may be available but inaccessible because of the way they are trained (memory retrieval) or cast in procedures. Plans are followed rigidly or serve as guidelines for action.
3	*Availability and accessibility of information*	The organisation and representation of information on the interface, procedures, and drawings (poor design may include: delays in finding data, irrelevant information, ambiguities, and unreliable data).
4	*Number of parallel tasks*	Attending to or performing many tasks at close time proximity (multi-tasking, time-sharing).
5	*Criteria of choice & decision-making*	Criteria for evaluating goals may be competing (partially incompatible) or conflicting (mutually exclusive).
6	*System dynamics and coupling*	The response of the system (e.g., lags) and its coupling affects feed-back (e.g., delayed feedback) and task interactions (e.g., side-effects).
7	*Teamwork*	Teamwork may include: team communication, distribution of roles, team planning, and team culture.
8	*Supervision*	Supervision is necessary for allocating tasks, prioritising tasks, and providing redundancy (e.g., cross checking the work of colleagues).
9	*Organisational factors*	They include company policies for task scheduling, policies for job aids and training, manning levels, and company culture.
10	*Capability Degrading Factors (CDF)*	CDFs are environmental and workplace factors that affect operators in a global way (e.g., distractions due to noise, fatigue and life threats).

3.4.5 Cognitive Error Causes

The causes of cognitive errors can be traced into failures that result from the interaction between work context and human problem solving. This section examines several cognitive error causes in the functions of identification, interpretation, decision-making and task planning. The list is not exhaustive but indicates plausible forms of cognitive error causes.

3.4.5.1 Error causes in identification and interpretation

Searching for information to identify the system state or diagnose the causes of the problem can be seen as a decision process. Information search can be interpreted (Rouse/Rouse 1983) as a trade-off decision between accuracy (e.g. gaining a better understanding of the problem) and effort or cost (e.g. sending an operator to gather data at the cost of not becoming available for other tasks). Information search is also guided by interpretation and the context of the task, such as missing or ambiguous data, changing parameters and complex relationships between system units.

Table **3.6** provides a taxonomy of cognitive error causes by using the same categories that were applied to the performance mechanisms, i.e., *setting of problem constraints*, *generating alternatives*, *testing alternatives* and *assessment* (refer also to Table **3.4)**. Using the same categories makes sense because cognitive error causes are influenced by the performance mechanisms at the first level and then performance conditions (refer also to Fig. **3.1**).

Failures in identifying and prioritising constraints for information search (items 1- 2) must be understood in the context of multiplicity of constraints, such as, effort or cost in searching for information, compliance with team culture, and influences of organisational policies. The interpretation processes of explanation generation and testing have attracted a lot of research in the fault-diagnosis literature (Su/Govindaraj 1986), (Patrick 1993). Many studies assume that there is a set of faults which is consistent with the information available; as the failure event evolves, more evidence becomes available that enables operators to narrow down the possible problem causes into one or two alternatives. In this sense, an operator may be unable to think of any explanations, or think of a few only, i.e., missed correct explanation (item 3) or consider unlikely explanations (item 4).

Table 3.6: Taxonomy of cognitive error causes for identification, interpretation, decision-making and planning

Number	Keywords	Cognitive error causes or mechanisms
	Setting of problem constraints	
1	*Overlooked constraints/ criteria (missed)*	Overlooked constraints in searching information, coping with unreliable cues, or shifting attention to cues as situation evolves. Overlooked decision criteria or tradeoffs to evaluate alternative means to apply a plan of action.
2	*Misordered constraints/ criteria*	Wrong priorities for search constraints, decision criteria and evaluation criteria of goals and plans.
	Generating alternatives	
3	*Missed states, causes, goals (other than)*	Overlooked an important system state or explanation. Considered fewer alternative goals or means of plan of action.
4	*Unlikely states, goals, means (as well as)*	Spent time in considering unlikely system states, causes or options in terms of goals and means of implementation.
	Testing of alternatives	
5	*Interrupted test (part of)*	Hypothesis test was incomplete because of many interruptions. Plan interrupted due to distractions or overload of information.
6	*Inefficient test or method (less than)*	Inefficient test or shortcut in assessing possible explanations. Inefficient handling of tradeoffs between conflicting goals. Plan is inefficient as it lacks a mental check to stop errors, may generate side–effects, or can't cope with contingent events.
7	*Over/under estimation of criticality (misjudged)*	Misjudged the criticality of the situation, or the consequences of alternative decisions or means upon the current situation
	Assessment	
8	*Over/under estimation of the cost of recovery (neglected the cost of being wrong)*	Cost of being wrong and implications for recovery actions are not taken into account. Side-effects implied by certain means to achieve goals are not considered. Delays and problems in correcting errors or compensating for contingent events were under-estimated
9	*Over/under confidence (more or less than)*	More or less confidence invested on certain hypotheses and explanations, competence of staff, or support provided by operating procedures or team culture.
10	*Failure to revise assessment or plan*	Recovery cues are missed, masked or discarded, or not provided resulting in failure to change initial assessment of situation or plan.

Testing alternative explanations may consist of following a diagnostic procedure or carrying out a mental stimulation of the system to confirm the correctness of a hypothesis. A test of a plausible explanation may remain incomplete when interrupted

by new developments or poor communications (item 5). Shortcuts in diagnostic tests or errors in the execution of the test could also fail the evaluation process (item 6). Finally, operators may select an inefficient test to confirm their hypotheses. Understanding failures in complex systems usually retains some sort of uncertainty about the real causes of the problem. For this reason, diagnosis is affected by the seriousness of the situation (e.g., one explanation may imply that we should take more drastic actions than another) and the perceived cost of being wrong in assessing the situation (items 7- 8).

3.4.5.2 Error causes in decision-making

Identifying and prioritising the constraints under which decisions are made is an important aspect of the decision-making process because it permeates the processes of searching and testing alternative goals or options. In complex systems, operators may be concerned not only with technical constraints (e.g., effort to perform a task, existence of liquid inside a pipe, high temperature of the investigated object, etc.) but also with organisational constraints (e.g., compliance with procedures, training practices, organisational policies, etc.). An analysis of decision-making errors should examine how important constraints and evaluation criteria may be missed or prioritised erroneously as shown in Table **3.6** (items 1 and 2). The processes of goal generation and testing have been debated a lot in the decision-making literature (Klein et al. 1993; Frensch/Funke 1995). Although there has not been any agreement with regard to the way that goals are selected and tested (e.g., some favouring sequential evaluation over concurrent one), the concept of Decisional Balance Sheet (Kontogiannis 1996) provides a useful tool for integrating problem constraints with goal evaluation. Cognitive errors for goal generation and testing can assume similar forms to those of situation interpretation (items 3 – 7).

A more subtle process of decision-making involves allowing for the cost of being wrong, assessing confidence in judgment and establishing revision steps (items 8-10).

3.4.5.3 Error causes in planning

In many respects, task planning resembles decision-making in the sense that a decision should be made with regard to the most appropriate criteria for selecting means and resources to achieve a particular goal. One of the main aims of the underlying methodology is to identify the decisional conflicts behind different means and examine

how several performance conditions can affect the final decision of the operating personnel.

Table **3.6** quotes four error causes that can be applied in the *planning* phase[10]. These are: overlooking some important evaluation criteria (item 1), making an error in prioritising criteria (item 2), considering fewer means or missing an alternative mean (item 3) and considering unlikely means (item 4).

Testing a plan of action entails more than comparing alternative means and resources. Failures to think how to cope with possible side-effects or diversions of how the situation will evolve can also lead to inefficient plans (item 6). In this sense, operator can pre-plan how to counteract side-effects and exploit any opportunities available to change the direction of their solution. These contingency steps should be thought of and organised well in advance of the execution of the actual plan to counteract any side effects. Neglecting to do that can make plan adaptations difficult to achieve within the short time window allowed, i.e., underestimation of situation criticality (item 7). In a similar manner, plan interruptions due to distractions or information overload can lead to incomplete tests and escalate the situation (item 5).

A related aspect of planning is remaining alert to changes of the situation and feedback that would signify inadequacies in the adopted plan. Operators may fail to revise a plan that is proving inadequate because recovery cues are not provided or not communicated in time or they are missed out (item 10). On the other hand, operators may have realised that the current plan is running into trouble but the cost of recovery and change to a new plan could be very high (item 8). Modifying plans as the situation worsens entails a complex process of forecasting side-effects of new plans and modifications in the context of high uncertainty and criticality. In many cases, the cost of changing to a new plan may be unjustified. Finally, the confidence of team members (item 9) on the support provided by procedures, team communications and organisational policies could affect their decision whether to change to a new course of action. In some cases, for instance, team members may need to react quickly even without agreement from the team leader. An authoritarian team organisation would make re-planning difficult to adapt to such circumstances.

[10] Additional error causes can be examined within the particular task context.

3.4.6 Error detection and recovery

With the increasing complexity of technical systems, there has been a realisation that total elimination of human error may be difficult to achieve. There are always complex situations in which errors may creep up due to high workload, psychological stress and poor team coordination. What seems to be more important in these situations is the prevention or containment of adverse consequences through the detection and correction of errors rather than the prevention or avoidance of errors in the first place. An important area elaborated in this framework is the issue of error detection and recovery, which has not been addressed systematically in error modelling.

While in error prevention we intervene between the action and the error, in error recovery we intervene between the error and the negative consequences as shown in Fig. **3.4**. In this figure, "consequences 1" correspond to an error propagation in which neither an error prevention nor an error recovery is possible. "Consequences 2" correspond to a successful process of error prevention whereas "consequences 3" correspond to a successful process of error recovery. The backward loops represent feedbacks for improving the performance of the action and developing better strategies for prevention and recovery.

We may distinguish two broad strategies in managing error recovery. The first strategy is to facilitate operators to correct their errors (*error handling*) while the second strategy (*mitigation*) is to minimise error consequences through system design (e.g., delaying the propagation of consequences, or preventing errors from being implemented by introducing limiting functions).

Studies in error recovery (Rizzo et al. 1995; Kanse/van der Schaaf 2001) have tended to distinguish three processes in error handling or error recovery, namely:

- ***Error detection*** - realising that an error is about to occur or suspecting that an error occurred, independent from understanding the cause of the error
- ***Error explanation*** - explaining why an error occurred
- ***Error correction*** - modifying a plan or developing a new one to compensate

The first mechanism of error detection takes place at the conceptual stage of identification, interpretation, decision-making and planning (e.g., wrong intentions, mismatches between intentions and plans, inadequate plans, etc.). The second mechanism takes place at the execution or outcome stage by monitoring the results of an action (e.g., a mismatch between expected results and observed outcomes). This

mechanism relies on a self-monitoring function that captures errors before any consequences are ensued.

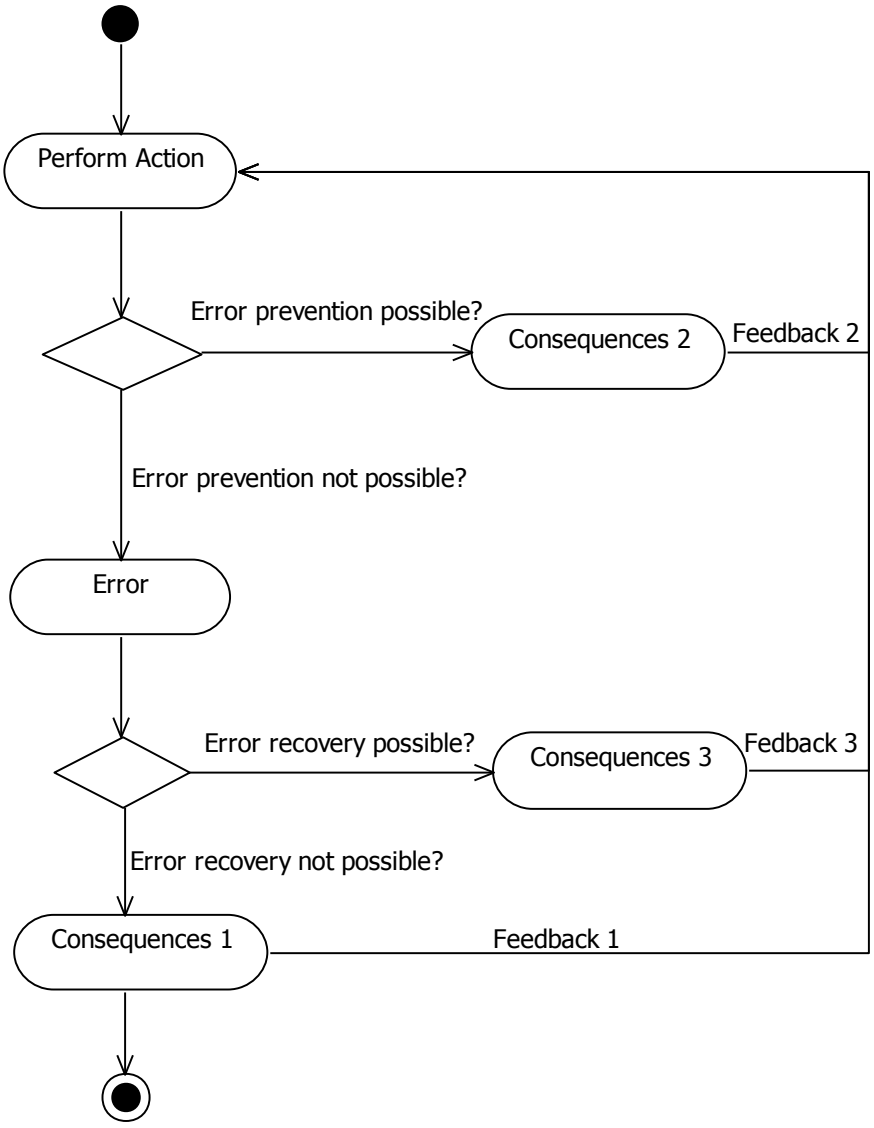


Fig. 3.4: A process diagram for error prevention and error recovery

Once an error has been detected, operators may try to identify or explain the causes of the error. The contribution of the error explanation phase to the error handling process is still a topic with a lot of research potential.

Error correction is a complex process that takes several forms. Three possible corrective goals in error correction have been distinguished in the literature (Mo/Crouzet 1996; Kontogiannis 1999):

- Backward recovery: the system is brought back to its initial state prior to the occurrence of the failure; this means that operators have got the means to reverse or "undo" the effects of their actions.

- Forward recovery: the system is brought into an intermediate state in order for the operators to "buy time" and find a better solution later on.

- Compensatory recovery: where redundant equipment is activated to bring the system to the final state that was desired.

In many critical situations, operators have to react quickly even when a thorough understanding of the problem has not been achieved yet. In these cases, the adopted plan should still allow operators to continue gathering new data to understand the situation better and, at the same time, respond to any adverse consequences and minimise an escalation of the problem. This is the concept of *viable plans* that allow operators to explore opportunities for detecting their errors and correcting their understanding of the situation or amending plans online to contain the problem. It is important, therefore, that some desirable features are proposed with regard to viable plans and specifically their control mechanism, capacity to cope with uncertainty, and their structure as explained below.

First, a viable plan should have a control mechanism that monitors progress towards the goal as well as any changes of the situation that may challenge current understanding. This control mechanism is important for error detection and re-assessment of problem diagnosis. Experienced operators make certain assumptions in order to build a coherent explanation of the situation and accept them as true until there is some reason to doubt them. Unfortunately, some assumptions may remain "hidden" and never get tested as operators may be unaware of them. Finding and testing hidden assumptions is part of the control mechanism for detecting errors and misunderstandings of the situation.

Testing the plausibility of assumptions may entail cognitive processes such as seeing whether a change is levelled-off or made worse in future, cross-checking functionally-relevant data (e.g., a temperature rise should be followed by a similar rise in pressure), and verifying the correct functioning of sensors. Taking account of temporal and relational patterns of cues is an operator search strategy that applies equally well to the interpretation of action outcomes. Due to limitations in time and resources, some assumptions may not be possible to test but this is not a sufficient reason to reject a conclusion. Operators should have several options to consider when an assessment rests on untested assumptions.

This brings up the second feature of viable plans with regard to their capacity to cope with untested assumptions, unsatisfied decision criteria and contingent events as the situation unfolds dynamically. When a diagnosis of the situation rests on untested assumptions, operators should acknowledge the risks in their current assessment but take corrective actions so that their plans do not depend upon these assumptions. Alternatively, they may develop contingency plans that specify how to counteract the risks arising from assumptions that have not been tested in the past. A similar approach can be taken for decision-making and planning where there is a residual cost of being wrong (e.g., certain goal tradeoffs and plan side-effects cannot be solved). In this sense, a viable plan should have some spare capacity to cope with unsatisfied decision criteria and plan side-effects at a later stage when such a risk may materialise. The spare capacity refers to the additional work involved in planning ahead of time about redundant human resources, standby equipment, and back-up means in cases of system failures.

Finally, a viable plan should have a "modular structure" that would allow operators to make changes in one part of the plan without worrying how the changes affect the other parts. In the opposite side, an "integrative structure" may be efficient in optimising resources and costs but would increase the coupling or dependencies between tasks. Drawing an analogy with "tight coupling systems" (Perrow 1984), it is possible to specify some features of modular plans. In this respect, error detection and recovery may be supported when plans take into account of the following issues:

- Identify alternative means of executing tasks and select those that do not affect performance of the following task.
- Build barriers between tasks so that errors do not propagate to the next task, thus making the final symptom easier to detect and attribute to the failed task.
- Delay performance of the second task until feedback from the first is available.

Overall, the control mechanism of a viable plan is important for detecting and correcting errors in the interpretation of the situation whilst a modular structure and a spare capacity are more appropriate for criticising and correcting decisions and plans of action. Section 3.5 shows how the concept of viable plans can be incorporated into a dynamic event tree (DET) to model the recovery of cognitive errors.

3.5 Applying the methodology to risk analysis

Since the underlying methodology aims at assisting safety or risk analysts in the qualitative analysis of cognitive reliability, human error prediction and analysis, it is necessary to simplify using it by drawing out the steps of applying this methodology to operational safety and risk analysis tasks.

Fig. **3.5** illustrates the steps of applying the methodology on risk analysis by utilising the taxonomies and findings provided in this chapter.

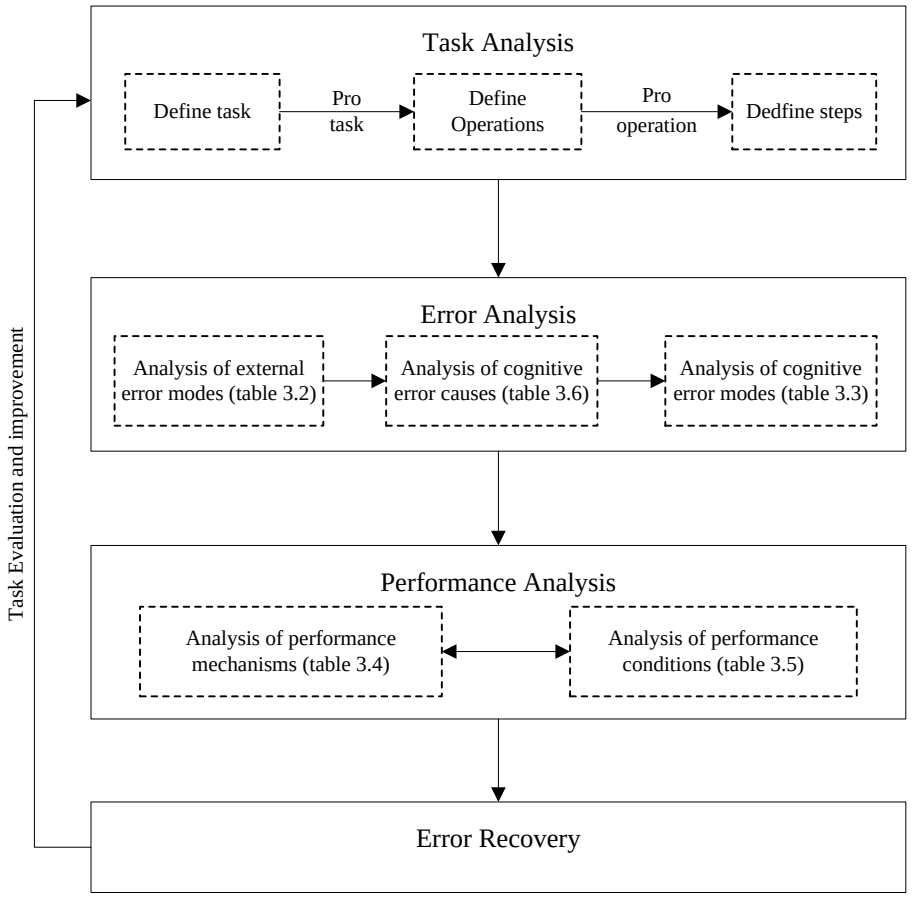


Fig. 3.5: Graphical representation of the methodology and steps of applying it to risk analysis

The contribution of the underlying methodology to risk analysis can be summarised by two major points:

1. Identifying cognitive error modes and error causes behind unsafe interventions (i.e., external error modes). Using the methodology to perform a task analysis and error analysis of operations can reveal several unsafe interventions that could be caused by delayed diagnosis, inefficient planning, wrong decisions, etc.

This first contribution to risk analysis is achieved by implementing the first three stages (refer to Fig. **3.5**) of the methodology that can be applied upon examining human reliability within the framework of risk analysis. These three stages are:

a. Task analysis of operator decision points, information needs to assess the situation, and detailed plans to achieve task goals.

b. Error analysis which covers:

   - Analysis of external error modes;
   - Analysis of cognitive (internal) error modes;
   - Analysis of cognitive error causes.

c. Performance analysis which covers:

   - Analysis of performance mechanisms;
   - Analysis of performance conditions such as, availability of plans (i.e., training and procedures), time window for response, decision criteria, goal tradeoffs, expertise, supervision and teamwork.

2. Modelling paths of error modes and recovery opportunities as the situation unfolds dynamically and performance conditions change in the course of events (e.g., control panel information, additional tasks, and capability degrading factors). In other words, the cognitive error modes identified in task analysis and error analysis are modelled in terms of a dynamic cognitive event tree so that opportunities for error detection and recovery are explored in the context of specific scenarios.

This second contribution to risk analysis is achieved by defining recovery plans and the producing dynamic event tree (DET), which combines error modes with opportunities for error recovery. This event tree consists of a tree representation of cognitive error modes and another tree of error recovery paths. Fig. **3.6** shows a tree representation of cognitive error modes identified through a process of task and error analysis in a generic scenario where operators try to respond to equipment failures. Unsafe interventions (i.e., wrong action or check) can be due to mistakes, slips or lapses; however, in order to keep the representation simple, slips and lapses are not shown here. The dotted paths with the designation "*continued*" refer to paths which can be further detailed or involve more tree branches. The continuation in these paths is not illustrated in Fig. **3.6** and the attention is paid to the outcome related to paths with "success" or "go to next tree" outcome (e.g., paths 1 and 2 in Fig. **3.6**).

In principle, a dynamic event tree explores many points in time where operators alternate between understanding the problem (i.e., functional identification and diagnosis) and responding to the problem (i.e., decision-making and planning). The DETAM method (Gertman et al. 1996), for instance, explores all possible combinations of understanding and responding at set time intervals (e.g., every minute). To avoid the huge space of event trees that result from this approach, we focus only on some critical points in time where significant changes occur in understanding and responding to the problem. Safety analysts start with a list of credible errors in functional identification or diagnosis and try to find whether a "viable plan" can help operators recover their errors.

A misdiagnosis or delayed diagnosis could be recovered when a correct functional diagnosis is made. For instance, operators may identify correctly the problem in functional terms (e.g., a gas leakage) but the diagnosis of the precise cause has to consider several possibilities (e.g., leakage location, leakage size, etc.). Fig. **3.6** represents an example of delayed diagnosis that could be due to several error causes (e.g., missing correct explanations or performing an inefficient diagnostic test). A viable plan would enable operators to recover diagnostic errors before it is too late. For this to happen, the viable plan should have a control mechanism that continues to gather information without fixating on one hypothesis only. Path 5 shows a recovery route that is further explored in order to produce another dynamic tree for error detection and recovery (Fig. **3.7**). A viable plan pays attention to additional recovery cues that form a meaningful pattern for diagnosis (box 6). These meaningful patterns might be utilised to re-diagnose and either yield a successful diagnosis (recovered one) or a wrong one that does not allow a recovery on time (path 15). In case of a correct recovered diagnosis, an ideal recovery can be achieved, if the available time window would allow operators to compensate with a proper response (paths 8, 9 and10).

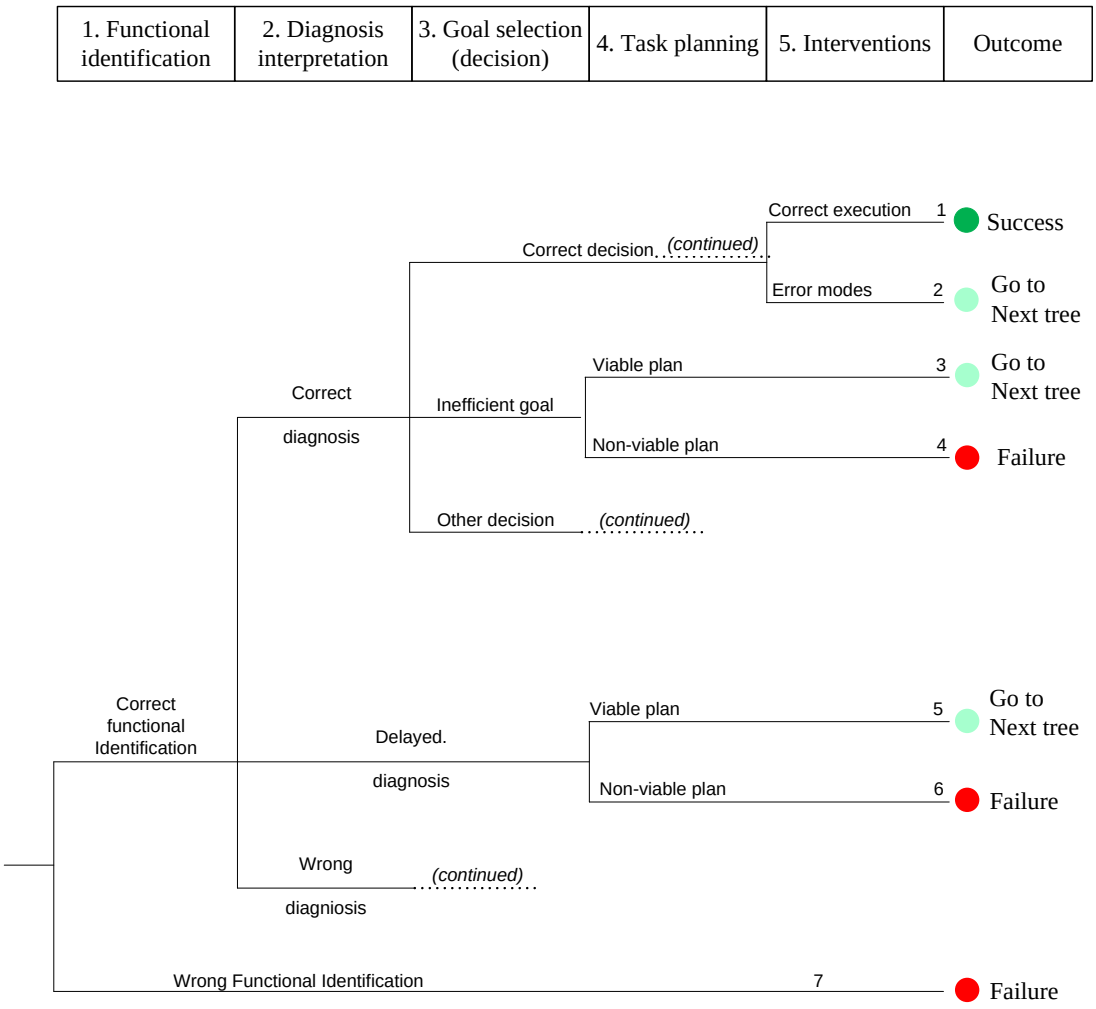


Fig. 3.6: A dynamic event tree of cognitive errors and viable plans

The concept of "viable plans" can also be applied to goal selection and task planning. Plans that have a modular structure and a spare capacity for dealing with unsatisfied criteria and contingent events can enable operators to recover from errors (path 3 in Fig. **3.6**). A spare plan capacity implies some form of pre-planning how to counteract side-effects and exploit any opportunities available to change the direction of their solution.

The last two decision nodes in boxes 9-10 (Fig. **3.7**) address the issues of error correction and mitigation (see Section 3.4.6). Error correction may take the form of backward recovery or "undo" (path 8), forward recovery (path 9) and use of redundant equipment (path 10). Several mitigation policies (e.g., delaying the propagation of consequences, or limiting functions) can minimise error consequences even in cases that errors cannot be corrected in time (path 11).

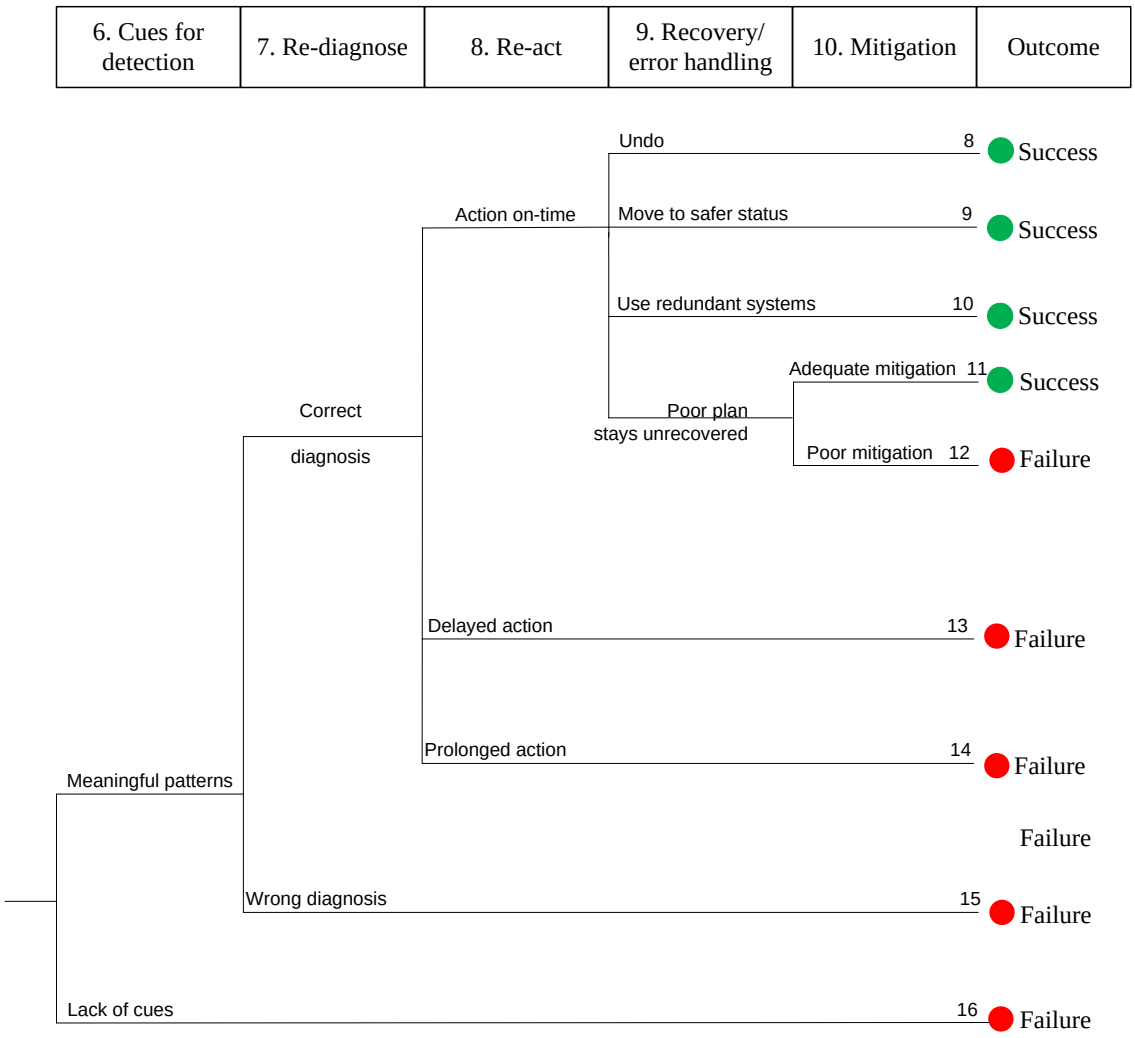


Fig. 3.7: A dynamic event tree of error detection and recovery

3.6 Summary

In this chapter a HF methodology for supporting risk analysis which takes the human behaviour and performance into consideration, i.e., human errors, has been introduced. It assists safety analysts in the qualitative analysis of cognitive reliability in process control tasks. The proposed methodology has four focal points: a causal model of operator behaviour, a HAZOP-like taxonomy of cognitive error modes and error causes, a dynamic representation of the interaction between work context and human behaviour, and a recovery model for detecting and correcting errors.

In comparison to the conventional event trees and fault trees used in risk analysis, the underlying methodology provides an explicit way of modelling:

- How error modes arise out of the context of work (e.g., conflicting goals, multiple tasks, inadequate procedures).
- How error modes are affected by previous decisions made by operators.
- How consequences propagate throughput the system in the dynamic event tree.
- What aspects of system complexity and coupling can reduce the available time and resources and, hence, hinder error recovery.

The methodology was developed based on limitations of existing methodologies and provides a comprehensible tool for analysing human error in complex industries. It has been taken as a reference for identifying the VR functional requirements in the next chapter. However, it has not been validated in a formal risk analysis study yet due to difficulties at some envisaged industrial sites. The primary objective of the methodology has been to help safety analysts to examine how operator performance may change in the course of an accident scenario. For this reason, a dynamic event tree for error recovery has been suggested in Fig. **3.6**. However, the methodology cannot generate estimates of time availability for error recovery because it does not include a model of plant behaviour and response. Other dynamic event trees (Acosta/Siu, 1993; Cojazzi/Cacciabue 1994) may overcome this specific problem but they are very demanding in time or resources and fall into another category of methodologies. Finally, error quantification has received limited attention in this methodology. It is understood, however, that expert judgment in quantification can benefit from an analysis of cognitive error causes and performance conditions where extrapolations of human error probabilities are made from simulator data and comparisons with other tasks.

The underlying methodology has also other benefits, aside from supporting risk analysis work. For instance, it can be used to examine how the presentation of information on the control panel can provide valuable cues for error detection. The methodology can be also used to evaluate operating procedures. The application of performance mechanisms and performance conditions can help safety analysts to identify goal trade-offs, conflicts between procedural compliance and performance variations, weak points in traversing from one procedure to another, and difficulties in monitoring progress within particular goals. Special warnings and notes can be inserted in the procedures to provide more opportunities for error detection and recovery. Finally, the concept of viable plans can be applied to examine how to design robust operating procedures that allow operators to explore new ways of carrying out tasks provided that they made a correct functional identification of the problem.

In summary, this methodology has sought to enhance the communication between safety analysts and the cognitive science community in the analysis of human reliability in process control systems. A model of human performance was presented and cast in terms of HAZOP-like taxonomies of cognitive error modes and error causes. The methodology demonstrates also the difficulties in characterising operator's diagnosis or decision as erroneous in the first place, i.e., the safety analysts have to consider all possible error recovery opportunities to become confident that the operator's diagnosis or decision was faulty. New developments in HRA methods should continue to address more aspects of error explanation, error recovery and explore models of dependency that may threaten opportunities for recovery.

A validation of the underlying methodology based on a real case study from the chemical process industry is presented in Chapter 6. The validation provides – among others – customised tables based on the taxonomies provided here, illustration of recovery paths using the dynamic event trees, possible risk and accident scenarios, influence of work context on the task under consideration, deficiencies in the operational procedures, etc.

4
Functional VR requirements and specifications

This chapter provides the functional requirements and feature specifications for improving risk analysis work using a VR environment. The definition of these functional requirements is based on end user scenarios (requirements) from the research domain (chemical process industry) and applying the HF methodology developed in Chapter 3 to these end user requirements.

4.1 Definitions

Before moving into the process of extracting functional end user requirements, the following definitions should be introduced and aim at providing understanding of the remaining parts of this chapter.

Functional requirements are "descriptions of the functionality delivered by software to its users" (Ebert/Dumke (2007), pp. 170). They provide information on the tasks and features of the software without detailing technical or quality requirements on its performance.

Non functional requirements are criteria that can be used to judge the operation and performance of a system, e.g., usability, testability, maintainability, extensibility, scalability, etc. (Ludewig/Lichter 2007)

Since the underlying thesis proposes a VR system layout (system design) which requires the definition of features and functionalities that should be considered in such a system, i.e., functional requirements, the focus here is on functional end user requirements as illustrated in this chapter.

Based on the fact that running and operating the proposed system design are not goals of this thesis, the criteria for evaluating its performance or operation, i.e., non functional requirements, is not a point of focus here. Focusing on functional requirements has been also favoured by end users due to their need of solving a demanding problem without defining pre-requisites on system performance, its usability or similar aspects.

4.2 The approach

The term "approach" here refers to the steps that are applied to define VR functional requirements based on end user scenarios. These steps are:

- Development of end user scenarios and requirements (Section 4.3);

- Applying the HF methodology developed in Chapter 3 to end user requirements:
  - Clustering the HF methodology (Section 4.4);
  - Definition of the functions covered by the clusters (Section 4.4);
  - Mapping end user requirements to the HF methodology (Section 4.5).
- Identifying functional VR requirements (Section 4.6).

Section 4.7 maps the identified functional VR requirements to technical features and modules as an intermediate step for the VR environment design (Chapter 5). Section 4.8 provides a functional model that links these modules and describes the information flow among them.

Fig. **4.1** illustrates these steps (the dark coloured boxes with bold text) based on an extraction from the integrated method presented in Chapter 1 (Fig. **1.2**).

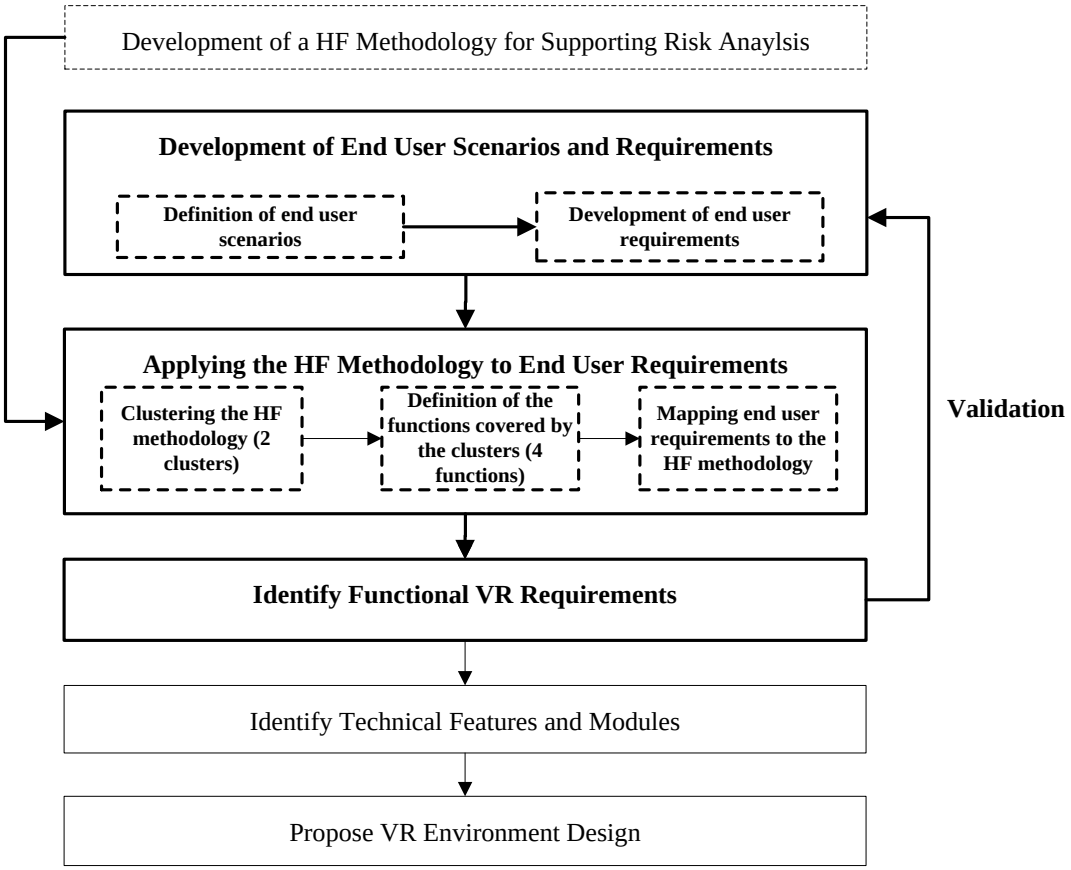


Fig. 4.1: The steps (dark boxes) of identifying VR functional requirements as part of the integrated method (Fig. **1.2**)

4.3 Development of end user scenarios and requirements

The development of end user scenarios as base for the definition of end user requirements took place within the framework of a multinational research project with the goal of improving safety at production plants and storage sites. In this regard, several workshops and interviews were carried out with end users (e.g., plant managers, safety analysts, plant engineers, shift supervisors, control room operators, field operators, etc.) from the research domain to identify typical safety scenarios. These safety scenarios are used as base for defining the end user requirements necessary for improving risk analysis. The interviewed persons have been asked about:

- Scenario general information: scenario name, origin of scenario (industry), short summary on scenario.
- A description of the problem that is being faced in the scenario and could be addressed by a VR solution.
- The staff members who are primarily faced with the situation/problem, e.g., field operator, safety manager, production engineers, etc.
- Description of the operational task(s) of the scenario, e.g., operation steps, involved plant items, available documentation, etc.
- Description of safety challenges in the scenario, e.g., impact of a poor execution of the task, frequency of the scenario critical events (frequent or rare), consequences, etc.
- Description of human factors related aspects in the scenario, e.g., human errors, error causes, performance conditions (work context), possibilities of error recovery, error consequences, etc.
- Description of how VR could assist in addressing the problem, e.g., navigating in a 3D scene to get familiar with plant objects, visualise and test properties of equipment to identify possible sources of risks, providing an interface for safety managers to introduce “virtual errors” in the scene, etc.

The result of the scenario generation phase was a set of 21 applicable safety scenarios (Gounelle et al. 2007).

In the second phase, the scenario details from the first phase have been used to formulate generic end user requirements, which have been considered as guidelines for applying the HF methodology (Section 4.4 and 4.5) and identifying the VR functional

requirements (Section 4.6). The result of this phase was a set of 19 end user requirements that have been classified into "requirements for modelling human error" or "requirements for modelling work context" and provided in Table **4.1**[11]. The scenarios and requirements have been reviewed and validated in further workshops as explained in Chapter 6. The list of requirements is not exhaustive, but indicates demanding requirements for improving risk analysis work in the domain industry as conceived by representatives of the domain industries during the scenario preparation and validation workshops.

It is worth mentioning that an explicit formulation of human factors related aspects by end users was not possible at this stage as most of the interviewed end users have no human factors background. This effect is noticed in Table **4.1** by the inability to distinguish between technological requirements (i.e., VR related) and HF related requirements (from an end user point of view). To overcome this obstacle at this stage, the end users have been sensitised to the human factors aspect, that match the underlying scenario, e.g., work context that might positively affect the scenario, human errors in similar situations based on their experience, organisational factors that influence the scenario, environmental conditions accompanying the scenario (noise, snow, etc.), possibilities or error recovery, qualification and experience levels of operators involved in the scenario, etc. This sensitisation enabled an adequate inclusion of human factors at this early stage. In the next step (Section 4.4 and 4.5), a more structured reflection of human factors based on the developed methodology (Chapter 3) took place and provided more confidence of a better consideration of relevant human factors in these requirements.

4.4 Clustering the HF methodology and definition of clusters' functions

In this step, a clustering of the HF methodology (Chapter 3) in terms of its modelling nature and a definition of cluster's functions is carried out. This intermediate step aims at a structured inclusion of human factors in the end users requirements.

The starting point here is the basic elements of the HF methodology which were introduced in Chapter 3 (Fig. **3.2**). These are[12]:

[11] To avoid duplication and provide them in categorised form, the end user requirements are listed only in Table 4.1 (Section 4.5).

[12] The remaining elements in Fig. 3.2 (unsafe intervention, consequences and system defences) represent actions and consequences of making a mistake, i.e., elements of a post-analysis (accident analysis) which is not the goal of the underlying research.

- Cognitive error causes;
- Cognitive error modes;
- Error recovery;
- performance mechanisms;
- Performance conditions.

To facilitate the process of reflecting these five elements in the end user requirements, these elements have been assigned to two clusters: a cluster for modelling human error and a cluster for modelling work context. The cluster "modelling human errors" includes the elements that deal with the human error and its causes which are: cognitive error causes, cognitive error modes and error recovery. The second cluster "modelling performance context" deals with the interplay between workplace factors and human performance and includes performance mechanisms and performance conditions.

Fig. **4.2** illustrates the two clusters and their elements. The direction of the arrows inside the cluster "modelling human error" refers to the information flow depicted in Fig. **3.2**. In the cluster "modelling performance context", the arrow refers to the interplay between performance conditions (work context) and human behaviour (performance mechanisms). The double sided arrow between the two clusters indicates the mutual impact of each cluster on the other, e.g., a human error would influence the performance context by proposing improvements in the work context and vice versa.

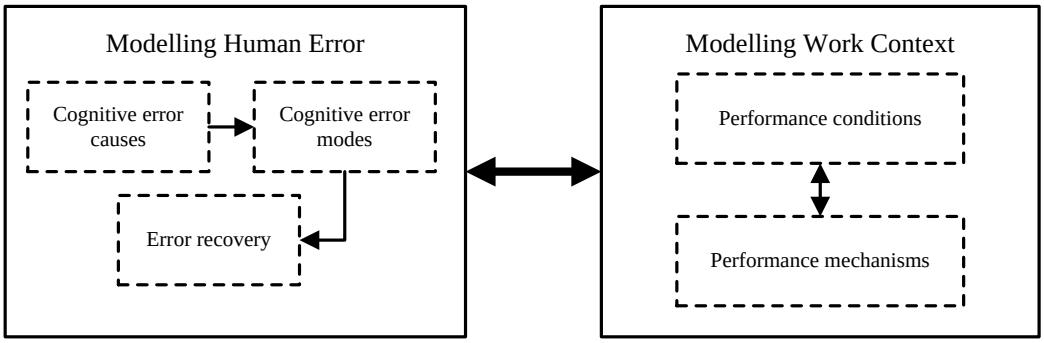


Fig. 4.2: The interplay between the two clusters of the HF methodology (Salem 2008)

Based on the predefined two clusters, the functions that are covered in each cluster are provided here (Salem 2008; Salem/Kontogiannis 2007):

Cluster 1: ***Modelling human errors***, i.e., defining functions (later: functional VR requirements) for understanding and representing the human error. This cluster covers the following functions:

Functions for errors in identification and interpretation which are covered by the following sub-functions:

- Familiarisation with plant layout and equipment design
- Identification and prevention of hazards by means of barriers (plant hazards, site hazards, human hazards, etc.)

Functions for errors in decision making and planning which are covered by the following sub-functions:

- Prediction of how the plant responds to disturbances and the impact of multiple events
- Identification and detection of errors and examination of task variations and error shaping factors
- Identification of error consequences
- Recording of human response and performance

Functions for error recovery which are covered by the following sub-functions:

- Error management
- Error correction

Cluster 2: ***Modelling work context***, i.e., defining functions for understanding and representing the performance conditions and mechanisms that affect the human performance. This cluster covers the following functions:

Functions for representing work constraints which are covered by the following sub-functions:

- Manipulation of information and work constraints
- Manipulation of ambient conditions
- Manipulation of team composition and interaction

4.5 Mapping end user requirements to the HF methodology

To ensure that the end user requirements are being considered from a HF perspective and to provide a structured reflection of these requirements, a mapping of the predefined requirements (Section 4.3) to the clusters of the HF methodology (Section 4.4) is carried out. The mapping process is based on assigning each of the end users requirements to one of the four aforementioned functions of the HF methodology (i.e., the four groups of functions listed under the two clusters). The result of this mapping is provided in Table **4.1**.

4.6 Identifying functional VR requirements

The only remaining step in the process of defining the functional VR requirements is to derive the VR support needed to represent the set of functions and sub-functions which have been defined in Section 4.4. This approach also ensures reflecting the end user requirements since they have been mapped to these functions as shown in Table **4.1**.

For the purpose of deriving these functional requirements, an information acquisition approach based on the following elements was applied:

1. An analysis of some VR systems and tools regarding their technical features in supporting the predefined functions, sub-functions and consequently the end user requirements;

2. Personal experience in VR environment design and scenario authoring;

3. Literature reviews in similar areas of applications (Salem/Kontogiannis 2007), (Loupus et al. 2007a), (Loupus et al. 2007b), (Bell/Folger 1996), (Haller et al. 1999), (Marsot et al. 2004), (Villa-Uriol et al. 2005), (Schatrik et al. 2003), (Gabbard et al. 1999).

Table 4.1: Mapping end user requirements to the HF methodology

Cluster	Function	End user requirements
Modelling Human Error	*1. Functions for errors in identification and interpretation* *2. Functions for errors in decision making and planning* *3. Functions for error recovery*	Req. 2: Improve existing Human Failure data and collections Req. 3: Allow industries and analysts to investigate events with extremely low likelihoods of occurrence Req. 4: Integrate equipment and human failures, and subsequently quantify failure probabilities Req. 5: Identify Operator Failure modes and responsiveness, such as time to act, assessment of decisional factors and influencing factors Req. 6: Identify the chain events that can lead to operator failures Req. 8: Examine whether an undesirable event can be stopped either by certain safety barriers or by human intervention including error detection and correction Req. 9: Represent official operating procedures and distinguish between permissible deviations and critical human errors Req. 11: Record, discuss and test - in an experimental facility - assumptions about human performance in certain conditions Req. 14: Provide estimates on parameters that only exist as an assumption and validate these estimates in the VR environment based on real operating situations Req. 16: Collect data about delays that may lead to crucial factors (e.g., pressing the emergency shutdown button when it is too late) Req. 17: Collect data about several types of human error related to different tasks (e.g., forgetting to test the reliability of gas detectors, starting the detection process from an inappropriate location, etc.);
Modelling Work Context	*4. Functions for representing work constraints*	Req. 1: Postulate hazards and incidents in different positions around a plant using a virtual environment with suitable task representations Req. 7: Integrate Risk Analysis methods and allow transfer of data about tasks, human errors and organisational factors Req. 10: Stimulate discussions between safety analysts (by means of virtual interactive meetings and discussions), training officers and operators on how to get a "feel" of the reliability of their assumptions Req. 12: Assess the combined effects of workplace & organisational factors in the risk assessment process Req. 13: Provide real-time approximate dynamic simulations of toxic dispersion, fire etc. for the operator to interact with (This creates a real-time dynamic response from the operator-process system and can drive the decision for further/different studies); Req. 15: Provide feedback for improving operational procedures Req. 18: Examine how the context of work affects human response and error probabilities. For this purpose, the same task can be carried out under different conditions (e.g., weather conditions, one or two field operators, easy vs. difficult access, etc.) Req. 19: Develop measures to reduce the overall risk by means of task and team changes. For instance, tasks can be tried out in different sequences or assigned to two or more operators in order to examine whether the overall risk is reduced.

Table **4.2** lists the functional VR requirements which can be further used as a base for a VR environment design. The list is not exhaustive but provides a set of 57 major functionalities that have been classified by end users as fundamental for supporting the risk analysis work in a VR environment under the consideration of non-negligible human factors aspects.

The provided list can be seen as a checklist for a VR system design in the target industry, i.e., guideline for functional software design. Since such a list can be further extended to include arising needs, e.g., due to plant's design changes or operational process modifications, the software design should enable adding new features to reflect the real setting with higher degree of completeness.

Table 4.2: Functional VR requirements

Cluster	Function	Sub-Function	Functional VR requirements
Modelling Human Error	*Functions for errors in identification and interpretation*	Familiarisation with plant layout and equipment design	1. Navigating in a 3D plant scene and superimposing on it a section of a Pipes and Instrumentation Diagram (P&ID) (e.g., walk-through) 2. Visualising and navigating inside the hardware components (walk-through, changes of view point, camera movement, etc.) 3. View a hierarchical decomposition of the plant in terms of units and equipment and Present virtual menus to search for equipment that its location is difficult to find 4. View geographical layout of units and equipment as well as all emergency exits and assembly points 5. Present virtual labels on equipment with appropriate information (e.g., name, purpose of use, constrains in use, etc) 6. Visualising and testing the properties of equipment to identify possible sources of accidents and eliminate unsafe operations or disassembly methods (e.g., hide/unhide) 7. Visualising pipelines and vessels (inside/outside) and extracting/calculating necessary parameters (e.g., volume, inventory, viscosity, etc) 8. Validating safety procedures by inserting virtual components inside the real plant (Augmented Reality) and testing whether the adopted plant design suits the desired safety requirements 9. Detecting and controlling sources of fire and explosion (e.g., sparks, frictions, high temperature surfaces) by means of object selection, setting transparencies, highlighting high-temperature surfaces, etc.
		Identification and prevention of hazards by means of barriers (plant hazards, site hazards, human hazards, etc.)	10. Presenting a catalogue of physical barriers to try-out in order to prevent or neutralise hazards. 11. Displaying the consequences of physical barriers both in real-time and in a fast-forward mode. 12. Simulating distressing environmental conditions and input variations to examine how robust a physical barrier may be (e.g., corrosion, heat stress, etc) 13. Examining how difficult it is to inspect physical barriers and carry out maintenance activities to keep them functional.

			14. Examining cases of inappropriate use of barriers where the barrier is used rather late, or in the wrong way. 15. Linking the VR scene with the dynamic process simulator to provide additional information about the behaviour of the plant in normal conditions as well as the response of the plant to abnormal events.
	Functions for errors in decision making and planning	Prediction of how the plant responds to disturbances and the impact of multiple events	16. Visualising and navigating inside the plant components 17. Creating and saving animations of single events and multiple events that can causes disturbances, e.g., a set of pointers and connections on the equipment affected by the disturbance, a set of pointers to indicate the sequence of the propagation of event, a virtual menu that contrasts the effects of two or more events in terms of a set of common and different process parameters 18. Using overlays or transparencies so that the effect of one event is superimposed on the effects of previous events, e.g., display all affected equipment in a highlighted or flashing mode, hide all items apart from the affected equipment, etc. 19. Coupling the VR environment with available simulators (process simulator, training simulator, etc.) 20. Enabling "what if" scenarios and a visual distinction of different event outcomes in order to check whether expectations match with reality 21. Visualising clouds of hazardous substances and changes in dispersion influenced by wind and rain 22. Identifying possible escalation scenarios when a hazardous material approaches any ignition sources (collision-detection)
		Identification and detection of errors / Examination of task variations and error shaping factors	23. Allowing a 3D visualisation of possible error shaping factors (e.g., ineffective barriers, faulty equipment, difficult access, etc) 24. Interactive exercises on possible error-shaping factors and erroneous actions 25. Using animations of mal-practices and asking operators to detect errors 26. Allowing task variations to occur from pre-defined procedures and visualising their effects
		Identification of error consequences	27. Visualising the propagation of the effects of human errors and equipment failures on the whole plant 28. Increasing or switching the Field Of View of operators so that they oversee the work

			of their colleagues and correct errors 29. Assessing different human responses by online visual comparisons of their system consequences 30. Providing an interface for safety managers to introduce "virtual errors" (e.g., false job card, work interruptions) and ask operators to correct them
		Recording of human response and performance	31. Measuring and logging human responses in executing tasks, e.g., by a time-limited execution of a task or a scenario 32. Measuring and logging human responses in discovering errors, e.g., by a time-limited execution of a test 33. Recording average error frequencies and operator response times for critical procedural steps to validate historical data (or provide data for risk analysis, if historical data is not available) 34. Measuring qualitative aspects of human performance based on fulfilled criteria, e.g., response time, number of successful checks, frequency of constraints' violations, number of unnecessary actions, etc.
	Functions for error recovery	Error management	35. Visualising and testing error consequences by safety managers or risk analysts 36. Providing a monitoring interface for safety managers to "manipulate" virtual errors and ask operators to correct them 37. Trying several safety barriers to minimise the impact of human error (machines' layout, safety procedure changes, workflow changes, etc.) 38. Examining dependencies between human behaviour and use of barriers (e.g., barriers are not used properly or not used at all)
		Error correction	39. Setting up the surrounding conditions to allow for error correction (undo effect for assembly operations) 40. Displaying proper warning notes (alarms) before executing critical task steps 41. Allowing/restricting facilities for backtracking to previous steps in the scenario 42. Mark plant information that was not consulted by the operator in error which could have assisted in the detection process. 43. Insert icons of information on specific equipment that could have prevented an error if an actual instrument had been installed earlier in the plant 44. Explore whether an operator can UNDO

			an action and return to the previous system state or, at least, to another state that is temporarily safe. 45. Explore how operators could delay the propagation of an effect that cannot be undone. 46. Explore how operators could moderate/attenuate the adverse effects of an erroneous action
Modelling Work Context	*Functions for representing work constraints*	Manipulation of information and work constraints	47. Providing unavailable information (e.g., invisible gauge, hidden indicators, etc.) or non-measurable information (e.g., friction, gravity, wind speed, etc.) 48. Experimenting with additional information that is usually not available at work in order to evaluate the extent to which human errors could be prevented or recovered on time 49. Simulating several constraints at the workplace and their impact on human response and performance (e.g., lack of tools, lack of procedures, difficult access to equipment, etc) 50. Presenting operational procedures and checklists and linking them to the VR environment
		Manipulation of ambient conditions	51. Providing audio effects to simulate real operational environment (e.g., noise, alarm, communication disturbance) 52. Manipulating weather conditions (such as smoke, smells of ordure, rain, wind, snow, hot/cold weather, etc) 53. Simulating operation and response under extreme conditions (e.g., fire, explosion, gas dispersion, etc.)
		Manipulation of team composition and interaction	54. Displaying parameters together that cannot be observed at work from the same position in order to increase the "Field Of View" of team members and allow them to oversee others. 55. Automating or speeding-up certain tasks so that the team members devote attention how to organise tasks rather than how to perform tasks. 56. Showing panoramic views of the scenario, e.g., the layout of safety equipment, the distribution of persons to the plant site, the location of the rescue teams etc. 57. Monitoring task progress by means of an overview of tasks that have been accomplished, interrupted or assigned to other colleagues.

4.7 Mapping VR functional requirements to technical feature groups

In Section 4.6 a set of 57 functional VR requirements (functionalities) has been identified. They were classified into eleven groups of functional features (third column in Table **4.2**). To propose a VR environment design that supports these functionalities (Chapter 5), it is necessary to map them to abstract groups of technical features to extract the technical capabilities of the VR environment based on these abstract features. Fig. **4.3** illustrates this intermediate stage (dark coloured box with bold text inside it) as part of the integrated method developed in this thesis.

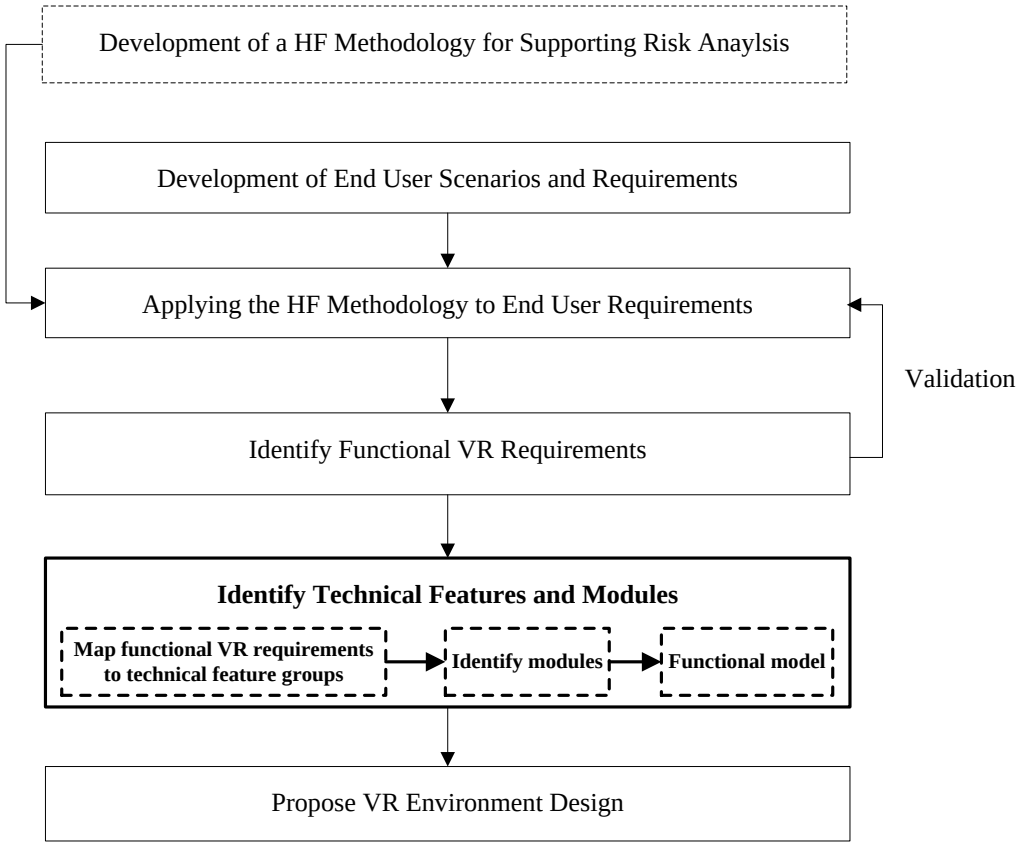


Fig. 4.3: The steps (dark boxes) of Identifying technical features and modules within the integrated method (Fig. **1.2**)

Table **4.3** provides an overview of the technical feature groups and the modules of the proposed VR design. In the first column, the eleven groups of functional features obtained from the previous step (Section 4.6, third column of Table **4.2**) have been listed. In the second column, these functional features have been mapped to the groups of technical features. The groups of technical feature represent a translation of functional descriptions into technical ones to facilitate assigning the VR component (third column) to the functional feature groups. The third column lists the part (module) of the proposed VR design that targets these groups.

Section 4.8 describes the functional model that links the modules of the proposed VR design and the information flow among these modules. Chapter 5 provides descriptions of the modules together with the technical features supported by each module.

Table 4.3: Groups of technical features and VR support

Functional feature group (third column in Table 4.2) (WHAT)	**Technical feature group** (HOW)	**Module of the proposed VR design** (WHICH tool)
Prediction of how the plant responds to disturbances and the impact of multiple events	Enrichment of the VR environment with simulations, i.e., dynamic simulations on plant and process behaviour, process and control room simulators, etc.	Process Dynamics Module
Manipulation of team composition and interaction	Considering of team work in the VR environment, i.e., collaborative environments	Core-Client Architecture
Familiarisation with plant layout and equipment design Identification and prevention of hazards by means of barriers (plant hazards, site hazards, human hazards, etc.)	Supporting 3D visualisation, i.e., navigation, interaction, manipulating objects and their attributes (pressure, temperature, valve status, etc.), etc.	Core-Client Architecture (runtime phase) Authoring Module
Recording of human response and performance Error management Error correction Identification of error consequences Error identification and detection / Examination of task variations/ error shaping factors	Awareness of HF in the VR environment, i.e., representation of tasks, supporting human error detection, error recovery, error modes, etc.	Event Based Module Logging Module Analysis Module
Manipulation of ambient conditions	Supporting environmental conditions, i.e., day/night conditions, weather conditions, etc.	Authoring Module Core-Client Architecture
Manipulation of information and work constraints	Supporting work context, i.e., sound, noise, communication, etc.	Authoring Module Core-Client Architecture

4.8 The functional model

Before concluding this chapter, an illustration of the functional model that links the aforementioned technical components and modules should be provided. This model aims at introducing the functional information flow upon using the listed VR components and modules (Table **4.3**) to run a scenario or an experiment.

The functional model is explained based on the following typical problem[13] from the target industry:

Problem:

- For a particular operational task, the safety analyst (or risk assessor) needs data and information on human behaviour (e.g., under different weather conditions, in case of fire, etc.), response times (e.g., in case of gas leakage detection), time to complete a certain task or part of it, error causes, error modes, error recovery (undo), etc. for completing the risk analysis work.

- The required data and information usually do not exist (e.g., because similar situations did not happen in the past, available data were obtained before process and operation modifications, new staff with specialised qualifications have been hired, changes in work conditions).

Solution:

The safety analyst uses the VR environment to obtain the required information.

Information flow:

- The safety analyst prepares (or adapts it, if a similar one exists) the scenario - e.g., gas leakage scenario, fire fighting scenario, pipe maintenance scenario, etc. - that corresponds to the information he is looking for with all its initial conditions (weather, barriers, escalation of situation, etc.). This step is achieved using the authoring module.

- A safety analyst asks operators to run the VR scenario and perform the assigned task(s) as they normally do in reality. While running the scenario (experimenting), the main VR application communicates with the process dynamics module and event based module to get experiment relevant data.

- Operators' actions and reactions during the virtual experiment are logged into log-files. This step is achieved via the logging module.

- Operators complete running the scenario and stop when finishing.

[13] The formulation of other problems or imaginary scenarios is possible and should lead to the same result, i.e., to illustrate the links among the components of the VR environment and the information flow.

- Once the data is logged, safety analyst can start analysing the data and storing the results into a database for accessing and querying it. This step is achieved via the analysis module.

The functional model is illustrated in Fig. **4.4**. An explanation of the components of this model is provided in Chapter 5.

4.9 Summary

This chapter introduced the functional requirements for supporting the performance of risk analysis in a VR environment. The definition of these requirements took into consideration a set of end user needs that have been derived during field work on industrial sites, interviews and workshops with safety experts from the chemical process industry. The HF methodology, which was developed in Chapter 3, was also applied here to make sure that the HF dimension is also well covered within these functional requirements. Chapter 5 moulds these functional requirements and specifications into a VR environment design.

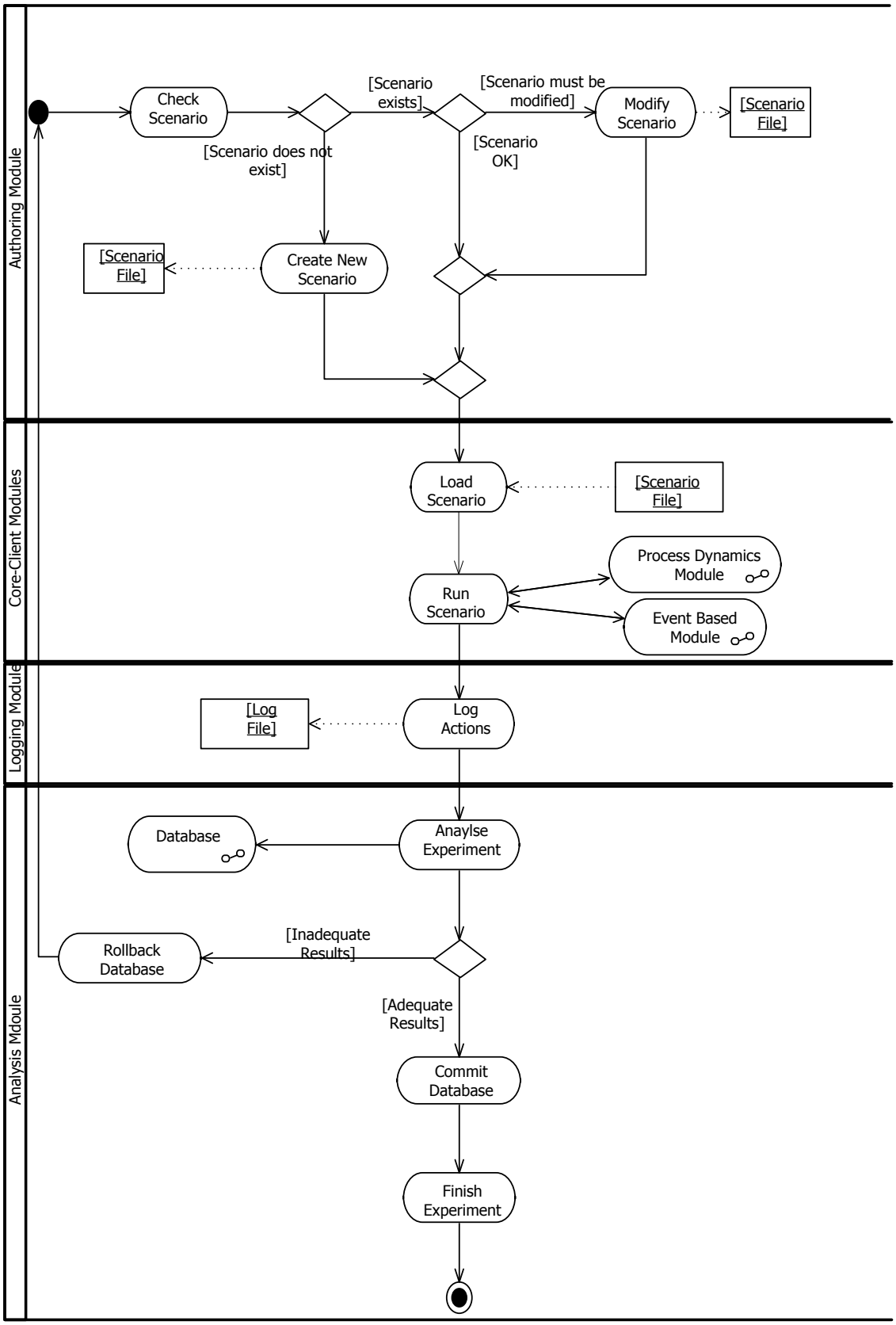


Fig. 4.4: Functional model that links the VR components and modules

5
VR environment design

It has been mentioned in Chapter 1 that in the underlying thesis, VR is considered as a bridge (representation medium) for bringing together the three key components that influence safety within the framework of this thesis: industrial needs (end user needs), risk analysis and human factors. This perception of VR contributes to enhancing its usability as an enabling technology for solving problems with high industrial and social impacts. This usability has been moulded into set of functional requirements and specifications as retrieved from field observations, i.e., application-oriented and end-user driven (Chapter 4) mapped to a HF methodology for improving risk analysis (Chapter 3).

These findings are used in this chapter to propose a VR environment design for supporting risk analysis work. Since the proposed VR environment design resembles standard VR systems in its core functionalities, it is not considered as unique from this point of view. However, it offers uniqueness from another perspective, which is the end user- and application-oriented nature, i.e., it focuses on the needs of the target industry (chemical process industry) and the challenges faced by the end users employed within these industries. This aspect has been achieved by integrating specific modules in the proposed design which is necessary to compensate for one of the major limitations in VR tools and applications, i.e., their usability and ability to solve end user problems as discussed in Chapter 2.

5.1 Architecture of the VR environment

The proposed architecture is based on the typical rendering process (pipeline) which consists of the three steps "application, cull & draw[14]" for scene generation (cf. Martz 2007, pp. 16 et seq.). The steps are normally put in a continuous iterative cycle, which produces a rendered image (one frame) per iteration. Furthermore, the proposed architecture has been designed to be:

- *Scalable* and ready for future evolution which is necessary as the complexity of applications might increase and new features are needed to cope with this complexity.

[14] APPlication: updating the scene (geometries, location and orientation), CULL: determines which geometries in the scene are visible, DRAW: rendering all visible geometries.

- *Modular* by having design modules that are separate and independent from the core system to allow a more effective implementation and a better performance upon running the application since necessary modules are only loaded.

The VR environment design is based on two building units as shown in Fig. **5.1** (Salem 2008; Loupos et al. 2008a; Loupos et al. 2008b):

1. The main VR application: provides the visualisation and interactivity features (i.e., the rendering process "application, cull and draw"). The main VR application is decomposed into:

    - Core system: the core part of the system, which processes all the requests that have an impact on the scene graph, i.e., in charge of the "application" step in the typical rendering process;

    - Client system: the part in charge of preparing the scene and actually drawing it, to produce the output frame, i.e., responsible for the "cull" and "draw" steps in the typical rendering process.

2. External Modules: necessary to support creating, modifying and running a scenario with all its specifications and surrounding elements. These modules are necessary to cover all functions that belong to a scenario which are outside the rendering process "application, cull and draw". These modules are introduced later in this chapter and are: authoring module, process dynamics module, event based module, logging module and analysis module.

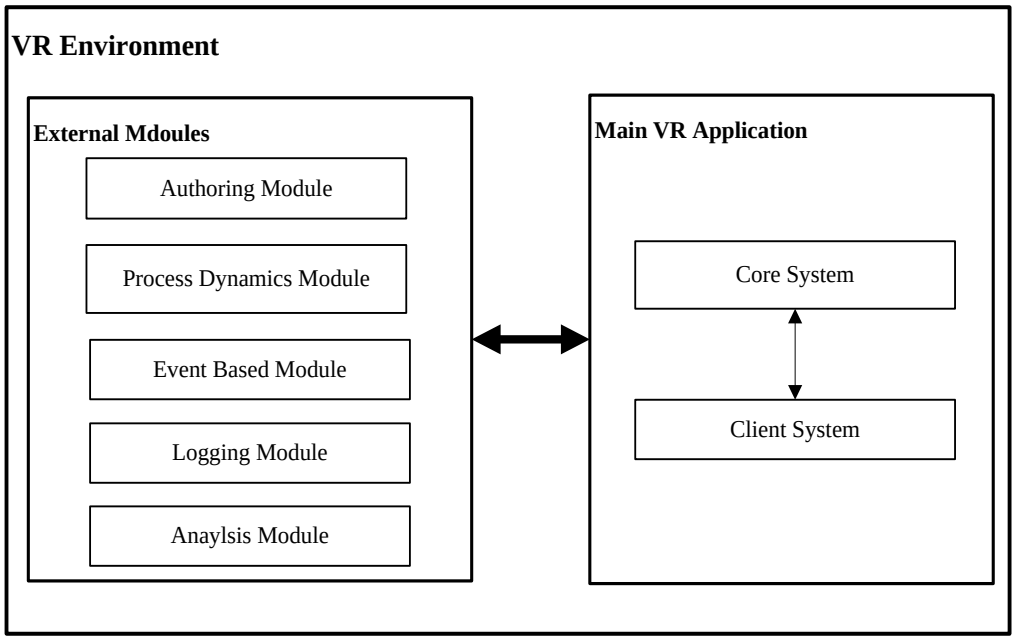


Fig. 5.1: Architecture of the proposed VR environment

The proposed architecture utilises the plug-in architecture pattern, i.e., external modules can be developed and maintained without expanding the main VR application to cover evolving requirements (Mayer et al. 2003). Furthermore, the external modules can be installed as individual components or an entire set of components depending on the intended use of the system without influencing the installation of the main VR application.

Compared to standard VR systems which typically consist of the core-client components, a content creation interface (authoring) and an information-logging component, the underlying architecture provides customised modules for supporting the predefined functionalities and features. These customised modules are the process dynamics module, the event based module and the analysis module. Descriptions of these modules, their supported functions and features and links to other modules are provided later in this chapter.

The authoring and logging modules proposed here provide similar functionalities to those supported by standard VR systems. However the logging module is presented here as a component that records all interactions for further analysis (e.g., in the analysis module) and replaying the scenario which is not the case in many VR systems, as they only record user input and system alerts in a log-file for error tracking or debugging.

It is worth mentioning that the proposed system architecture provides high level design guidelines and descriptions of the required components to ensure a consideration of the predefined functional requirements. Implementing this architecture requires further technical details which are not provided here as they do not belong to the goals of the underlying thesis.

5.2 Core system

The core system is a program which is in charge of handling the greatest part of the "*application"* step in the rendering process. It takes care of updating objects' positions and states, it processes user actions and input from external devices (tracking devices, mouse, joystick, keyboard, etc.) and it keeps all the state attributes up to date. The core system does not invoke any image rendering; it has a main cycle in which each iteration processes all the received input and updates the scene, but it does not produce an output frame. It has a copy of the scene graph in memory; this is needed to update positions, compute interactions and prepare for next steps. Since the core system does not draw an

image, the actual geometry (triangles) and the material information are not used inside it. This information is used in the client system, which is in charge of the *"cull and draw"* steps.

The core system processes all the requests that have an impact on the scene graph: tracking devices, collision detection, interactions that may impact how an object is displayed, etc. and communicates to the client system all the modifications that occur to the scene graph.

The core system is composed of "state module", "task module" and "log module" which are in charge of handling specific parts of the scene update step as shown in the next subsections.

5.2.1 State Module

The state module is the central module in the core system which is responsible for the administration of the entire scenario and keeping all scene information up to date. The whole core system behaves like a state machine in which the "state module" manages the state attributes of this machine. The following is a list of functionalities assigned to the state module:

- It reads/modifies state attributes[15].
- It controls when a state changes and reacts accordingly, e.g., to detect when a given object has to move (due to some user action like pushing a button or moving a piece of equipment). To achieve that, it constantly queries model components to know when they need to change state (based on their predefined behaviour).
- It controls and modifies the local copy of the scene graph based on actions and events to be executed. It also computes collision detection (used also by the actor module as described later).
- It communicates to the scene module of the client system all the changes in the state that affect the scene.
- It accesses model and state data (attributes) of each component by communicating with the modules in charge of delivering and maintaining these data, i.e., the

[15] State attributes are attributes that describe the current state of an object, e.g., valve status (open/close), pipe temperature (high/middle/low), gas pressure (high/middle/low), etc.

component library as provider of model data and the external modules (e.g., process dynamics module, event based module) as providers of state data.

5.2.2 Task Module

This component is in charge of monitoring the execution of a task - in cooperation with the event based module - which requires the ability to detect when a given action occurs. To illustrate the concept of task module, the following instruction "place gas detector over the valve", which is part of the task "gas leakage detection" can be taken as an example. The task module checks that a given user is executing the "gas leakage detection" task and it knows that the next step should be "place gas detector over the valve". Based on that, the task module constantly monitors the objects involved in this instruction, namely the "gas detector" and the "valve".

At some point, the user will move the "gas detector" and put it over[16] the "valve" which is detected by the task module as the time point for casting a message that confirms the correctness of performing this step. In a similar manner, the task module has the key role of applying the logic behind each task step for the entire scenario in order to understand and confirm when a given action occurs. The task module embeds a task tracker that assists in monitoring the completion of a task by the proposed actor and logging relevant task information to the log module, e.g., duration of task steps, user interactions during running the task, response times, etc.

5.2.3 Log Module

The log module is in charge of processing all requests from the various modules to log information. The log module receives from the components of the core system requests for logging information and routes them to the recorder of the external logging module (Section 5.4.4) to record or skip the logging request.

A typical log request from the core system consists of asking the system to write all the state changes for the plant elements – caused either by an actor or by some internal action – so to analyse them later.

[16] Since the term "over" would be confusing, it can be imagined that when the vertical axis of the "gas detector" is aligned with the vertical axis of the "valve" with a pre-defined minimum vertical translation, the system accepts that as "being over".

Fig. **5.2** shows the architecture[17] of the core system. The elements "External Modules", "Component Library" and "Task File" are not components of the core system, but provide input to its components. These elements are explained in the upcoming sections.

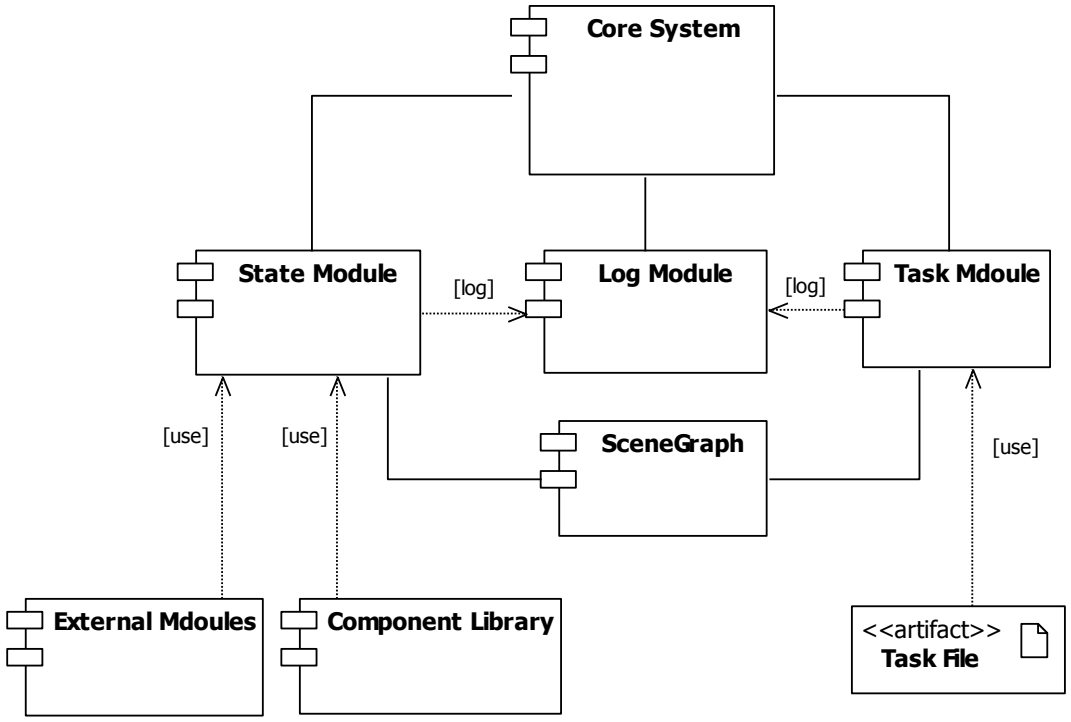


Fig. 5.2: Architecture (component diagram) of the core system

5.3 Client system

The client system is the part in charge of handling the "*cull"* and "*draw"* steps of the rendering pipeline. It has a main cycle which produces one rendered image (one frame) per iteration.

The client system is in charge of preparing the scene and drawing it to produce the output frame. It has a copy of the scene graph in memory, which is synchronised with the main one managed by the core system via updates received from the core system itself. The client system receives updates from the core system concerning modifications to the scene graph, it processes them and stores them to the local copy of the scene graph and proceeds to drawing the frame. Therefore, before drawing a frame it

[17] The architecture diagrams introduced in this Chapter have been produced using the tool StarUML version 5.0.2. This tool is based on UML 1.5 and accepts UML 2.0 notation. [StarUML 2009]

applies all the changes sent by the core system which is necessary to complete the "application" step mentioned above. The "cull" and "draw" steps are handled completely in the client system. The client system is also in charge of producing output other than the images, e.g., sound, noise, tactile feedback based on input from sensory devices, etc.

It should be mentioned here that it is possible to have more than one client system running on different machines (e.g., for multi-display systems). The simplest hardware configuration would be to have the core and client systems running on the same machine.

5.3.1 Scene Module

The scene module is in charge of updating all the data so that a scene can be drawn, which includes updating positions, materials, textures, environment, etc. based on the input received from the state module. The scene module updates the scene objects by accessing the model data stored in the component library. This module is also in charge of audio rendering, i.e., reproducing the needed sounds according to the current conditions.

5.3.2 Actor Module

The actor module controls and updates all the information related to the actor[18] while running a scenario. This information ranges from the user profile, user roles up to his/her visual representation (position, orientation, collision, etc.). In particular, the actor module is in charge of:

- Managing interaction devices connected to the actor (for example a tracker placed on a user's hand) and accordingly updating the actor position.
- Checking if the actor (or a part of it) is colliding with any object in the scene. The actor module facilitates differentiating between colliding directly with a plant element and collision that is mediated for example by a tool, i.e., placing a screw driver on a bolt or similar.

[18] An actor is a player who can act (perform operations) in the VR environment. An actor can be a real user interacting with the VR environment via tracking devices or a fully virtual character.

- Notifying the core system (and in particular the state module) when actions occur, using the proper messages.

- Driving the system through the execution of a given task (which consists in a series of operations that have to be performed on the plant). For example it can raise alerts when an actor does not perform correctly a task. For this purpose, the actor module works in cooperation with the task module which was presented in Section 5.2.2.

It is worth mentioning that since actors are handled independently from each other by the actor module, the task module is responsible for managing situations where more than one actor are interacting with the scene.

5.3.3 Log Module

The log module here has a similar function to the one of the core system, i.e., processes all requests from the various modules to log information. The log module receives from the components of the client system requests for logging information and routes them to the recorder of the external logging module (Section 5.4.4) to record or skip the logging request.

A typical log request from the client system would be asking the system to write the current user position and time value to disk, so that a reconstruction of the path walked by the user is possible. Another request would be to log the time that elapses between receiving an alarm signal and taking the proper action, which can be further used for extracting response time.

5.3.4 Component library

The component library is a building block that can be used or accessed by either the core or the client system and considered as a shared or common module. It is a library of components which lists all the elements that can be used to create a full plant model. Each component in the library is linked to a component model that provides the following information about the component itself:

- Properties to describe the geometry and the link to piping and instrumentation diagram;

- A series of specific attributes and all their possible values (called “states”). For example a “switch” object has a “Status” attribute which can have two states only:

ON or OFF. A “valve” can have an “Open” attribute which is a continuous set of values between 0 and 1 or represented as a discrete set of five possible values (for example): 0% (closed), 25%, 50%, 75% and 100% (fully open);

- The rules which determine the behaviour of the component, e.g., Valve “Xvlave” can only rotate around its Y axis. When asked to do so, a component can update its information based on its behaviour.

The information about the plant model and the components listed in the component library are mainly accessed by the state and scene modules. The accessed information is designated as “model data” and normally stored in a specific file format that can be interpreted by other modules (e.g., authoring module to modify a scenario). In this context, “model data” is the complete information needed to describe a plant model and its properties including environmental data, e.g., lightening conditions, weather effects (snow, rain, wind, etc), noise.

Fig. **5.3** shows the architecture of the client system. The element “Actor Input” refers to user’s interactions while running a scenario as explained in Section 5.3.2 (actor module).

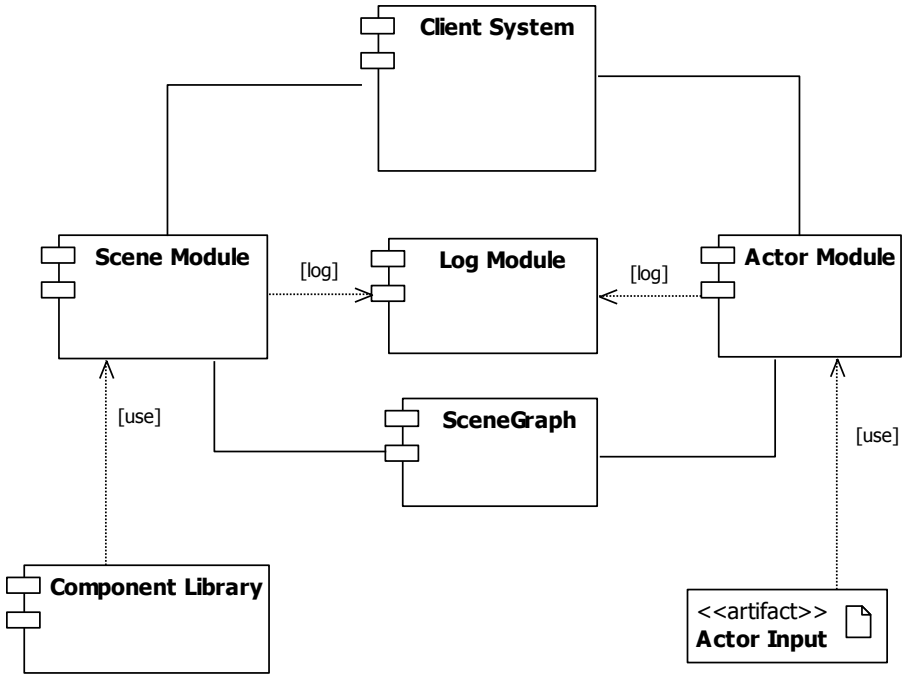


Fig. 5.3: Architecture (component diagram) of the client system

Fig. **5.4** illustrates the links among core system, client system and the external modules (external modules are explained in the next section).

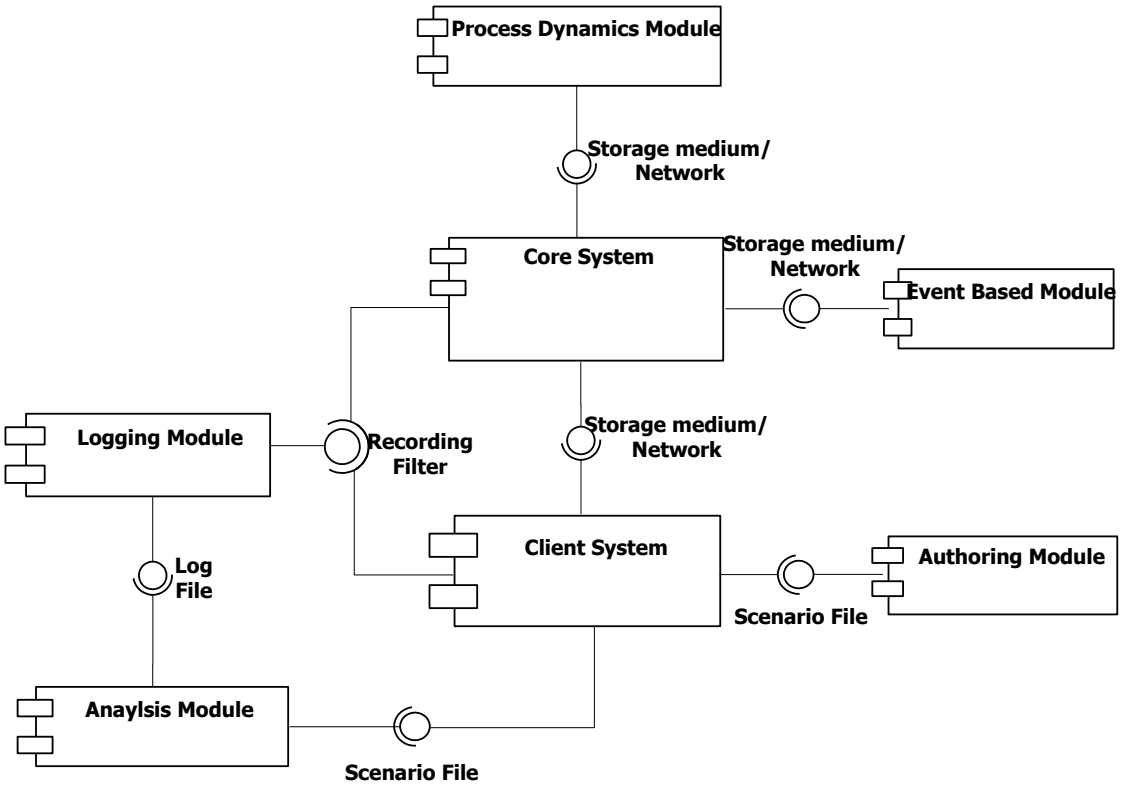


Fig. 5.4: The core and client systems and their links to the external modules

5.4 External modules

External modules are important elements that provide functions[19] that do not belong to those covered by the core and client systems. These elements can run on separate machines and communicate with the core and client system using a network protocol. This modular structure which can be extended over time represents one of the major features of the proposed VR environment design.

Some functions that are covered by external modules (based on the functional requirements provided in Chapter 4) include:

- Authoring and configuration functions for scenario preparation and configuration (Authoring Module);
- Linking the VR environment process simulator to ensure a reflection of process dynamics within the VR scenarios (Process Dynamics Module);

[19] These functions can be described as non-visualisation functions which are not covered by the core-client components.

- Monitoring the execution of procedures and rules of plant-specific behaviour (Event Based Module);
- Logging (recording) events and messages for replaying scenarios or post-analysis (Logging Module);
- A module for analysing the logged results and extracting the data that can be used by HF and safety experts (Analysis Module).

The next sections provide more descriptions on these modules supported by architectural diagrams of each module.

5.4.1 Authoring module

The goal of the authoring and configuration module is to provide an environment for creating and modifying the VR scenarios by target users. The authoring and configuration module enables performing two main functions:

- Configure the 3D content of the virtual environment, i.e., plant components, objects, geometries, materials, textures, etc. (visual appearance).
- Configure the content of the scenarios that are running in the VR system, i.e., scenario steps, initial conditions, parameters, properties, etc. (scenario content).

The authoring module is mainly used by the persons who are responsible of creating and editing scenarios and not by those who run these scenarios. The term "scenario authors" could be used here to indicate the group of person who create and edit scenarios. It should be emphasised here that scenario authors are not computer specialists or programmers. The authors of a scenario could be also users of the scenarios. A scenario author in the target industry, i.e., chemical process industry, could be:

- Safety manager who is about to improve the safety plan of the plant.
- Trainer who is about to design a new training course on a certain procedure and then develop this scenario using the authoring module.
- An experienced technician, who knows the details of the machine and how it can be operated, disassembled or maintained.

- An accident investigator who is about to build the collected field data inside the VR environment and produce an “accident investigation scenario”.

- A safety analyst, process engineer, etc.

Preparing data and scenario authoring involves several aspects:

- Handling 3D geometry and the related materials or textures;

- Setting initial values and conditions for all the parameters that affect the scenario once it runs.

The result from the authoring module is a scene file which can be directly loaded by the client system and viewed. This scene file is enriched with specific procedures that are executed in a VR experiment (i.e., a maintenance procedure, an operational procedure for doing a certain job, etc.), environmental conditions and other components which comprise together a safety scenario.

Fig. **5.5** provides the architectural layout of the authoring module which consists of the following layers:

- View Editor: for displaying the plant items and components as individual 3D models for further processing. This enables manipulating these objects, i.e., translation, scaling and rotating them in the viewport. The camera can be moved through the plant using the viewport, to get the optimal viewpoint and save it as a favourite viewpoint.

- Model Editor: for importing, editing and deleting model libraries. The hierarchy of the scene's objects can be also created or updated in this layer.

- Property Editor: for setting, modifying and displaying the properties assigned to each component of the scene. The properties need to be set and changed to correspond to the desired state and appearance of the plant components under certain conditions, i.e., increased temperature, opened valve, a switched-on pump, etc.

An additional element that can support authoring functions is the “P&ID Wizard[20]”. It supports translating the P&ID diagrams into a 3D representation which can be further used in the authoring module.

[20] The “P&ID Wizard” is an optional external component and will not be further introduced due to lack of information and APIs on translating P&ID into 3D modelling data. A recommendation for future work on P&ID is provided under “future work” in Chapter 7.

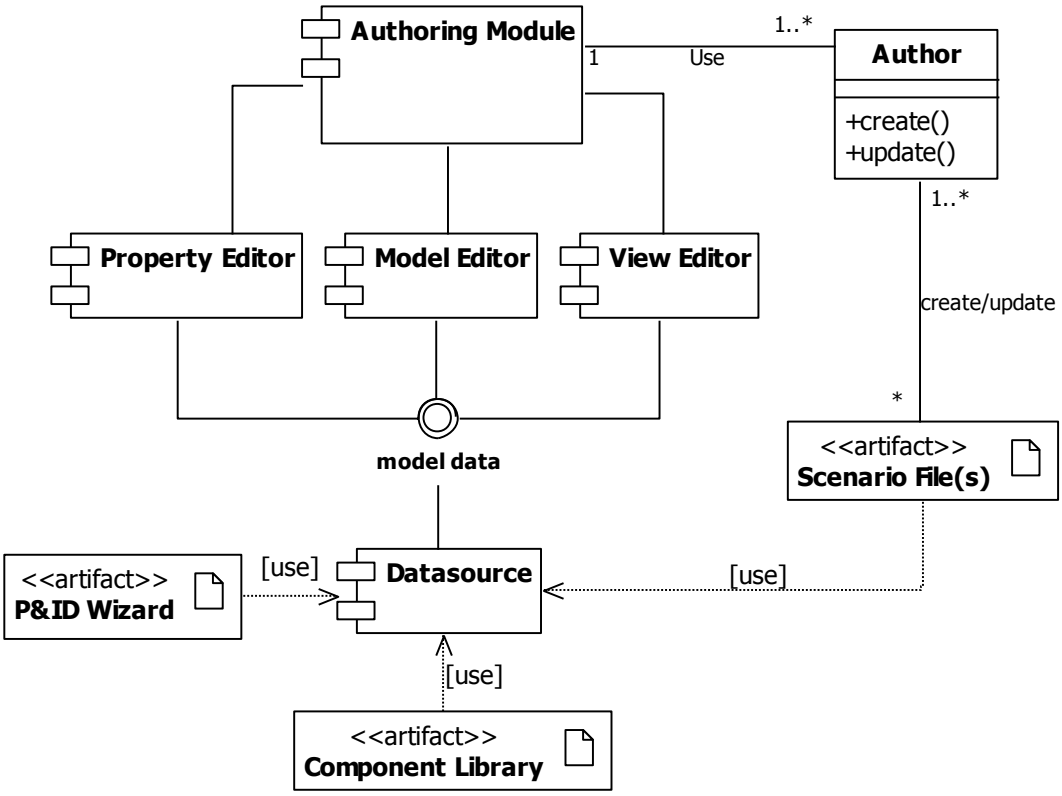


Fig. 5.5: Architecture (component diagram) of the authoring module

5.4.2 Event based module

The goal of this module[21] is to respond in predefined ways when certain conditions occur. To perform this function, the event based module has to manage two sets of internal data:

1. A set of attributes that represents the parameters to monitor, e.g., valve widely open, high increase in temperature inside pipes, sudden drop of pressure, etc.

2. A set of predefined rules that defines the system response when a specific state change occurs, i.e., when the attributes take on a specific set of values. An example rule would be "if the valve is more than 80% open (widely open), send an alarming signal".

[21] The terms "rule based module" and "expert system module" are also used in the literature to refer to these systems.

When something changes, the event based module checks if a rule applies for the new state and reacts accordingly. This module can be used for four main purposes:

- To add visual effects to the virtual environment according to what is happening. For example, when the temperature in a given pipe reaches a certain value and if in that pipe a flammable gas is flowing, the event based module reacts by directing the state module to put a fire in that specific position.

- To apply a plant-specific behaviour, which is not part of CAD or P&ID models. For example a given process line may be designed so that a single button activates two pumps and opens a valve. The event based module manages such cases, i.e., when that button is pressed, a specific rule is activated and the produced event triggers two pumps on and opens the valve.

- To help monitoring execution of tasks and procedures. The task module (see Section 5.2.2) is driving this monitoring activity, but it relies on the event based module to detect if and when a given step of the task has been executed. For example, it may be required that a pump is turned on before a particular valve is opened. If the valve is open whilst the pump is still off, a warning message is sent.

- As a replacement for the external process simulator. When an actor performs a given operation (i.e. activating a pump), instead of always invoking the simulator, this module can react in predefined ways. This feature can be utilised in situations where no process simulator is available or no link between the VR system and the available process simulator can be produced.

The input to this module is in a simple and abstract form, a syntax that can be used to quickly specify system behaviour that can be read and understood by people who are not familiar with programming.

Fig. **5.6** provides the architectural layout of the event based module which consists of two main components:

- Message translator: grasps ongoing messages from the state module of core system, translates them into facts that can be processed by the rules shell. The message translator receives also messages from the rules shell regarding actions which are forwarded to the state module again to update scene stat (outgoing messages).

- Rules shell: processes input files which consist of list of *facts* and *rules*. These input files monitor the execution of procedures and rules on plant-specific behaviour.

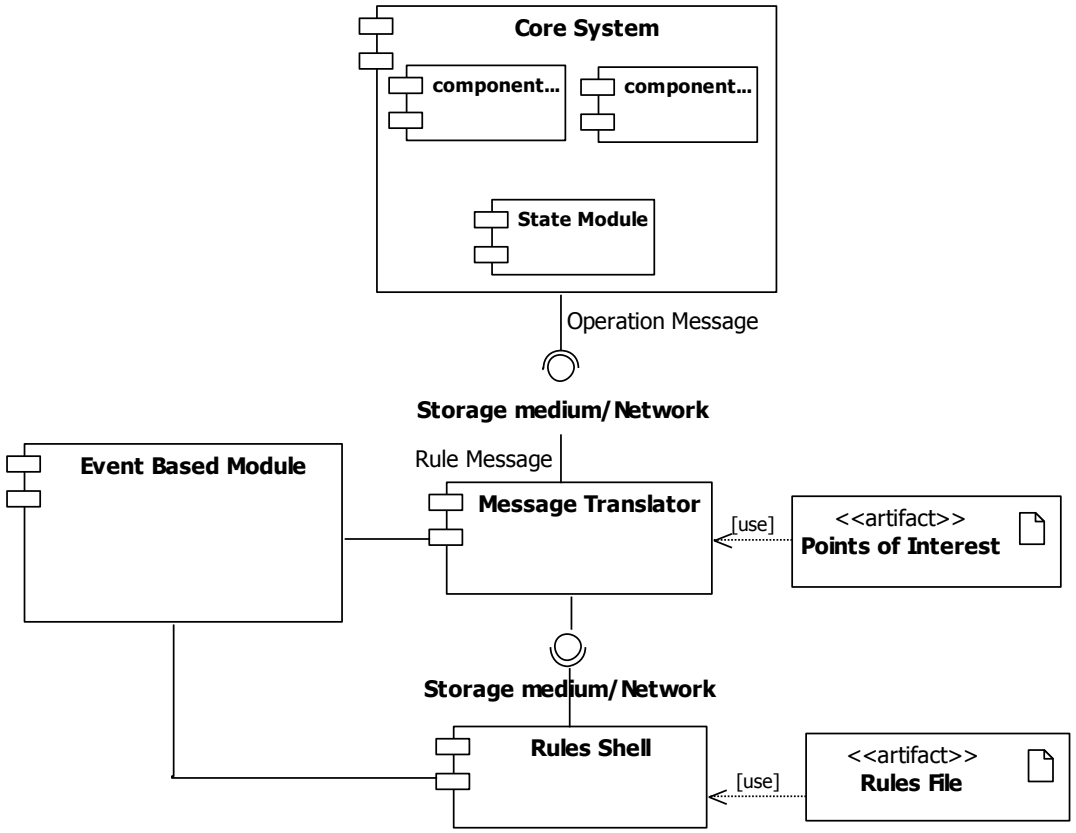


Fig. 5.6: Architecture (component diagram) of the event based module

Since a VR scenario file involves hundreds of objects (plant elements) - where each of them has its own variables and properties that can be monitored during a VR experiment - the core system can receive and dispatch a high number of messages on scene objects. Processing all these messages by the event based module affects its performance and response which is reflected into delayed update of object states or actions.

To reduce this effect and since the user (safety analyst, technician, operator, trainer, etc.) is interested in monitoring a few objects and properties, certain "points of interest" are inserted in the scenario file. These "points of interest" represent indications on the objects and properties that should be reported to the event based module, i.e., only messages concerning these objects are forwarded to the event based module. A "point of interest" can be seen technically as a class that consists of a few basic members:

- object name;
- property name;
- current property value, used to store the last know value for that property;

- tolerance, used as threshold to detect when the value has changed.

When the scenario is loaded, the message translator reads the list of "points of interest" and starts listening to messages from the core system about those objects and properties only.

5.4.3 Process dynamics module

The process dynamics module provides the link between the VR system and an external process simulation[22] engine, thus providing realistic, dynamic plant and process behaviour to VR scenarios. The link between this module and the actual process simulator depends on which specific simulator is chosen. The process dynamics module is linked to the state module of the core system and processes messages to and from the external process simulator, e.g., Dynsim™ (INVENSYS 2008), D-SPICE® (Kongsberg (2008)), etc.

In the proposed process dynamics module it is assumed that the external process simulator adheres to the OPC (Object-linking and embedding for Process Control) standard. OPC is "a series of industry standards specifying a standard set of objects, interfaces and methods for use in process control and manufacturing automation applications to facilitate interoperability" (Wikipedia (2008b)). The purpose of OPC is to define a common interface that is written once and then reused by any business or customised software package. OPC was originally based on Microsoft's OLE COM (component object model) and DCOM (distributed component object model) technologies. (OPC Foundation (2008))

OPC based process simulators provide an OPC server, also called an OPC Gateway engine, which allows the exchange of data between the process simulator and the external application, which is called OPC client. Providing an OPC based module ensures the compatibility with industrial standards, being independent from particular commercial software and provides design flexibility by replacing the bottom box (process simulator) in Fig. **5.7** without the necessity of making radical modifications in the OPC client.

Fig. **5.7** illustrates the architectural layout of the process dynamics module which consists of two main components:

[22] A dynamic process simulator is a program that enables engineers and designers to test the dynamics of designing and operating a process plant in a safe manner based on a dynamic copy of the real plant.

- OPC client: the interface that passes messages between the state module of the core system and the process simulator. An example message that would arrive from the state module would be to request the current value of tank X from the process simulator. Once received from the OPC server, the value is forwarded to the state module to update the scene accordingly.

- Process simulator: commercial software that simulates the process dynamics and is interfaced to external applications using its OPC server.

The OPC client initiates communications with the OPC server which reads a properties file that specifies which item properties (called "points" in OPC terminology) in the process simulation should be exposed to the outside world. Only these points may be read or written by external applications through the OPC server. The points are read from the OPC server and added to a list maintained by OPC client who passes messages of particular types to and from the state module, e.g., get value, set value, stop reporting, resume reporting, etc.

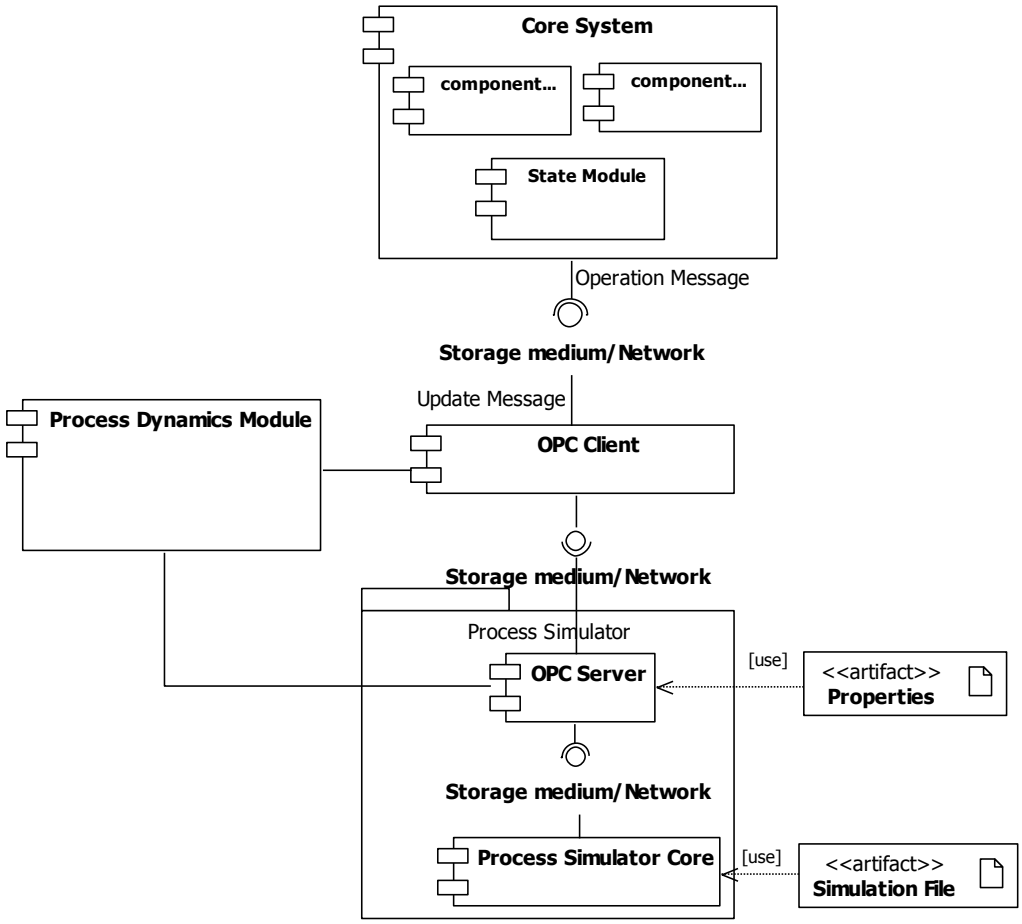


Fig. 5.7: Architecture (component diagram) of the process dynamics module

5.4.4 Logging module

The logging module logs all the activities occurring while running a VR scenario. Actions and updates that are logged range from change to objects' properties (e.g. changing the open value of a valve, change pump status to “off”, etc.) up to changes in user’s position, time to respond, completion of tasks, etc. The goals of such a logging module are:

- Using the logged data to playback a particular simulation at a later stage. This helps reviewing procedures, discovering errors and putting necessary plans to avoid them in reality, monitoring bottle-nicks, etc.

- Recording information on events, actions, operations, etc. which can be used as source for extracting HF-relevant data (error modes, error causes, etc.).

The output produced by the logging module (Fig. **5.8**) is a file that contains all the relevant information to reproduce the entire simulation or extract necessary information. This file represents an important input for the analysis module which uses this file as basis for extracting and populating particular information, i.e., time to perform an action, time to take a decision, path followed to reach a leakage point, etc.

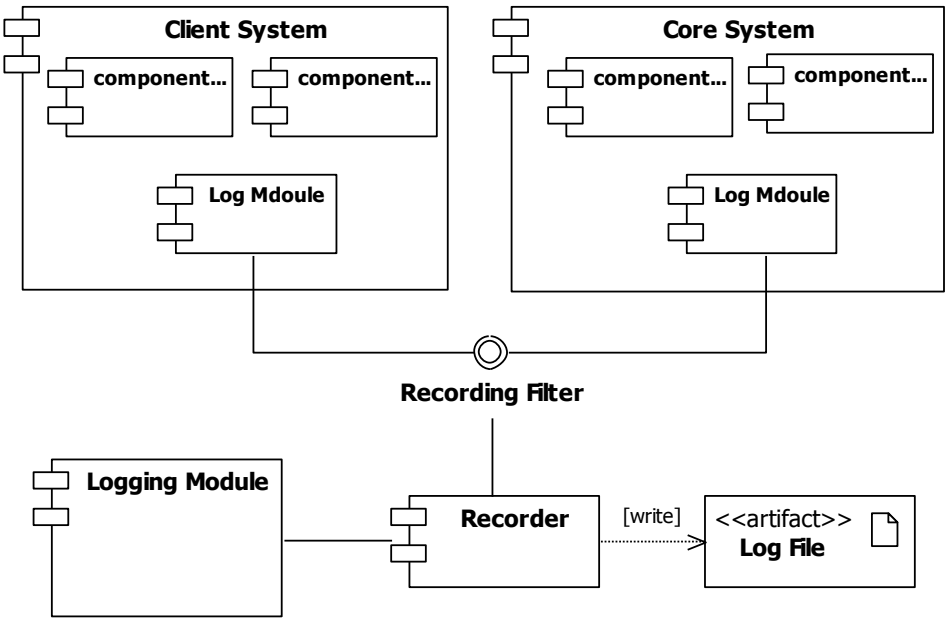


Fig. 5.8: Architecture (component diagram) of the logging module

To make sure that the user, i.e., operator, trainee, technician, etc. is aware of logging his actions and reactions, a recording button (recorder) should be activated so that the logging process can run as illustrated in Fig. **5.8**. If the recording is disabled, an empty

log file is produced. A recording filter is used to specify the information that should be logged and avoid producing huge log files.

5.4.5 Analysis module

This module is in charge of extracting necessary data from the log files (logging module), storing it in a structured form that allows using it by HF or safety experts for analysis purposes and querying the stored information when needed.

The analysis module is responsible for the following operations:

- Data processing: for processing the log files together with the initial condition file – which are produced upon creating and running a VR scenario – and extracting the information to be stored in the database, i.e., the data and information that are needed by the risk and safety analyst;
- Data storing: for storing the extracted information in a database so that it can be queried when needed;
- Data querying: for interfacing with the database and querying the stored data.

Fig. **5.9** illustrates the architecture of the analysis module. A description of the operations covered by the components of the analysis module is provided as next.

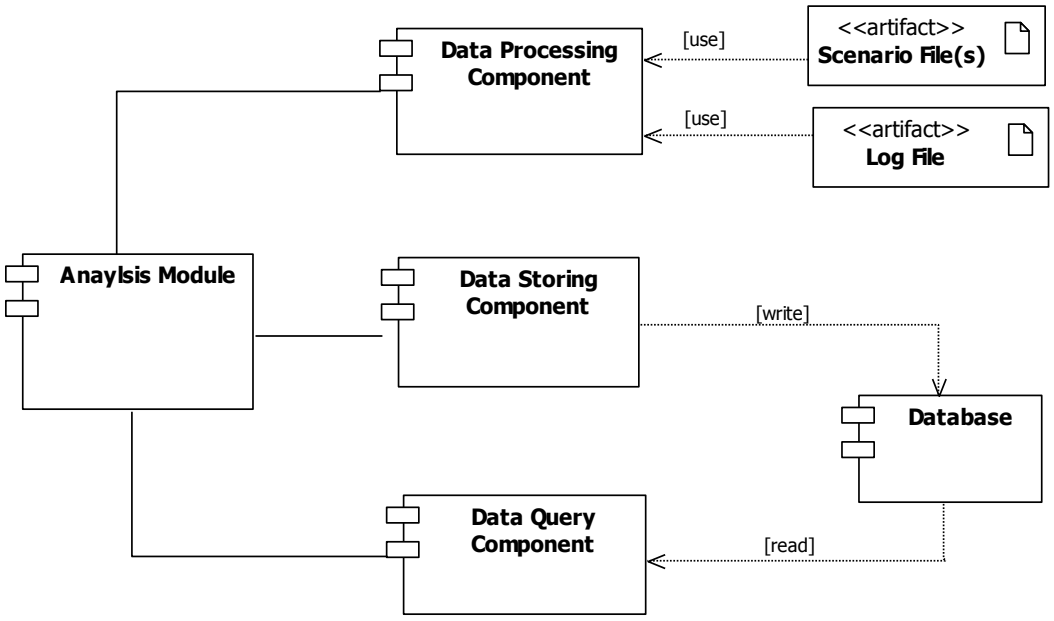


Fig. 5.9: Architecture (component diagram) of the analysis module

5.4.5.1 Data processing

The data processing is performed in the following sequence:

1. Select the following input files (necessary for analysis):

- The scenario file: the file that contains all information about initial conditions of a VR scenario[23]. It summarises the elements that are necessary to run the VR scenario which include:
    - Scenario context: scenario name and paths to map files (i.e., path to Component Library in Fig. **5.4**, Fig. **5.3** and
    - Fig**. 5.5**);
    - Points of interest: the path to the objects and properties that are monitored while the scenario is running (i.e., path to Points of Interest in Fig. **5.6**);
    - Rules: path to rule file that applies for the underlying scenario and to be processed by the event-based module (i.e., path to Rules File in Fig. **5.6**);
    - Process dynamics: the path to the configuration file which includes the parameters needed to start the process simulator interface and the properties in the process simulation that should be communicated (i.e., path to Properties File and Simulation File in Fig. **5.7**);
    - Actor information: information about the actor who is supposed to run the underlying scenario, i.e., his role: field operator, control room operator, shift supervisor, etc. It contains also information about the path to the task files to assign the appropriate task for each actor. (i.e., path to Task File in Fig. **5.4** and Actor Input in Fig. **5.3**);
- The log files: the files which contain all information about running a VR scenario at a specific date and time and which are produced by the logging module. Log files record all events, actions and interventions that occur at run-time as illustrated in Fig. **5.8**.

2. Extract all general information about the scenario, actors, roles, etc. from the scenario file. This information provides content to the tables persons, actors and experiments in the database as shown in Section 5.4.5.2.

[23] Annex F provides an overview (checklist) on the data and information required for creating a VR scenario.

3. Search for completed tasks in the log files. The completion of tasks is being monitored by the task tracker inside the task module who then indicates the completion of a task by the proposed actor in the log file. For each completed task, the information related to tasks, operations and events of the database are filled accordingly as shown in Section 5.4.5.2.

4. For each task, the safety analyst - who is running the analysis module - is asked to indicate if the task's operations have been completed correctly or not. If not, he can specify the corresponding external error modes, cognitive error modes, performance conditions and error causes (e.g., via drop-down lists or similar). These elements have been introduced in Chapter 3 as basic elements that are needed to apply the HF methodology. The values that can be assigned here are based on the entries of the corresponding tables in Chapter 3 (Table 3.1, Table 3.2, Table 3.3, Table 3.5 and Table 3.6).

It is worth mentioning here, that some error modes can be automatically discovered in this data-processing phase based on a comparison between task file and log file. Below are some examples of these error modes:

- An operation exists in the task file and does not exist in the log file. This corresponds to the error modes *Not do*ne (Table **3.1**, Table **3.2**), *part of* (Table **3.2**), *None* (Table **3.1**).

- The time for completing this operation in the log file is less or more than the time in the task file. This corresponds to the error modes *sooner than*, *later than* (Table **3.2**).

- The sequence for performing an activity in the log file is different than the sequence in the task file. This corresponds to the error mode out of *out of sequence* (Table **3.2**), *skipped* (Table **3.1**).

- An operation appears more than one time in the log file and only once in the task file. This corresponds the error mode *out of sequence* or r*epeated* (Table **3.2**).

- An operation appears only in the log file. This corresponds to the error mode *as well as* (Table **3.2**).

This automatic recognition of some error modes should not prevent the safety analyst from rechecking their correctness and validity in relation with the underlying situation. Cognitive error modes (Table 3.3), performance conditions (Table **3.5**) and cognitive error causes (Table **3.6**) should not be automatically selected since the safety analyst has

to evaluate the actions taken by the operator and then select the error modes that fit to the situation.

5.4.5.2 Data storing

The data extracted in the first analysis phase (i.e., *data processing*, Section 5.4.5.1) together with the initial evaluation of the safety analyst (the person who is running the analysis module) are stored in a structured form in a database so that relevant information about performed experiments can be retrieved. In this database, the data are stored in the following tables[24]:

1. Persons: general data about persons[25] who can be involved in experimenting with the VR system. This table should be prepared by the organisation or the unit who experiments with the VR system in advance. Examples of this data include: name, job title, qualification, experience, anthropometric information (weight, height, stretch, etc.), etc.

2. Actors: data about the actors who can perform operations in the experiment. It can be a real user (e.g., a field operator who is interacting with the system via tracking devices) or a fully virtual character. Examples of this data include: actor identification, role, link to persons who can act as this actor, link to the experiments that can be assigned or performed by this actor, etc.

3. Experiments: all data about experiments and related scenarios. Some of the data are obtained from the scenario file whereas other data are obtained from the log files. Examples of this data include: name of experiment, start/end date and time of the experiment, name of the map file used in this experiment, name of the rules file used in this experiment, environmental conditions (wind speed, weather, etc.), etc.

4. Tasks: all data about the task(s) that can be performed in an experiment. Examples of this data include: task name, task description, actor in charge of performing this task, task file, start/end date and time of the task, etc.

[24] An experiment in the virtual environment involves the execution of a task - which consists of operations - by an actor. An experiment might include events (actions) that are not part of the task operations.

[25] It is assumed that the organisation that runs such a system pays attention to personal data and privacy protection, i.e., the involved persons are informed about the process and the stored data will not be misused, distributed, etc.

5. Operations: all data about the operations performed by the actor in a task and mostly obtained from the log files. Operations play an important role in providing key information on operator's behaviour and response. The information stored under "operations" includes the name, the property and the value of the object (component) that the actor "operates" with. Further information stored here cover the final result related to a particular operation, i.e., success or failure of the operation itself. This information includes external error modes, cognitive error modes, performance conditions and error causes as was introduced in Section 5.4.5.1. This information is entered or verified by the safety analyst who is also familiar with the experiment conditions as well as real operating conditions for further analysis.

6. Events: contains all incidents that happen in the experiment at run-time. Unlike operations, events represent manual or automatic actions that are not part of the operational task for performing a certain process. An event can be caused by a safety analyst, field operator, control room supervisor, etc. Typical examples on events are automatic gas alarms, temperature change, igniting a gas leak, etc.

5.4.5.3 Data querying

The results and data stored in the database can be accessed and queried using a dedicated tool or interface. Using a query-interface, it is possible to extract customised information on persons, the experiments they performed, error types and modes during running these experiments and any other information that might be needed by the safety or human factors analyst. The queried information can be displayed in a web browser, stored in a text-file, exported to an EXCEL sheet, etc.

An example that illustrates the extraction of some human factors and risk analysis related data after running a VR experiment is presented in Section 6.3.

5.5 Summary

This chapter proposed a VR environment design for supporting risk analysis work. The provided design focused on the needs of the end users from the research domain (chemical process industry) by basing it on a HF supported set of functional requirements that have been developed and introduced in chapters three and four. The proposed system architecture emphasised the need of linking external modules, i.e., authoring module, process dynamics module, analysis module, etc. for the purpose of providing support for functions that are not typically supported by a VR system.

6
Validation

In this chapter a validation of the findings of the underlying thesis is introduced. The chapter applies the same structure followed in this thesis, i.e., in Section 6.1 the results of Chapter 3 are validated (the HF methodology for supporting risk analysis), in Section 6.2 the results of Chapter 4 (end user scenarios and functional VR requirements) are validated and in Section 6.3 the findings of Chapter 5 (VR environment design) are validated.

6.1 Validation of the HF methodology: A case study

To validate the HF methodology, it is applied to a case study on "detection of gas leakage at a gas processing plant" (chemical process industry). This case study stems from a plant for processing and transporting gas and condensate (light oil). An improper or delayed detection of gas leakage might have dangerous consequences as the gas clouds might be easily transformed into fire upon approaching an ignition source. A successful detection of gas leakage (i.e., exact leakage location, leakage cause, leakage quantity, etc.) reduces the negative consequences and increases the opportunity of a safe removal of the leakage. In case of uncertainties in dealing with the gas leakage, i.e., leakage could not be correctly identified, leakage quantity is high, location of leakage is not accessible, etc., the field operator might press the next Emergency Shut-Down (ESD) button close to him. This action represents the safest solution in case of uncertainties but at the same time the most expensive one due to the resulting production stop for days, the investigations that have to be conducted, the reports that have to be produced by involved persons, the revisions, etc.

Based on that, it is of great importance to perform a correct and satisfactory gas detection to enhance safety and reduce the chance of pressing the ESD button[26].

It is worth mentioning here that due to confidentiality of data and the signed secrecy agreements, no plant-specific illustrations, diagrams or equipment photos are presented here.

[26] None of the reported gas leakages in the plant required pressing ESD button so far. Based on that, there are no experience values on response time, plant consequences, escalations, etc. in such a case.

6.1.1 The process under consideration

The pressure-drop process which takes place at the “Pressure Drop Station” (PDS) of the plant is considered here as a potential source of gas leakage. The pressure-drop process can be decomposed into the following steps:

1. The process gas, which comes from the field, is processed in a cyclone liquid separator to be drained (inlet pressure 120-180 bar);
2. The gas is heated from 4 °C to 21°C using two parallel heat exchangers;
3. The pressure is then reduced to 118 bar using a parallel set of Pressure Reducing Valves,
4. The 118-bar gas passes through mercury removal columns to be cleaned of mercury particles;
5. The gas passes further to H2S removal,
6. The gas leaves the PDS to further process pipelines.

6.1.2 Data collection

An empirical method of data collection has been followed based on:

1. Interviews with involved persons: Safety managing director, process supervisor, ESD supervisor, fire brigade operators, control room operator, field operator and shift supervisor;
2. Review of available documentation on the plant's specific process of gas leakage detection;
3. Monitoring the operators while performing the job;
4. A joint analysis of the results with the involved persons.

The collected data focused on the operational, safety and emergency procedures applied to the PDS. The data covered:

- Description of the pressure-drop process
- Detailed description of operations during:

    - PDS and plant Start-up
    - Normal functioning
    - Programmed maintenance
- Description of procedures to be adopted and consequences in case of:
    - Shut-down
    - Blow-down
    - Emergency
    - Fire
    - Evacuation
- Roles' description during each procedure:
    - Control Room operators
    - Field supervisors
    - Field operators
    - Maintenance operators
    - Emergency response team
    - Fire brigade operators

This work has been carried out within the framework of 3 visits to the plant and a total of 10 days of on-site-work. These visits have been also utilised to review and fine tune the end user requirements presented in Chapter 4.

6.1.3 Applying the HF methodology on the gas leakage detection

6.1.3.1 Task analysis

A gas leakage detection process is carried out in the following simplified sequence:

1. Detection phase: an alarm flashes in control room, alerting operators of a possible leakage;

2. Alert phase: control room operator communicates with the field operator, using a walkie-talkie, to go to the area to check the possible leakage with a portable gas detector;

3. Observation and classification phase: field operator observes and classifies the leakage. The leakage is classified as small if the measured gas concentration up to 25%. A medium leakage corresponds to a gas concentration of 25-65% whereas a large leakage is reported by a concentration of more than 65% (also called explosion leakage to due to the high explosion risk);

4. Confirmation phase: field operator reports to control room by confirming the leakage (size, location, etc.);

5. Decision phase: control room operator, shift supervisor and field operator take a decision on the correct action to perform;

6. Action phase, leading to 2 possible operations:

    - ESD and, if necessary, blow down (BD) by isolating a segment of the pipeline, by means of ESD valves. This action is done by pressing the ESD/BD button, in case of an escalated medium or large gas leakage.

    - Corrective maintenance: field operator or maintenance technician repairs the leakage without closing the operative pipeline or pressing ESD button. This action is mostly performed in case of small gas leakages due to the lower risk of gas leakage escalation.

One of the most important factors for a safe and adequate execution of the gas leakage detection on the field is the response time of the operators (control room and field operators). Short response times mean a safe and adequate dealing with the problem whereas long response times increase the risk of escalation.

It is worth mentioning, that the confirmation phase of the gas leakage detection process represents the most critical phase as reported by end users. This is due to the fact that a wrong (or delayed) confirmation would lead to an incorrect (or delayed) decision and negative consequences, e.g., explosion, fire, production stop for a couple of days, plant damages, etc. For this reason, the dynamic event trees that are produced in later steps focus on the confirmation phase and its impact on subsequent phases.

The result of the task analysis is illustrated in the task diagram of the gas leakage detection as shown in Fig. **6.1**.

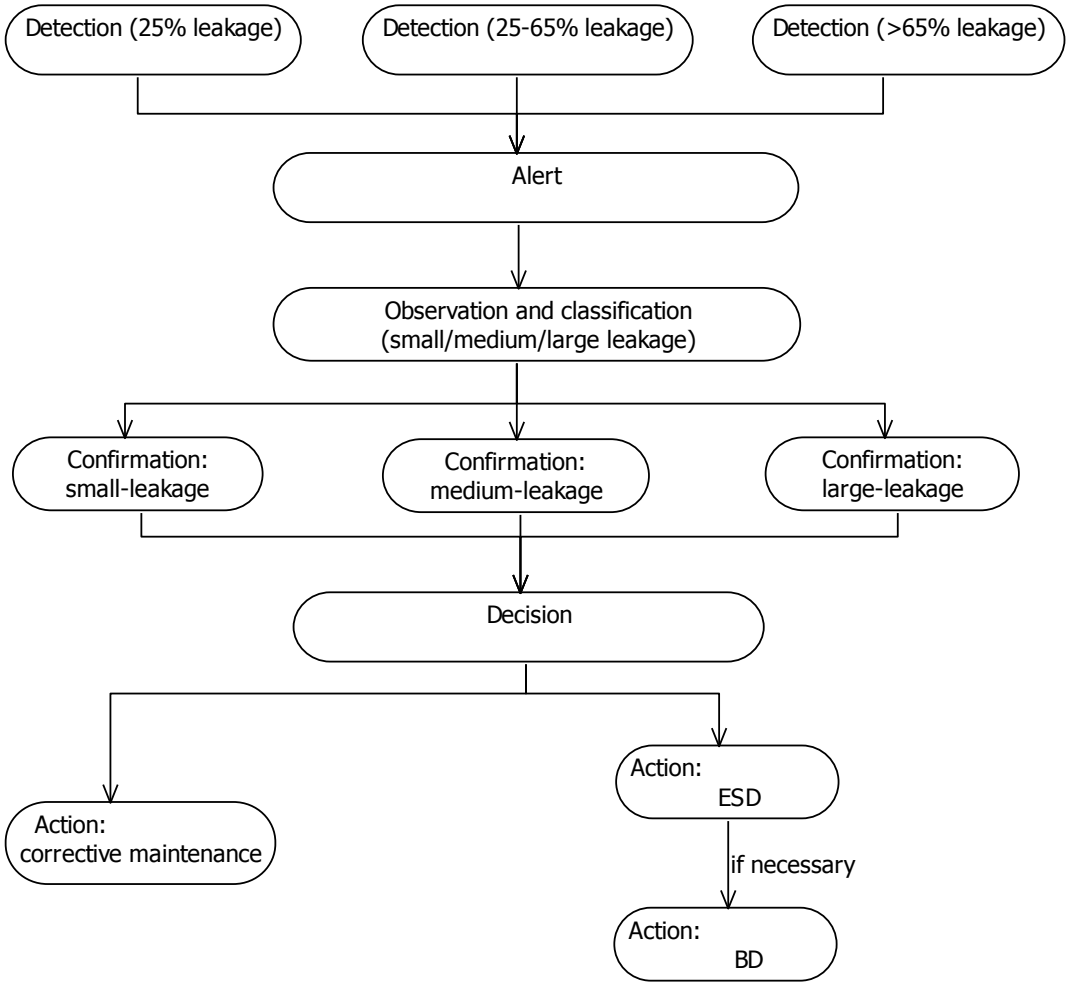


Fig. 6.1: Task analysis results

6.1.3.2 Error analysis

I) Define possible deviations (external error modes)

Table **6.1** lists the most common and relevant deviations that might occur during the gas leakage detection as reported by the interviewed persons (first column). The corresponding external error mode is assigned to the deviation in the second column and an explanation of the error mode is provided in the third column.

Table 6.1: Possible deviations and the corresponding external error modes

Deviation	**External error mode**	**Explanation**
Detection		
Detection fails	Not done	An important piece of information on detecting a leakage is not displayed (i.e., faulty sensor)
False alarm	Skipped	Received data (i.e., alarm signal) is ignored because they are not relevant. Happens often in case of snowy or windy weathers.
Delayed observation by control room operator	Later than	Cues of data are not identified in time
Misreading of tag number from control room screen	More/less than	Error in reading instruments
Alert		
No communication to field operator	None	An important piece of information, i.e., the communication process, is not available
Delayed connection	Later than	Cues of data are not identified (i.e., communicated) in time
Misunderstanding	Misunderstood	An event is mistaken
Observation and classification		
Wrong part of plant	Other than	Collected data are not pertinent to the situation
Component failure, i.e., faulty portable detector	Mistrusted	Unreliable instrument
Wrong detection procedure	Not done	Failure to identify critical information
Wrong classification of the leakage size	Other than	Cues are wrongly associated to the implications of the situation
Omit to check some parts	Part of	Data are not sufficient to understand the situation and make a decision
Confirmation		
No confirmation from field operator	None	An important piece of information, i.e., the confirmation statement, is not available
Wrong confirmation from field operator	Other than	Cues of data are wrongly associated to the implications of the situation
Delayed confirmation	Later than	Cues of data (i.e., the confirmation statement) are not identified in time
Decision		
Wrong decision on corrective maintenance Wrong decision on pressing ESD button Wrong decision on not-pressing ESD button	Other than	Cues of data are wrongly associated to the implications of the situation
Delayed decision on initiating ESD	Later than	Cues of data (i.e., initiating ESD) are not identified in time

Action		
Wrong/insufficient corrective maintenance	Other than/part of	Cues of data are wrongly associated to the implications of the situation Action is not sufficient to solve the situation
Delayed corrective maintenance	Later than	Action is not performed in time
Failure in Field ESD button	Mistrusted	Unreliable instrument

II) Define possible causes (cognitive error causes)

Table **6.2** lists the most common and relevant causes of errors and deviations that might occur during the gas leakage detection as reported by the interviewed persons (second column). The corresponding cognitive error cause is assigned in the third column and an explanation of the cognitive error cause is provided in the fourth column. An empty field under the column "cognitive error cause" means that no cognitive error cause can be assigned to the particular deviation. This is common in technical deviations[27] caused by instrument errors, device failures, equipment damage, etc. or environment caused deviation, i.e., weather, ambient noise, etc.

Table 6.2: Possible deviation causes and the corresponding cognitive error causes

Deviation (external error modes)	**Causes**	**Cognitive error cause**	**Explanation**
Detection			
Detection fails **(not done)**	Faulty detector		A technical deviation, no cognitive error causes
False alarm **(skipped)**	Faulty detector		A technical deviation, no cognitive error causes
	Weather (snow/wind)		Environment caused deviations, no cognitive error causes
Delayed observation by control room operator **(later than)**	Attenuation to repeated false alarm sound	Underestimation of criticality	Frequent false alarms might lead to ignoring a real one, i.e., Operator misjudged consequences
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Overlooking the real alarm Operator misjudged consequences Operator is not aware of costs of recovery

[27] The technical deviations meant here are unexpected ones that are identified while performing gas leakage detection. A pre-existing device failure or wrong sensor readings do not belong to this category as they might have cognitive error causes like "under-estimation of criticality" or "under-estimation of cost of recovery".

	Multitasking	Inefficient method	The control room operator is involved in other tasks. Working method (procedures) and task allocations is inefficient.
Misreading of tag number from control room screen **(more/less than)**	Ambient lightening conditions	Inefficient method	Working conditions in control room are not adequate
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Overlooking the real alarm Operator misjudged consequences Operator is not aware of costs of recovery
	Multitasking	Inefficient method	Control room operator is involved in other tasks. Working method (procedures) and task allocations is inefficient
Alert			
No communication to field operator **(none)**	Distortion on walkie-talkie Battery problems		Technical deviations, no cognitive error causes
	Difficulty in directing field operator to leakage location	Interrupted test	Due to inability of control room operator to direct field operator, the communication is interrupted.
Delayed connection **(later than)**	Weather Ambient noise		Environment caused deviations, no cognitive error causes
Misunderstanding **(misunderstood)**	Heavy communication traffic on radio	Inefficient method	Inefficient handling of situation. Working method (communication priority procedures in case of gas leakage) is inefficient.
	Ambient noise		Environment caused deviation, no cognitive error causes
Observation and classification			
Wrong part of plant **(other than)**	Mis-communication	Misordered criteria	Wrong evaluation criteria leading to a wrong selection of leakage location
Component failure, i.e., faulty portable detector **(mistrusted)**	Battery failure Calibration failure Reliability of device		Technical deviations, no cognitive error causes
Wrong detection procedure (**not done)**	Very close or far from the leakage source	Inefficient method	Inefficient handling of situation. Working method (detection procedures in case of gas leakage) is inefficient.
	Approaching the leakage source from wrong direction	Inefficient method	Inefficient handling of situation. Working method (detection procedures in case of gas leakage) is inefficient.
Wrong classification of the leakage size **(other than)**	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Weather/Ambient noise		Environment caused deviation, no cognitive error causes

Omit to check some parts **(part of)**	Source of leakage is difficult to access		No cognitive error cause
	Overlooked due to distraction	Overlooked criteria	Overlooking an important criteria, i.e., an important part of the plant
	Stress	Inefficient method	Inefficient handling of situation. Lack of appraisals and personal talks with field operators
Confirmation			
No confirmation from field operator **(none)**	Channel Occupied	Inefficient method	Inefficient handling of situation. Working method (communication priority procedures in case of gas leakage) is inefficient
	Ambient noise		Environment caused deviation, no cognitive error causes
	Microphone distortion Battery problems		Technical deviations, no cognitive error causes
Wrong confirmation from field operator **(other than)**	Field operator at wrong place	Misordered criteria	Wrong evaluation criteria leading to a wrong selection of leakage place
	Wrong measurements	Misordered criteria	Wrong evaluation and decision criteria leading to a wrong measurement
	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
Delayed confirmation **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Inefficient handling of situation. Working method (responsibility of confirmation) is ambiguous.
	Time pressure	Unlikely states	Field operator spent time in considering unlikely system states. In most cases, this deviation is situation dependent, i.e., there is a very narrow time slot to confirm due to severity of situation.
	Stress	Inefficient method	Inefficient handling of situation. Lack of appraisals and personal talks with field operators
	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Heavy communication traffic on radio	Inefficient method	Inefficient handling of situation. Working method (communication priority procedures in case of gas leakage) is inefficient
	Ambient noise		Environment caused deviation, no cognitive error causes
Decision			
Wrong decision on corrective maintenance **(other than)** Wrong decision on pressing ESD button **(other than)** Wrong decision on not-pressing ESD button **(other than)**	Ambiguous delineation of responsibility	Inefficient method	Inefficient handling of situation. Working method (responsibility of confirmation) is ambiguous.
	Stress/Fatigue	Inefficient method	Inefficient handling of situation. Lack of appraisals and personal talks with field operators
	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Lack of procedural guidance	Inefficient method	Inefficient handling of situation. Working method (decision procedures) is not available.

Delayed decision on initiating ESD **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Inefficient handling of situation. Working method (responsibility of confirmation) is ambiguous.
	Stress/Fatigue	Inefficient method	Inefficient handling of situation. Lack of appraisals and personal talks with field operators
	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Lack of procedural guidance	Inefficient method	Inefficient handling of situation. Working method (decision procedures) is not available.
	Underestimation of consequences	underestimation of recovery cost	Costs and consequences of being wrong are not taken into account
Action			
Wrong/insufficient corrective maintenance **(other than/part of)**	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Underestimation of consequences	Underestimation of cost of recovery	Costs and consequences of wrong maintenance are not taken into account
	Overlooking a system state	Missed state	Technician considered fewer alternatives and plans of action for maintenance
Delayed corrective maintenance **(later than)**	Lack of experience	Over/under confidence	Staff experience and competence is inadequate
	Underestimation of consequences	Underestimation of cost of recovery	Costs and consequences of delayed maintenance are not taken into account
Failure in Field ESD button **(mistrusted)**	Reliability of device		Technical deviations, no cognitive error causes

III) Define cognitive error modes

After an examination of the listed deviations and their causes and with the assistance of Table 3.3**,** the applicable and situation-relevant cognitive error modes have been identified and provided in Table **6.5** (fifth column). These cognitive error modes are further used in producing the dynamic event tree of cognitive errors and viable plans.

6.1.3.3 Performance analysis

I) Define performing mechanisms

The definition of performance mechanisms that affect the execution of a particular task or operation represents a supporting tool for the analyst to examine behavioural reasons of making a particular decision.

The application of performance mechanisms on the underlying case study is illustrated for the confirmation phase in which the operator has to trade off two conflicting goals:

spending more time in the confirmation phase to have a more reliable decision or make a quick (uncertain) confirmation which might lead to an ESD action. The first option entails a higher risk of increased leakage and escalation whilst the second option has a higher risk of financial losses. This decision dilemma is likely to be influenced by the cost of recovering from one option to another and the operator confidence in their judgment as illustrated in Table **6.3**.

Table 6.3: Analysis of goal tradeoffs in terms of performance mechanisms (confirmation phase)

Evaluation criteria	**Option 1: Longer confirmation time**	**Option 2: Quick (uncertain) confirmation leading to ESD**	**Explanation**
Plant consequences			
Risk of leakage escalation	Higher risk of uncontrolled gas leakage	Lower risk of uncontrolled gas leakage	A longer confirmation increases the risk of uncontrolled gas leakage
Financial losses	Low risk of financial losses (no production stop)	Higher risk of financial losses due to production stop	A quick (uncertain) confirmation increases the risk of financial losses
Confidence in judgment			
Performance demands (experience and training)	High performance demands	High performance demands	In both cases, a high level of experience and training is required to cope with task demands
Quality of procedural guidance	Decision seen as stretching procedure	Decision interpreted as conform with procedure	Pressing ESD in similar cases is consistent with operational procedures
Cost of recovering errors			
Reverse or undo decision	Possible	Impossible	In case of longer confirmation, there is a possibility to switch to option 2, i.e., press ESD. No possibility to recover, in case of pressing ESD
Performance feedback	Possible	Impossible	Operator may choose later to switch to option 2, i.e., press ESD.

II) Define related work context (performance conditions)

Table **6.4** introduces the performance conditions (work context) related to the listed deviation, i.e., the working conditions that participate in causing the deviation (fourth column). An explanation of the performance conditions is provided in the fifth column. An empty field under the column "performance conditions" means that no performance conditions can be assigned to the particular deviation. Similar to cognitive error causes, this is common in technical deviations[28] caused by instrument errors, device failures, equipment damage, etc.

[28] The technical deviations meant here are unexpected ones that are identified during the task. A pre-existing device failure or wrong sensor readings do not belong to this category as they might have causes related to performance conditions, e.g., "availability of plans" or "organisational factors".

Table 6.4: Performance conditions

Deviation (external error modes)	**Causes**	**Cognitive error cause**	**Performance conditions**	**Explanation**
Detection				
Detection fails **(not done)**	Faulty detector			
False alarm **(skipped)**	Faulty detector			
	Weather (snow/wind)		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
Delayed observation by control room operator **(later than)**	Attenuation to repeated false alarm sound	Underestimation of criticality	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Frequent false alarms might lead to ignoring a real one, i.e., Operator misjudged consequences
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Poor training and poor supervision are main reasons of distraction
	Multitasking	Inefficient method	Performing many tasks at close time proximity (Number of parallel tasks)	The control room operator is performing many tasks at close time proximity
Misreading of tag number from control room screen **(more/less than)**	Ambient lightening conditions	Inefficient method	Inadequate policies for job aids (organisational factors)	Job aids and supports which includes adequate lightening conditions to perform work belongs to the company policy.
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Poor training and poor supervision are main reasons of distraction
	Multitasking	Inefficient method	Performing many tasks at close time proximity (Number of parallel tasks)	The control room operator is performing many tasks at close time proximity
Alert				

No communication to field operator **(none)**	Distortion on walkie-talkie Battery problems			
	Difficulty in directing field operator to leakage location	Interrupted test	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience, poor training and poor supervision contribute to the causes of this deviation
Delayed connection **(later than)**	Weather Ambient noise		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
Misunderstanding **(misunderstood)**	Heavy communication traffic on radio	Inefficient method	Poor supervision (Supervision) Inadequate policies for task priorities (Organisational factors)	The supervisor has the authority of stopping non urgent communications. Control room operators do not have this authority (company policy)
	Ambient noise		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
Observation and classification				
Wrong part of plant **(other than)**	Miscommunication	Misordered criteria	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience, poor training and poor supervision contribute to the causes of this deviation
Component failure, i.e., faulty portable detector **(mistrusted)**	Battery failure/ Calibration failure/ Reliability of device			
Wrong detection procedure (**not done)**	Very close or far from the leakage source	Inefficient method	Poor procedures (Availability of information)	Lack of a clear written procedure for gas leakage detection. Lack of guidelines in case of inaccessible gas leakage.
	Approaching the leakage source from wrong direction	Inefficient method	Poor procedures (Availability of information) Poor training (Availability of plans and instructions)	Lack of a clear written procedure for gas leakage detection. Lack of guidelines in case of inaccessible gas leakage. Inadequate training of field operators
Wrong classification of the leakage size **(other than)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions)	Lack of experience and poor training of field operators
	Weather Ambient noise		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
Omit to check some parts **(part of)**	Source of leakage is difficult to access		Poor procedures (Availability of information)	Lack of a clear written procedure for gas leakage detection. Lack of

				guidelines in case of inaccessible gas leakage
	Overlooked due to distraction	Overlooked criteria	Poor training (Availability of plans and instructions) Workload distraction (CDFs)	Field operator is not well trained and distracted himself to unimportant information. Field operator is distracted due to workload (e.g., intensive leakage at many locations)
	Stress	Inefficient method	Capability Degrading Factors (CDFs) Lack of teamwork (Teamwork)	Field operator is distracted due to personal or workload factors (stress) Lack of team communication and team culture for "stress-relief"
Confirmation				
No confirmation from field operator **(none)**	Channel Occupied	Inefficient method	Poor procedures (Availability of information) Poor supervision (Supervision)	Lack of a clear written procedure. Poor supervision as supervisor has the authority of stopping non urgent communications
	Ambient noise		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
	Microphone distortion Battery problems			
Wrong confirmation from field operator **(other than)**	Field operator at wrong place	Misordered criteria	Poor procedures (Availability of information) Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of a clear written procedure for gas leakage detection Inadequate training of field operators Lack of guidance by supervisor
	Wrong measurements	Misordered criteria	Poor procedures (Availability of information) Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of a clear written procedure for gas leakage detection Inadequate training of field operators Lack of guidance by supervisor
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor

Delayed confirmation **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Lack of sharp procedure for confirmation
	Time pressure	Unlikely states	Narrow time slot to respond (availability of time to respond)	The time to respond is very short
	Stress	Inefficient method	Capability Degrading Factors (CDFs)	Field operator is distracted due to personal or workload factors (stress)
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor
	Heavy communication traffic on radio	Inefficient method	Poor supervision (Supervision) Inadequate policies for task priorities (Organisational factors)	The supervisor has the authority of stopping non urgent communications. Field operators do not have this authority (company policy)
	Ambient noise		Capability Degrading Factors (CDFs)	Environmental factors that affect operators in a global way
Decision				
Wrong decision on corrective maintenance **(other than)** Wrong decision on pressing ESD button **(other than)** Wrong decision on not-pressing ESD button **(other than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Lack of sharp procedure for decision and consequences in case of wrong decision
	Stress/Fatigue	Inefficient method	Capability Degrading Factors (CDFs)	Field operator is distracted due to personal or workload factors (stress)
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor
	Lack of procedural guidance	Inefficient method	Inadequate procedures (Availability of information)	Lack of sharp procedure for decision
Delayed decision on initiating ESD **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Lack of sharp procedure for decision and consequences in case of wrong decision
	Stress/Fatigue	Inefficient method	Capability Degrading Factors (CDFs)	Field operator is distracted due to personal or workload factors (stress)
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor

	Lack of procedural guidance	Inefficient method	Inadequate procedures (Availability of information)	Lack of sharp procedure for decision
	Underestimation of consequences	underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)	Lack of experience and poor training of field operators Lack of supervision Lack of teamwork for a better estimation of consequences
Action				
Wrong/insufficient corrective maintenance **(other than/part of)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor
	Underestimation of consequences	Underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)	Lack of experience and poor training of field operators Lack of supervision Lack of teamwork for a better estimation of consequences
	Overlooking a system state	Missed state	Poor training (Availability of plans and instructions)	Lack of experience and poor training of field operators
Delayed corrective maintenance **(later than)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Lack of experience and poor training of field operators Lack of guidance by supervisor
	Underestimation of consequences	Underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)	Lack of experience and poor training of field operators Lack of supervision Lack of teamwork for a better estimation of consequences
Failure in Field ESD button **(mistrusted)**	Reliability of device			

6.1.3.4 Define possibilities of error detection and recovery

A closer consideration of the underlying case study and its individual operations and steps lead to defining three possibilities for performing each operation:

- Operation is performed correctly (i.e., detection is successful, confirmation is successful, etc.).
- Operation is performed with delays (i.e., detection is delayed, confirmation is delayed, etc.).
- Operation is performed wrongly (i.e., wrong detection, wrong confirmation, etc.).

The potential of error recovery (viable plans) is very high in delayed operations and limited in wrongly performed operations. Correctly performed operations do not require recovery plan as they represent safe implementation of the operational procedures. Based on that, the consideration of possible cues for error recovery is limited to delayed operations as shown in the sixth column "error recovery" of Table **6.5**.

To reduce complexity and enable producing a well-arranged DET (see next section), only 7 possible viable plans[29] for error recovery have been presented in Table **6.5**:

1. Viable plan 1 for error recovery in the detection phase;
2. Viable plan 2 for error recovery in the alert phase;
3. Viable plan 3 for error recovery in the observation and classification phase;
4. Viable plan 4 for error recovery in the confirmation phase;
5. Viable plan 5 for error recovery in the decision phase;
6. Viable plan 6 for error recovery in the action phase in case of insufficient corrective maintenance;
7. Viable plan 7 for error recovery in the action phase in case of delayed corrective maintenance.

[29] The possibilities of error recovery in this case study are not only limited to these 7 viable plans. Further recovery plans can be defined.

Table 6.5: Cognitive error modes and error recovery plans (viable plans)

Deviation (external error modes)	**Causes**	**Cognitive error cause**	**Performance conditions**	**Cognitive error mode**	**Error recovery**
Detection					
Detection fails **(not done)**	Faulty detector				
False alarm **(skipped)**	Faulty detector				
	Weather (snow/wind)		Capability Degrading Factors (CDFs)		
Delayed observation by control room operator **(later than)**	Attenuation to repeated false alarm sound	Underestimation of criticality	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Delayed plan (delayed diagnosis)	<u>Viable plan 1:</u> Shift supervisor recognises the alarm and takes responsibility
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Multitasking	Inefficient method	Performing many tasks at close time proximity (Number of parallel tasks)		
Misreading of tag number from control room screen **(more/less than)**	Ambient lightening conditions	Inefficient method	Inadequate policies for job aids (organisational factors)	Wrong plan (wrong diagnosis)	
	Distraction	Missed states/under-estimation of criticality/under-estimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Multitasking	Inefficient method	Performing many tasks at close time proximity (Number of parallel tasks)		
Alert					

No communication to field operator **(none)**	Distortion on walkie-talkie Battery problems			Wrong plan	
	Difficulty in directing field operator to leakage location	Interrupted test	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
Delayed connection **(later than)**	Weather Ambient noise		Capability Degrading Factors (CDFs)	Delayed plan	
Misunderstanding **(misunderstood)**	Heavy communication traffic on radio	Inefficient method	Poor supervision (Supervision) Inadequate policies for task priorities (Organisational factors)	Delayed plan Unable to understand	<u>Viable plan 2:</u> Shift supervisor stops all unnecessary communications and alerts field operator
	Ambient noise		Capability Degrading Factors (CDFs)		
Observation and classification					
Wrong part of plant **(other than)**	Miscommunication	Misordered criteria	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Wrong plan	
Component failure, i.e., faulty portable detector **(mistrusted)**	Battery failure/ Calibration failure/ Reliability of device				
Wrong detection procedure (**not done)**	Very close or far from the leakage source	Inefficient method	Poor procedures (Availability of information)	Wrong plan	
	Approaching the leakage source from wrong direction	Inefficient method	Poor procedures (Availability of information) Poor training (Availability of plans and instructions)		
Wrong classification of the leakage size **(other than)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions)	Wrong plan	
	Weather Ambient noise		Capability Degrading Factors (CDFs)		
Omit to check some parts **(part of)**	Source of leakage is difficult to access		Poor procedures (Availability of information)	Incomplete plan Delayed plan	<u>Viable plan 3:</u> Shift supervisor re-checks situation with field operator
	Overlooked due to distraction	Overlooked criteria	Poor training (Availability of plans and instructions) Workload distraction (CDFs)		

	Stress	Inefficient method	Capability Degrading Factors (CDFs) Lack of teamwork (Teamwork)		
Confirmation					
No confirmation from field operator **(none)**	Channel Occupied	Inefficient method	Poor procedures (Availability of information) Poor supervision (Supervision)	Unable to make plan	
	Ambient noise		Capability Degrading Factors (CDFs)		
	Microphone distortion Battery problems				
Wrong confirmation from field operator **(other than)**	Field operator at wrong place	Misordered criteria	Poor procedures (Availability of information) Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Wrong plan	
	Wrong measurements	Misordered criteria	Poor procedures (Availability of information) Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
Delayed confirmation **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Delayed plan Inefficient plan	<u>Viable plan 4:</u> Shift supervisor stops all unnecessary communications Shift supervisor sends a more experienced field operator to re-observe and re-classify Shift supervisor takes complete responsibility of
	Time pressure	Unlikely states	Narrow time slot to respond (availability of time to respond)		
	Stress	Inefficient method	Capability Degrading Factors (CDFs)		
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Heavy communication traffic on radio	Inefficient method	Poor supervision (Supervision) Inadequate policies for task priorities (Organisational factors)		

	Ambient noise		Capability Degrading Factors (CDFs)		confirmation
Decision					
Wrong decision on corrective maintenance **(other than)** Wrong decision on pressing ESD button **(other than)** Wrong decision on not-pressing ESD button **(other than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Wrong decision Unable to recover	
	Stress/Fatigue	Inefficient method	Capability Degrading Factors (CDFs)		
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Lack of procedural guidance	Inefficient method	Inadequate procedures (Availability of information)		
Delayed decision on initiating ESD **(later than)**	Ambiguous delineation of responsibility	Inefficient method	Ambiguous procedures (Availability of information)	Delayed plan	<u>Viable plan 5:</u> Shift supervisor takes decision and presses ESD button
	Stress/Fatigue	Inefficient method	Capability Degrading Factors (CDFs)		
	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)		
	Lack of procedural guidance	Inefficient method	Inadequate procedures (Availability of information)		
	Underestimation of consequences	underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)		
Action					
Wrong/insufficient corrective maintenance **(other than/part of)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Incomplete plan	<u>Viable plan 6</u> Maintenance technician calls for additional support
	Underestimation of consequences	Underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)		

	Overlooking a system state	Missed state	Poor training (Availability of plans and instructions)		
Delayed corrective maintenance **(later than)**	Lack of experience	Over/under confidence	Poor training (Availability of plans and instructions) Poor supervision (Supervision)	Delayed plan	Viable plan 7 Maintenance technician recommends pressing ESD
	Underestimation of consequences	Underestimation of cost of recovery	Poor training (Availability of plans and instructions) Poor supervision (Supervision) Poor teamwork (teamwork)		
Failure in Field ESD button **(mistrusted)**	Reliability of device			Wrong plan	

6.1.3.5 Produce dynamic event trees

In this section, two dynamic event trees are produced: a dynamic event tree for cognitive error modes and viable plans and a dynamic event tree for error recovery.

It is obvious that producing dynamic event trees that cover all cognitive errors and recovery plans provided in Table **6.3** would lead to complex trees. To illustrate how dynamic event trees can be applied in the underlying case study, the focus is on the most critical part of the case study, i.e., the confirmation phase as explained in Section 6.1.3.1 (Task Analysis). Based on that, an abstracted scenario of delayed confirmation and its recovery mechanism (recovery plan 4) - as shown in Fig. **6.2** - is considered for producing the dynamic event trees.

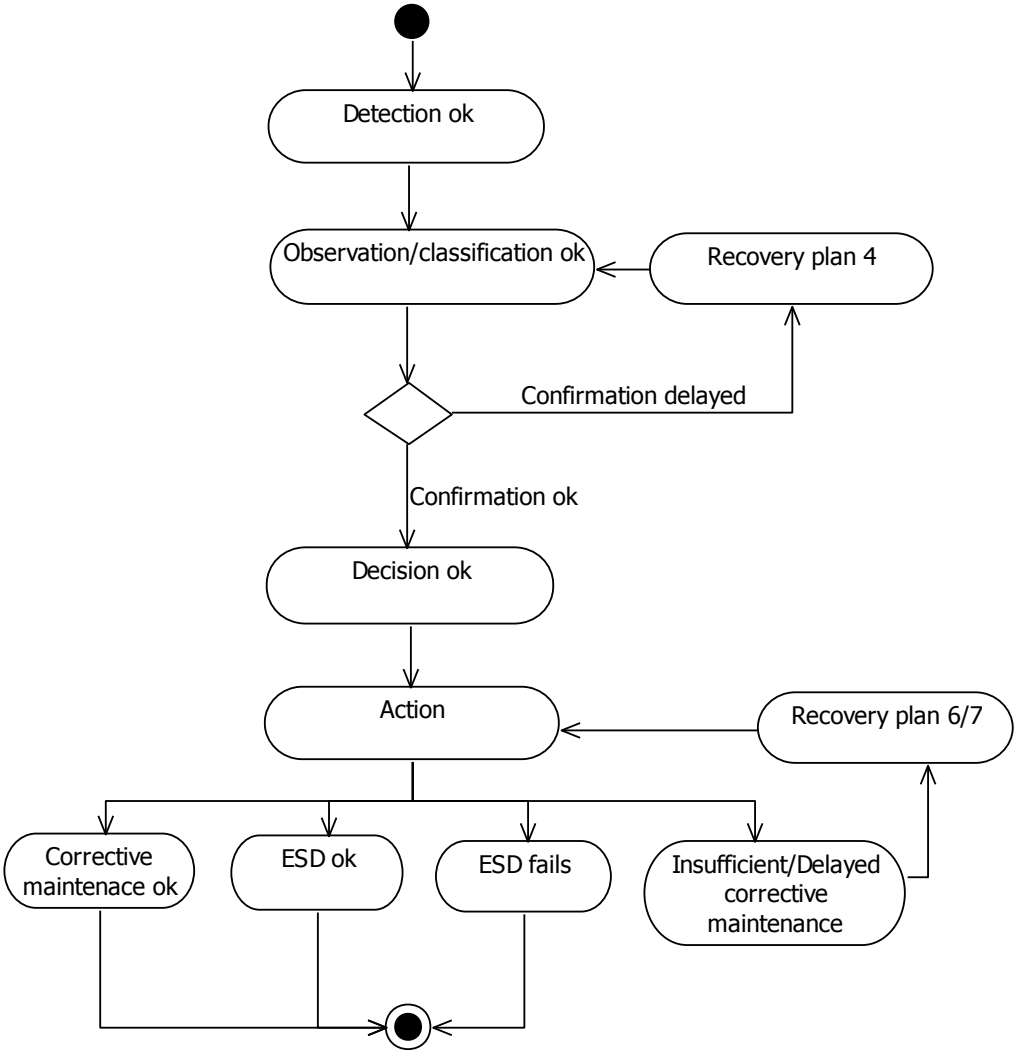


Fig. 6.2: The scenario to be used for producing dynamic event trees

The scenario assumes that detection and classification/observation phases are performed successfully. The confirmation phase is delayed which might lead to escalation if this delay is not treated correctly. A delayed confirmation requires an operational deviation to recovery plan 4 (viable plan 4 in Table **6.5**). Based on viable plan 4, a re-observation and re-classification take place since uncertainty in observation and classification is one of the reasons for delaying the confirmation. A successful execution of viable plan 4 recovers the situation and lead to "confirmation ok". The scenario proceeds by making a decision on the action to be taken. The two safe actions here are a successful corrective maintenance or a successful pressing of ESD button. The third action is "insufficient or incomplete corrective maintenance" which requires an operational deviation to viable plan 6 or 7. The fourth and last action is "ESD fails", which is rare.

Fig. **6.3** provides the dynamic event tree for cognitive error modes and viable plans based on a delayed confirmation that requires executing viable plan 4. Fig. **6.4** provides a dynamic tree for error recovery upon executing viable plan 4.

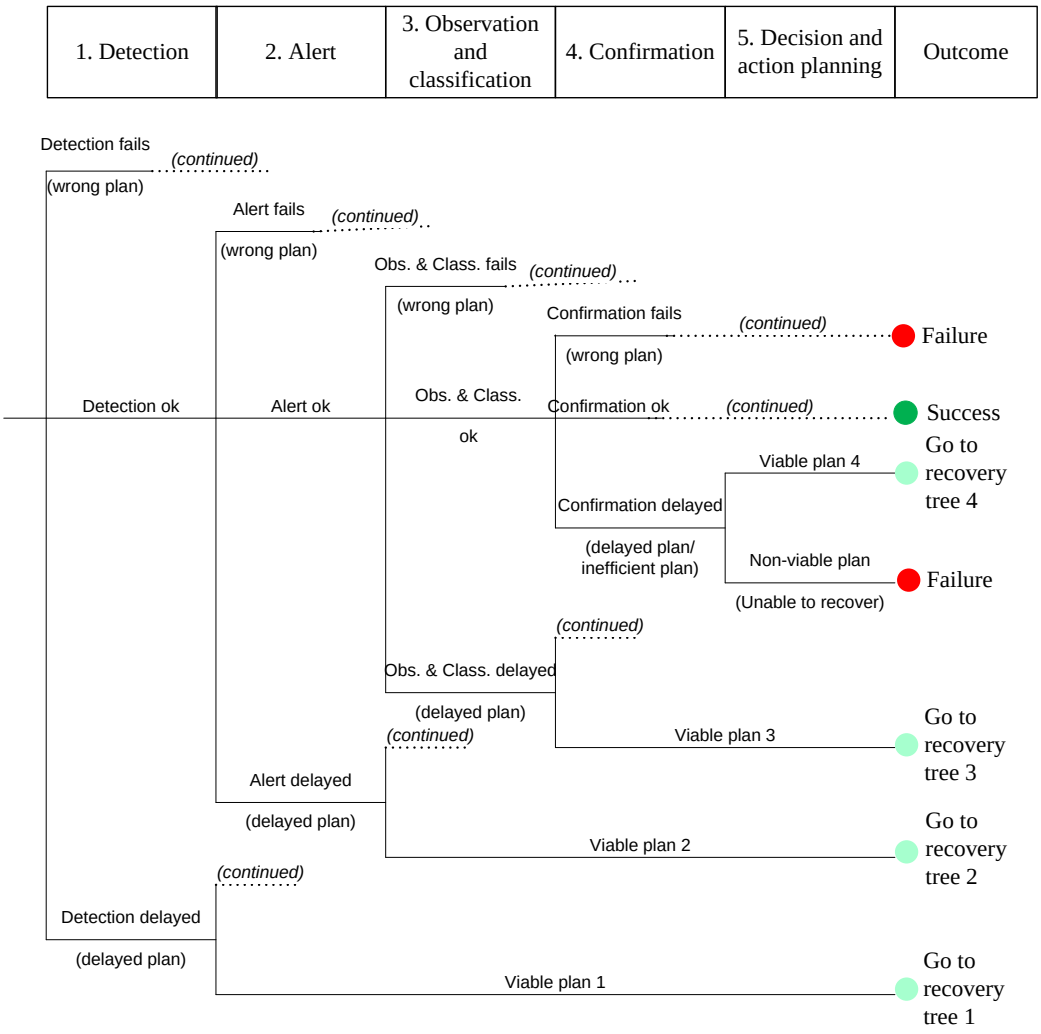


Fig. 6.3: A dynamic event tree of cognitive error modes and viable plans of the case study

The dotted paths with the designation "*continued*" refer to paths which can be further detailed or involve more tree branches. These branches are not illustrated here to reduce complexity and focus on the core part related to "delayed confirmation" and "viable plan 4" as explained above.

The outcome of the event tree is an identification of the branches that lead to "success" and "failure". The branches that end with "go to recovery plan" require further elaboration to see whether a "success" or "failure" would come out.

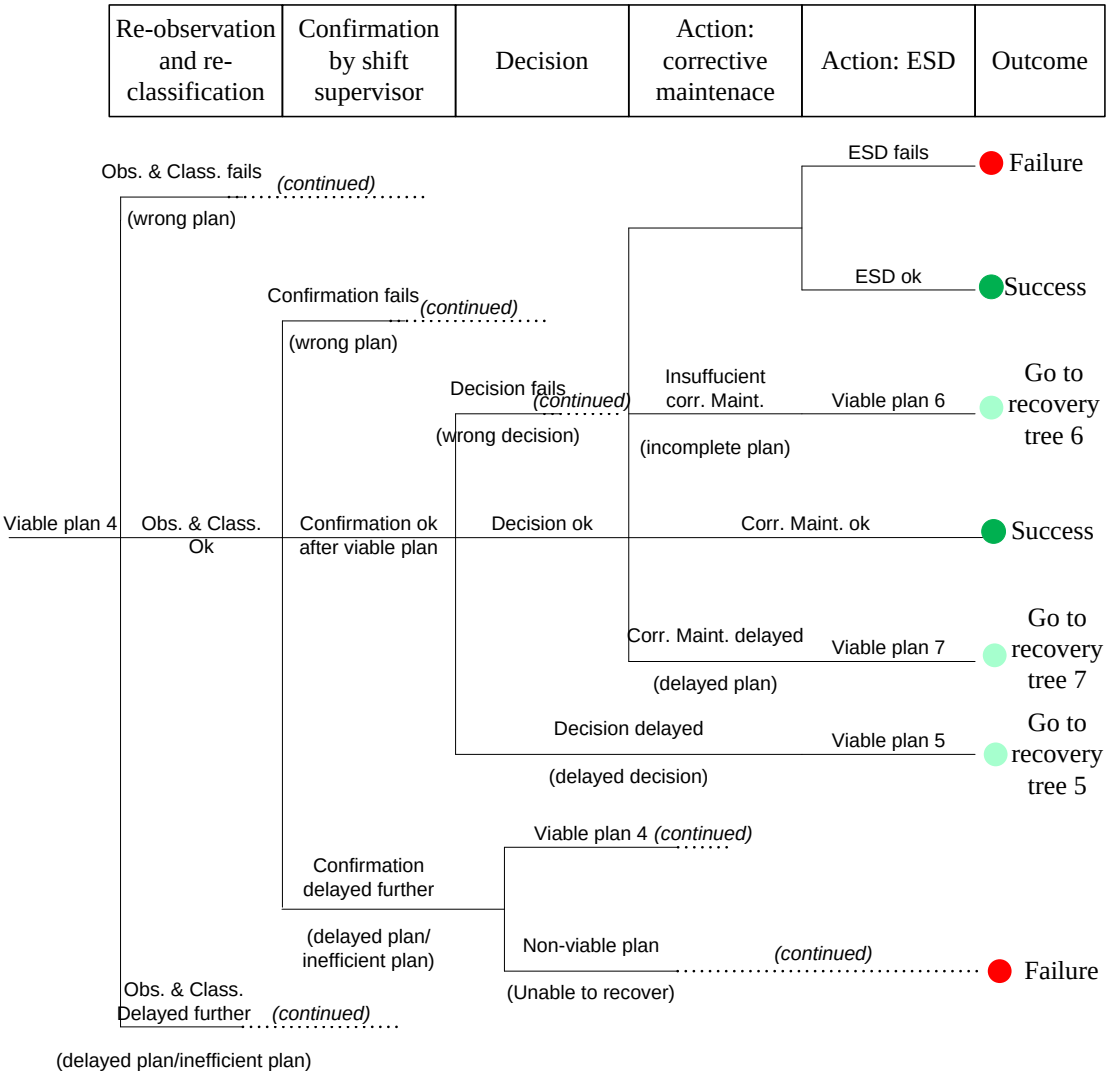


Fig. 6.4: A dynamic event tree of error recovery upon executing viable plan 4

6.1.4 Case study: conclusions

The underlying industrial case study "detection of gas leakage at a gas processing plant" has been used to validate the developed HF methodology and explain how the

methodology can be applied to other case studies by providing its implementation steps (Chapter 3: Section 3.4.2 until 3.4.6 and Fig. **3.5**).

To illustrate the usability of the methodology, it is necessary to figure out how the safety analyst can utilise the results achieved upon applying the methodology to the case study in an improved risk analysis (compared to the conventional QRA that was presented in Section 2.1.6):

1. Define accidental scenarios based on the illustrated deviations, including human-caused one. The definition of human-caused deviations is possible due to the nature of the underlying methodology which focuses on "cognition" and the projection of the simple model of cognitive functions - in the form of tables (Table **3.1**, Table **3.2**, Table **3.4** and Table **3.6**) - on each phase of the underlying case study. Conventional QRA supports defining accidental scenarios based on technical deviations as explained in Chapter 1. An example on one of the most critical and possible scenarios has been introduced and illustrated in Section 6.1.3.5.

2. Improving the way of dealing with errors compared to conventional risk analysis, which is based on defining errors, error causes and probabilities. This has been achieved by dividing errors into external and cognitive errors, defining cognitive error causes and cognitive error modes. This 3-step analysis off errors has the advantages of deriving communalities between errors by classifying them into a higher level, i.e., error modes, and optimising the analyst's effort of solving the error roots. For example, if we consider the cognitive error modes of the confirmation phase (Table 6.5), we identify 4 modes: delayed plan, wrong plan, unable to make plan and inefficient plan. Providing a solution for each of these error modes, i.e., by changing operational procedure, changing safety instructions, introducing new communication equipment, providing field operators with more decision power, etc. would eliminate or reduce 13 roots (second column in Table 6.5) that would cause these types of errors. In a similar way, the safety analyst can extract the error modes of the remaining phases and propose design or operational improvements for eliminating their roots.

3. Including aspects of human performance, i.e., performance conditions, in the risk analysis. This enables identifying the work context elements that affect the performance of the task or a certain step of the task. For example, if we examine the confirmation phase, we identify five major performance conditions that contribute to a wrong or inefficient execution of this phase: availability of information (operational procedures), availability of plans and instructions (training), supervision, organisational factors and capability degrading factors. Improving the work

conditions related to these performance conditions, i.e., sharpening operational procedures, providing regular customised training, introducing a second supervisor during the shift, etc. affects positively the operator's accuracy and efficiency during the confirmation phase. In a similar way, the safety analyst can extract the performance conditions related to the remaining phases and propose necessary operational or organisational improvements for reducing their effects. A definition of performance mechanisms can be supportive here to provide an analysis of goal tradeoffs related to certain situation. The definition of performance mechanisms represents a supporting tool for the analyst to examine behavioural reasons of making a particular decision as illustrated in Table 6.3.

4. Including recovery plans in the analysis, which is not provided in conventional QRA. The recovery plans represent mechanisms for error correction or minimisation of negative consequences. For each step or phase of the case study, a recovery plan might be defined and initiated upon demand. An example of a recovery plan for the confirmation phase has been introduced here (i.e., viable plan 4) and shown that despite the delay that would accompany the execution of this recovery plan, it produces tolerated consequences compared to a wrong confirmation. Defining several recovery plans for operational deviations gives operators flexibility in making decisions and reduces the stress of taking immediate decisions, since incorrect decisions might be recovered.

5. Producing dynamic event trees (DETs) as a combination of cognitive error modes, viable plans and consequences. DETs provide a visualisation of the dangers incorporated into an operation and reflect the dynamic nature of an operational procedure. They allow examining critical paths and check how an error can be completely corrected or recovered. An example of DETs has been provided here for the scenario of "delayed confirmation" and the recovery plan (viable plan 4) that is initiated to recover the situation. The safety analyst should pay special attention to scenarios leading to "failure" in the DETs.

6.2 Validation of end user scenarios and functional VR requirements

The end user scenarios and functional VR requirements have been validated in a loop of iterations under the participation of end users within the framework of the multinational research project mentioned under Section 2.3.3 and Section 4.3. In this regard several workshops took place at industrial sites to ensure a wider qualification and experience profile of the involved end users.

First workshop:

In the first workshop (2 days), the end users were interviewed to fill in the questionnaire template illustrated in Section 4.3. The filled questionnaire template provided an initial input on safety demands, end user requirements and possible scenarios (case studies) that can be defined and detailed.

Second workshop:

In the second workshop (2 days), representatives of the interviewed industries and further invited industries joined a workshop that aims at sharpening the collected requirements from the first workshop and merging the scenarios based on similarities and degree of importance. In this workshop, key industries have been identified as originators of the scenarios and agreed to support a further detailing of the scenario at their own sites. The result of this workshop was a first validation of scenarios.

Third workshop:

The third workshop (3 days) took place at the industrial sites that have been selected in the second workshop. In this workshop, the following aspects have been covered:

- Presentation and validation of the scenario(s) under consideration and agreement on the most relevant one.
- Agreement on the part of the plant to be considered for detailing the scenario.
- Initial evaluation of the availability of documentation related to the selected scenario (operational procedures, safety instructions, risk analysis documentations, etc.).
- Initial evaluation regarding the availability of CAD and 3D data for VR modelling.
- Agreement on the layout of the next workshop and the persons to be involved.
- The management's commitment to support the entire process and clarifying issues on data confidentiality.

The main result of this workshop was a second validation of scenarios with focus on the scenario of interest for the hosting industrial partner.

Fourth workshop:

The fourth workshop (5 days) took place at the same industrial site of the fourth and had the goal of detailing the selected scenario. To achieve this goal, the workshop has been divided into the following blocks:

- First block: review of risk analysis documents (ET, FT, HAZOP, HAZID, etc.) related to the part of the plant and the operational process under consideration;
- Second block: Detailed task analysis via interviews with the persons in charge at the selected part of the plant. The interviewed persons were: process engineer, control room operator(s), field operator(s), shift supervisor, maintenance technician, one member of the emergency response team, one member of the fire brigade team and the safety manager. This part has been accompanied by 2 site tours to the operational part of the plant under consideration and the control room to explain the task (gas leakage detection) inherited in the scenario and show the equipments and devices involved in the task.

Third block: final review of documents and briefing with the involved staff

Fifth workshop:

In the fifth workshop (2 days), a consolidated task analysis was produced based on all interview results from the fourth workshop. Based on the results of task analysis, the required VR support (functional VR requirement) for each step in the task has been identified.

Sixth workshop:

In the sixth workshop (1 day), the results from the fifth workshop have been presented to selected staff from the industrial site. A step-by-step validation and review of the task details and the identified VR support took place. The result was a third validation of the results with focus on the functional VR requirements. These functional VR requirements have been grouped into groups of technical features for the purpose of defining the VR module required to realise these features as illustrated in Table **4.3**.

The entire process of requirements' validation and review is illustrated in the activity diagram presented in Fig. **6.5.**

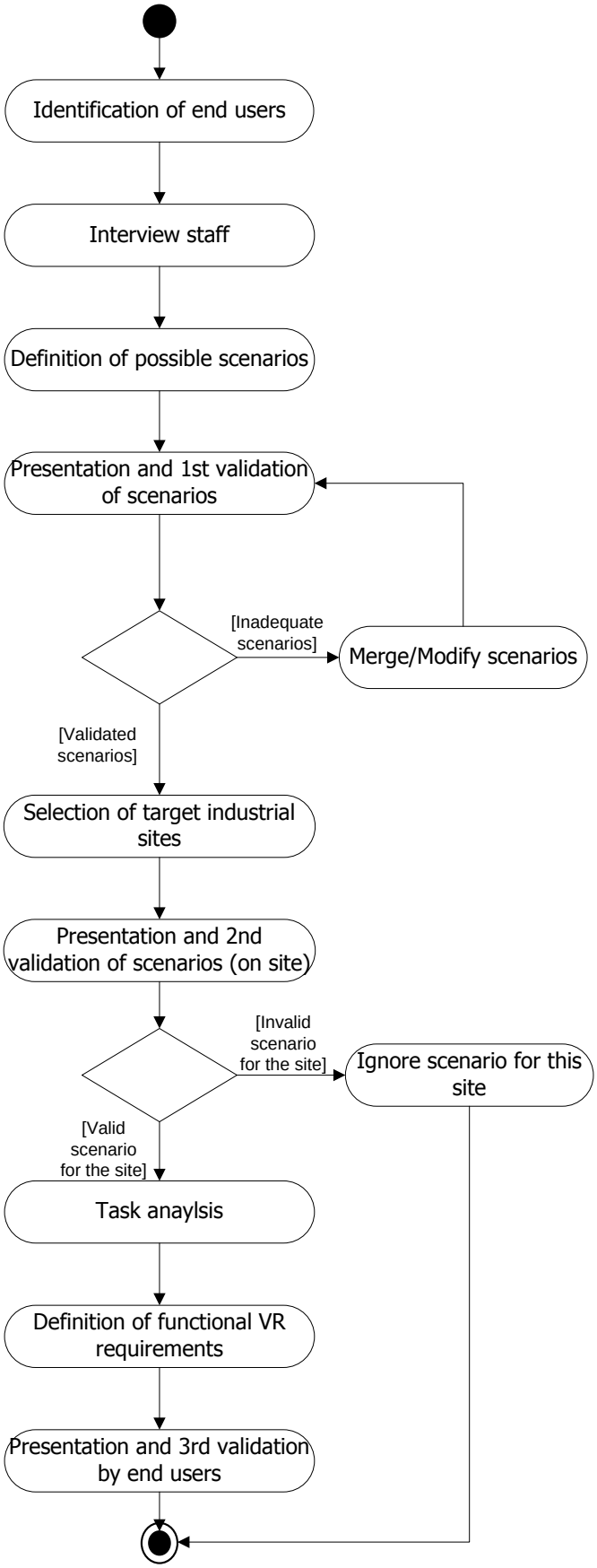


Fig. 6.5: Requirements validation and review

6.3 Validation of VR environment design

The proposed VR environment design (Chapter 5) is being implemented within the framework of the multinational research project mentioned in Section 2.3.3, Section 4.3 and Section 6.2.

An intermediate step before starting the implementation of the proposed design was a definition of the VR technical modules needed to realise the predefined functions. This work has been introduced in Section 4.7. The definition of these modules is based on the foundations achieved in the workshops mentioned in Section 6.2 which were confirmed by the industrial end users participating in the project.

It is worth mentioning, that the dynamics of the ongoing development process in the project lead to several adaptations and modifications in the proposed VR environment design to cope with further safety demands other than those identified in typical risk analysis applications.

Due to issues on data secrecy and confidentiality of project results, it is not possible to insert screenshots or similar proofs of implementation.

To illustrate how the VR environment is used as a medium for running safety scenarios and obtaining relevant data for risk and safety analysis, Table **6.6** provides an example of querying information after running the task "gas leakage detection" (the case study presented in Section 6.1) in the VR environment. In this example, the safety analyst is looking for the following information:

- A list of the persons and actors who run the task "gas leakage detection" (in the VR environment) on the first two days of the current week and acted as field operator (Experiment: standard gas leakage detection, task: gas leakage detection, actor: field operator);
- Error modes upon executing the operation "confirmation" of the task (operation: confirmation);
- Response time[30] of the actors who run the experiment during the operation "confirmation";
- Time of completing the entire task,

[30] Response time is defined here to be the time for the field operator, who located a leakage point, to report to control room operator.

- Possibilities of recovery.

Table 6.6: Example on information that can be retrieved (queried) after running a VR experiment

Person	**Actor**	**Error modes (operation: confirmation)**	**Response time (operation: confirmation)**	**Time of completing task (seconds)**	**Recovery**
A. Averageman	Field Operator	Later than	33	196	Plan 4
B. Wrongman	Field Operator	Other than	7	170	No Recovery
C. Goodman	Field Operator	No Error	29	188	N.A.
D. Newman	Field Operator	None	No value	404	Plan 4
E. Quickman	Field Operator	Sooner than	19	100	Plan 4

Assuming an ideal response time of 30 seconds and a period of 190 seconds for completing the task, the following knowledge is gained from the results of this experiment:

- The employee "A. Averageman" is performing on average and was able to confirm without large delays. His delay can be recovered by viable plan 4. (error mode: later than).

- The employee "B. Wrongman" made a wrong confirmation (error mode: other than), which does not allow any recovery. The reason for the wrong confirmation might be the quick confirmation of the leakage (7 seconds).

- The employee "C. Goodman" is performing very well (no error).

- The employee "D. Newman" is confused and finished the task with more than double of the average task time (error mode: none, i.e., operation is not performed).

- The employee "E. Quickman" is rushing to finish the experiment (error mode: sooner than).

Based on these results, the safety analyst makes recommendation on how to improve the performance of the employees, i.e., "D. Newman" should be trained further before doing field work, an appraisal should be conducted with the employee "B. Wrongman" since his results are frequently inadequate, the employee "E. Quickman" should

accompany the employee “E. Goodman” during field work and be educated to avoid quick reactions, etc.

In a similar manner, further data and information can be retrieved from different tasks and experiments executed by different persons and actors in the VR environment. The obtained information can be analysed and further used to enhance operators' familiarity with the operational tasks, improve operational procedures, identify human performance problems, recommend work improvements, identify training needs, etc.

7
Conclusions and outlook

The underlying work provided an integrated method for improving the risk analysis process by enriching it with human factors. It also proposed a VR environment design based on functional VR requirements that stem from industrial field works. The proposed VR environment can be used as an experimentation medium for extracting and evaluating human factors and risk analysis related data to compensate for unavailable data or validate existing ones.

The underlying work utilises enabling technologies to provide a link between safety (risks), human factors and industrial requirements. This link has been achieved via virtual reality (VR) as an enabling technology and a platform for integrating further enabling IT tools and modules (authoring tools, process simulators, event-based techniques, etc.).

7.1 Results and concluding remarks

A list of the results of the underlying thesis and the conclusion related to each result is provided below:

- Result 1: a HF methodology for supporting risk analysis which takes the human behaviour and performance into consideration. This methodology builds on limitations of existing approaches, e.g., ATHEANA, CREAM, THERP by providing:

    1. An explicit model of human performance for cognitive tasks;
    2. A comprehensible taxonomy of error modes and error causes that can be easily applied by safety analysts;
    3. A representation of the dynamic interaction between workplace factors and human performance;
    4. A consideration of the error detection and recovery processes.

The methodology provides a comprehensible tool for analysing human error in complex industries. Its primary objective is to help safety analysts to examine how operator performance may change in the course of an accident scenario. It should also enhance the communication between safety analysts and the cognitive science community in the analysis of human reliability in process control systems. The methodology has been taken as a reference for identifying the VR functional requirements (result 2).

This methodology has been validated on an operational task from the chemical process industry (gas leakage detection).

- Result 2: Identification of functional requirements and features specifications for supporting risk analysis work in a VR environment.

The definition of these requirements followed a user-centred design approach, i.e., end user needs that have been derived during field work on industrial sites, interviews and workshops with safety experts from the chemical process industry.

A set of 21 applicable safety scenarios have been shaped and validated. After detailing and validating the scenarios, a task analysis of the scenarios was carried out for the purpose of detailing the requirements and boundaries of each scenario step. The result was a non-exhaustive list of the most demanding end users requirements for a better performance of risk analysis in the domain industry.

Utilising the components of the proposed HF methodology (result 1), four major groups of functions have been defined:

1. Functions for errors in identification and interpretation;
2. Functions for errors in decision making and planning ;
3. Functions for error recovery;
4. Functions for representing work constraints.

After mapping the end users requirements to the listed functions, a further detailing of these functions into sub-functions and functionalities was performed. As a conclusion, a set of 57 major functionalities were extracted and classified as fundamental for supporting the performance of risk analysis work in a VR environment under the consideration of non-negligible HF aspects as confirmed by end users. These functional requirements have been used as a base for the VR environment design (result 3).

- Result 3: Proposing a VR environment design that supports risk and safety analysts in performing their analyses (based on result 1 and result 2). The following conclusions can be listed here:

    1. The need to translate the functional requirements (HOWs) into technical feature groups (HOWs) to enable deriving the appropriate system architecture;

2. The need to integrate specific modules and components into the VR platform to cover some identified functions, which do not belong to VR functionalities, e.g., authoring, analysing, linking to process simulator, etc.;

3. The need to have a scalable and modular design to gain more flexibility and expandability.

Based on that a system architecture that consists of the main VR part supported by five external modules for content authoring, linking the VR environment to external process simulators, monitoring the execution of procedures and rules of plant-specific behaviour, recording events and messages for post-analysis and analysing the data for further use by safety or risk analyst has been proposed.

The advantage of the proposed VR environment design is its end user- and application-oriented nature, i.e., it focuses on the needs of the target industry (chemical process industry) and the challenges faced by the end users employed within these industries.

7.2 Outlook

The following ideas for future work can be derived from the underlying work and its results:

1. The execution of further case studies for the purpose of validating the HF methodology (Chapter 3) in a formal risk analysis study. This requires the collaboration of at least one industrial partner from the research domain (chemical process industry) and the availability of plant facilities and personnel for interviews and analysis work during the period of performing the case study. Carrying out such an on-site case study would also serve the re-validation of the functional requirements and ensuring a better integratibility with the HF methodology.

2. Performing a dedicated research on piping and illustration diagrams (P&ID), technical specifications, interfacing possibilities with external read/write tools, etc. This would enhance the features of the proposed authoring module and enhance an automated generation of 3D content based on exiting P&ID illustrations and information.

3. Translating the underlying functional requirements and the proposed VR environment design into detailed technical software specifications for a structured implementation of the proposed system architecture.

4. Utilising the findings of the underlying thesis for other safety actions (rather than risk analysis), e.g., accident analysis, safety management and safety training. This can be achieved by applying the methodology to a case study which is relevant to one of these safety actions (or all) and reviewing the functional VR requirements to cover functions of importance for these actions.

5. Utilising the findings of the underlying thesis in areas of application with high demand on risk management (other than chemical process industry). A typical application area could be “IT infrastructures” where the developed HF methodology (Chapter 3) can be utilised to examine and analyse typical risks, their escalation scenarios and the role of the human in avoiding or minimising these risks.

Bibliography

Acosta, C.; Siu, N. (1993): Dynamic event trees in accident sequence analysis: Application to steam generator tube rupture. Reliability Engineering & System Safety, volume 41, pp. 135-154.

Amalberti, R. & Deblon, F. (1992): Cognitive modelling of fighter aircraft process control: A step towards an intelligent on-board assistance system. International Journal of Man Machine Studies, volume 36, pp. 639-671.

Augmented Inspection Team (AIT 1992): On site analysis of the human factors of an event: Loss of coolant and residual heat removal cooling at Prairie Island Unit 2. ATI-Report No 50-306/92-005US Nuclear Regulatory Commission, Washington DC.

Bainbridge, L. (1989): Cognitive processes and training methods. In L. Bainbridge & R. Quantanilla (Eds.) Developing Skills with Information Technology, New York: Wiley & Sons.

Banerjee, S. (2003): Industrial Hazards and Plant Safety. New York.

Bell, J. T.; Fogler, H. S. (1996): Preliminary Testing of a Virtual Reality Based Module for Safety and Hazard Evaluation. Proceedings of the 1996 Illinois / Indiana ASEE Sectional Conference, March. Peoria.

Blümel, E.; Müller, G.; Salem, W.; Schenk, M. (2005): Technology Enhanced Training at Workplace: A Virtual Reality Based Training System for the Technical Domain. Proceedings of the first International Conference on e-Business and e-Learning, pp. 57-62. Amman.

Blümel, E.; Salem, W.; Schenk, M. (2003): Using Virtual Reality in In-Factory Training: Adding More Value to the Production System. proceedings of the 36th CIRP-International Seminar on Manufacturing Systems, pp. 219-224. Saarbruecken.

Bohmann G. (1999): Virtual Reality - Sinnvolle Anwendung oder technische Spielerei? Universität Osnabrück. Osnabrück.

Burdea, G.; Coiffet, P. (2003): Virtual Reality Technology. 2nd ed., New York.

Cacciabue, P. C. (2000): Human factors impact on risk analysis of complex systems. Journal of Hazardous Materials, Volume 71, Number 1, pp. 101-116.

Cacciabue, P. C. (2001): Survey of Human Reliability Methods for Safety Assessment and Risk Management, Human Factors Sector European Commission, Joint Research Centre. Ispra.

Cacciabue, P. C. (2004): Guide to Applying Human Factors Methods. London.

Card, S.; Moran, T. P.; Newell, A. (1983): The Psychology of Human-Computer Interaction. Hillsdale.

Centre for Chemical Process Safety (CCPS 2004): Guidelines for Preventing Human Error in Process Safety. New York.

Chorafas, D. N. (2004): Operational Risk Control With Basel II: Basic Principles and Capital Requirements. Oxford. (eBook, http://www.netLibrary.com/urlapi.asp?action=summary&v=1&bookid=10469)

Chronéer, D. (2005): Product Development in Process Industry – Changes and consequences. Luleå.

Cojazzi, G.; Cacciabue. (1994): The DYLAM approach for the reliability analysis of dynamic systems. In T. Aldemir, N.O. Siu, A. Mosleh, P.O. Cacciabue & B.G. Goktepe (Eds.), Reliability and Safety Assessment of Dynamic Process Systems, NATO ASI Series F. Vol. 120, Berlin: Springer-Verlag.

Colombo, S. (2006): VIRTHUALIS Project: a paradigm shift in using and developing 3D real-time applications for safety purposes. In: Schenk, M (Hrsg.): Tagungsband der 9. IFF-Wissenschaftstage - Virtual Reality und Augmented Reality zum Planen, Testen und Betreiben technischer Systeme, pp. 173-180. Magdeburg.

Cooper, S. E.; Ramey-Smith, A. M.; Wreathall, J.; Parry, G. W.; Bley, D. C.; Luckas, W. J.; Taylor, J. H.; Barriere, M. T. (1996): A technique for human error analysis (ATHEANA). Washington (NUREG/CR-6350).

Dechy, N.; Bourdeaux, T.; Ayrault, N; Kordel, M.; Le Coze, J. (2004): First lessons of the Toulouse ammonium nitrate disaster. Journal of Hazardous Materials, volume 111, pp. 131–138.

Dhilon, B., S. (2004): Reliability, Quality, and Safety for Engineers. Florida.

Diaper, D. (1989): Task Analysis for Human Computer Interaction. Chichester.

Dien, Y.; Liory, M.; Montmayeul, R. (2004): Organisational accidents investigation methodology and lessons learned. Journal of Hazardous Materials, volume 111, pp. 147–153.

Dougherty, E. (1993): Context and human reliability analysis. Reliability Engineering & System Safety, volume 41, pp. 25-47.

Dougherty, E. M. (1990): Human Reliability Analysis - where shouldst thou turn? Reliability engineering and System Safety, volume 29, pp. 283-299.

Ebert, C.; Dumke, R. (2007): Software Measurements - Establish, Extract, Evaluate, Execute. Berlin/Heidelberg.

Edwards, E. (1988): Introductory overview, in E. L. Wiener, and D. C. Nagel (Eds.), Human Factors in Aviation, pp. 3-25. San Diego. Elsevier. New York.

Embrey, D.; Kontogiannis, T.; Green, M. (1994): Guidelines for Reducing Human Error in Process Operations. New York: Centre for Chemical Process Safety.

European Commission (1998): VR for Europe – Industrial Application of VR. Brussels.

European Commission (2008): Enterprise - SME Definition. http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/index_en.htm. 15 July 2008.

European Communities (Eurostat Unit D6) (2004): Work and health in the EU, A statistical portrait. Luxembourg.

Experton-Group (2009): Marktentwicklung für Outsourcing – Deutschland 2007-2010. http://www.experton-group.de/fileadmin/experton/press/2008/pm-2008-07-22_Outsourcing_Sourcingmodelle.pdf. 19 February 2009.

Forester, J.; Bley D.; Cooper S.; Lois E.; Siu N.; Kolaczkowski A.; Wreathall J. (2004): Expert elicitation approach for performing ATHEANA quantification. Reliability Engineering and System Safety, volume 83, pp. 207–220.

Fragniere, E.; Sullivan, G. (2006): Risk Management: Safeguarding Company Assets. 1st ed., Boston.

Frensch, P. A.; Funke, J. (1995): Complex Problem Solving: The European Perspective. New Jersey: Lawrence Erlbaum Associates.

Fujita, Y.; Hollnagel, E. (2004): Failures without errors: quantification of context in HRA. Reliability Engineering and System Safety, volume 83, number 2, pp. 145-151.

Gabbard, J. L.; Hix, D.; Swan, J. E. (1999): User-centred design and evaluation of virtual environments. IEEE Computer Graphics and Applications, vol. 19, pp. 51- 59.

Gertman, D. I.; Haney, L. N.; Siu, N. (1996): Representing context, cognition, and crew performance in a shutdown risk assessment. Reliability Engineering & System Safety, 52, 261-278.

Gertman, D. I.; Blackman, H. S.; Haney, L. N.; Seidler, K. S.; Hahn, H. A. (1992): INTENT: A method for estimating failure rates for decision based errors. Reliability Engineering & System Safety, volume 35, pp. 127-136.

Gertman, D. I.; Blackman, H.S. (1993): Human reliability & safety analysis data handbook. New York et al.

Goldstein, F. C.; Levin, H. S. (1987): Disorders of reasoning and problem-solving ability. In Meier, M.; Benton, A.; Diller, L. (Eds.): Neuropsychological rehabilitation, pp. 327-354. New York.

Gounelle, C.; Cabon, P.; Burkhardt, J.-M.; Couix, S.; Fabre, D.; Anastassova, M.; Salem, W.; Colombo, S. (2007): Integrating Human Factors approaches with Virtual Reality for Safety in the VIRTHUALIS project. Virtual Reality International Conference (VRIC) . Laval.

Grau, O.; Broszio, H. (1999): Vorstudie über Potentiale und Chancen zur Entwicklung Hannover als VR-Standort. Technologie-Centrum Hannover GmbH. Hannover.

Haller, M.; Kurka, G.; Volkert, J.; Wagner, R. (1999): omVR - A safety training system for a virtual refinery. Proceedings of ISMCR99, Topical Workshop on Virtual Reality and Advanced Human-Robot Systems, pp. 291-298. Japan.

Halpern, D. (2003): Thought & Knowledge: an introduction to critical thinking. Mahwah.

Hammond, K. R.; Hamm, R. M.; Grassia, J.; Rearson, T. (1987): Direct comparison of the efficacy of intuitive and analytical cognition in expert judgment. IEEE Transactions on Systems, Man, and Cybernetics, SMC-17, 753-770.

Haney, L. N.; Blackman, H. S.; Bell, B. J.; Rose, S. E.; Hesse, D. J.; Minton, L. A.; Jenkins, J.P. (1989): Comparison and application of quantitative human reliability analysis methods for the risk method integration and evaluation program (RMIEP) (NUREG/CR-4835). Washington.

Harms-Ringdahl, L. (2004): Relationships between accident investigations, risk analysis, and safety management. Journal of Hazardous Materials, Volume 111, pp.13-19.

Hollnagel, E. (1993): Human reliability analysis: Context and control. London.

Hollnagel, E. (1998): Cognitive Reliability and Error Analysis Method. 1st ed., Oxford et al.

Hollnagel, E. (2004): Barriers and Accident Prevention. Hamsphire.

Hollnagel, E.; Wreathall, J. (1996): HRA at the turning point? In P. C. Cacciabue & I. Papazoglou (Eds.), Probabilistic safety assessment and management. Berlin.

Institution of Chemical Engineers (IChemE 2008): Hazards XX: Process Safety and Environmental Protection, Harnessing Knowledge, Challenging Complacency. Warwickshire.

International Electrotechnical Commission (IEC) (2006): IEC 60300-3-9 Ed. 2.0: Dependability management - Part 3-9: Application guide - Risk analysis of technological systems. Geneva.

INVENSYS 2008: Dynsim. http://ips.invensys.com/en/products/processdesign/Pages/Dynsim.aspx

Iwata, H. (2003): Food Simulator. Emerging Technologies-SIGGRAPH 2003. San Diego. (http://www.siggraph.org/s2003/conference/etech/food.html. 15 July 2008).

Johnsen, S. O.; Bjørkli, C.; Steiro, T.; Fartum, H.; Haukenes, H.; Ramberg, J.; Skriver, J. (2008): CRIOP®: A scenario method for Crisis Intervention and Operability analysis. SINTEF Technology and Society (SINTEF A4312). Trondheim.

Johnson, A. G. (2003): The Blackwell dictionary of sociology: a user guide to sociological language. 2nd ed., Malden et al.

Johnson, P. (1991): User interaction: a framework to relate Tasks, Users, and Design. In H.J. Bullinger (Ed.), HCI91. Stuttgart.

JRC (2006): Major Accident Reporting System (MARS). http://mahbsrv.jrc.it/mars/Default.html. 25 November 2006.

Kanse, L.; van der Sschaaf, T. (2001): Recovery from failures in the Chemical process industry. International Journal of Cognitive Ergonomics, 5, 199-211.

Karaseitanidis, I.; Amditis, A.; Patel H.; Sharples S.; Bekiaris E.; Bullinger A.; Tromp J. (2006): Evaluation of virtual reality products and applications from individual, organisational and societal perspectives – The "VIEW" case study". International Journal of Human-Computer Studies, volume 64, number 3, pp 251-266.

Karwowski, W. (2006): International Encyclopedia of Ergonomics and Human Factors. London et al.

Kim, I. S. (2001): Human reliability analysis in the man-machine interface design review. Annuals of Nuclear Energy, volume 28, pp. 1069-1081.

Kim, J.W.; Jung, W.; Ha, J. (2004): AGAPE-ET: A methodology for human error analysis of emergency tasks. Risk Analysis, 24, 1261-1277.

Kim, M. C.; Seong, P. H.; Hollnagel, E. (2006): A probabilistic approach for determining the control mode in CREAM. Reliability Engineering and System Safety, volume 91, pp. 191-199.

Kirwan, B. (1994): A guide to practical HRA. London.

Kirwan, B. (1996): The validation of three Human Reliability Quantification Techniques – THERP, HEART and JEHDI: Part 1 – technique description and validation issues. Applied Ergonomics, volume 27, number 6, pp. 359-373.

Kirwan, B. (1998): human error identification techniques for risk assessment of high risk systems – Part 2: towards a framework approach. Applied Ergonomics, volume 29, number 5, pp. 299-318.

Kirwan, B.; Ainsworth, L. K. (1992): A guide to task analysis. London.

Klein, G. A.; Orasanu, J.; Calderwood, R.; Zsambok C. E. (1993): Decision Making in Action: Models and Methods. New Jersey: Ablex Publishing.

Klocke, F.; Straube, A. M.; Pypec, C. (2003): Vorsprung durch Virtual Reality. Fraunhofer IPT. Aachen.

Kongsberg (2008): D-SPICE Dynamic simulation tool. http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/89E63E039C7B9AC9C12572440047326B?OpenDocument

Konstandinidou, M.; Nivolianitou, Z.; Kiranoudis, C.; Markatos, N. (2006): A fuzzy modelling application of CREAM methodology for human reliability analysis. Reliability Engineering and System Safety, volume 91, pp. 706-716.

Kontogiannis, T. (1996): Stress and operator decision making in coping with emergencies. International Journal of Human-Computer Studies, 45, 75-104.

Kontogiannis, T. (1997): A framework for the analysis of cognitive reliability in complex systems: a recovery centred approach. Reliability Engineering and System Safety, volume 58, pp. 233-248.

Kontogiannis, T. (1999): User strategies in recovering from errors in man machine systems. Safety Science, volume 32, pp. 49-68.

Kontogiannis, T.; Embrey, D. (1997): A user-centred design approach for introducing computer-based process information systems. Applied Ergonomics, volume 28, number. 2, pp. 109-119.

Lager, T. (2002): Product and process development intensity in process industry: A conceptual and empirical analysis of the allocation of company resources for the development of process technology. International Journal of Innovation Management, volume 6, number 2, pp.105-130.

Leveson, N. (1995): Safeware: System Safety And Computers: A Guide To Preventing Accidents And Losses Caused By Technology. Massachusetts.

Loupos, K.; Christopoulos, D.; Vezzadini, L; Hoekstra, W.; Salem, W.; Chung, P. (2007a): Application Of VR And HF Technologies For Improving Industrial Safety. Proceedings of 5th International Conference New Horizons in Industry, Business and Education. Rhodes Island.

Loupos, K.; Vezzadini, L; Hoekstra, W.; Salem,W.; Chung, P.; Bimpas, M. (2007b): VR, HF and Rule-Based Technologies Applied and Combined for Improving

Industrial Safety. In Constantine Stephanidis (Ed.): Universal Access in Human-Computer Interaction, volume 4555, part III, pp. 676-680. Berlin-Heidelberg.

Ludewig, J.; Lichter, H. (2007): Software Engineering - Grundlagen, Menschen, Prozesse, Techniken. 1st ed., Heidelberg.

Marseguerra, M.; Zio E.; Librizzi, M. (2006): Quantitative developments in the cognitive reliability and error analysis method (CREAM) for the assessment of human performance in "Annals of Nuclear Energy", pp. 894–910.

Marsot, J.; Ciccotelli, J.; Gardeux, F. (2004): Virtual environment for Safe Design. 35th International Symposium on robotics (ISR 2004). Paris.

Martz, P. (2007): OpenSceneGraph Quick Start Guide. California.

Mayer, J.; Melzer, I.; Schweiggert, F. (2003): Lightweight Plug-In-Based Application Development. In: Lecture Notes in Computer Science, pp. 87-102. Volume 2591, Berlin/Heidelberg.

McDermott, R. E..; Mikulak, R. J.; Beauregard, M. R. (2008): The Basics of FMEA. 2nd ed., Florida et al.

Meister, D. (1995): Cognitive behaviour of nuclear power operators. International Journal of Industrial Ergonomics, volume 16, pp. 109-122.

Merriam-Webster (2008): Methodology. http://www.merriam-webster.com/dictionary/methodology. 14 July 2008.

Merriam-Webster (2009): Methodology. http://www.merriam-webster.com/dictionary/method. 13 February 2009.

Meyer, O.R.; Hill, S.G.; Steinke, W.G. (1992): Studies of human performance during operating events 1990-1992. NUREG/CR-5953. US Nuclear Regulatory Commission, Washington DC.

Mo, J.; Crouzet, Y. (1996): Human error tolerant design for air-traffic control systems. In P. C. Cacciabue & I. A. Papazoglou (Eds.): Probability Safety Assessment and Management' 96, PSAM-III, Crete, Greece, June 24-28, 1996.

Nivolianitou, Z.; Kefalas, D. (2005): S2S: A Gateway for Plant and process safety. 1st edition, Athens.

OPC Foundation (2008): About OPC. http://www.opcfoundation.org/Default.aspx/01_about/01_whatis.asp?MID=AboutOPC. 22 July 2008.

Papadakis, G.A.; Amendola, A. (Eds.) (1997): Guidance on the Preparation of a Safety Report to Meet the Requirements of Council Directive 96/82/EC (Seveso II). Luxembourg.

Patrick J. (1993): Cognitive aspects of fault-finding training and transfer. Le Travail Humain, 56, 187- 209.

Payne, S. J.; Green, T.R.G. (1986): Task-action grammars: a model of the mental representation of task languages, Human Computer Interaction, volume 19, number 1, pp. 73.

Perrow, H. (1984): Normal Accidents: Living with High Risk Technologies. New York: Basics Books.

Pimentel, K.; Teixeira, K. (1995): Virtual Reality: through the new looking glass. 2nd ed., New York.

Pyy, P. (2000): Human reliability analysis methods for probabilistic safety assessment. VTT Technical Research Centre of Finland, VTT Publications 422.

Rankin, W.; Krichbaum, L. (1998): Human Factors in aircraft maintenance, Integration of Recent HRA Developments with Applications to Maintenance in Aircraft and Nuclear Settings. Seattle.

Rasmussen J. (1986): Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering. Amsterdam: North-Holland.

Rasmussen, J.; Pejtersen, A. M.; Goodstein, L. P. (1994): Cognitive Systems Engineering. New York.

Rautenstrauch, C. (1997): Effiziente Gestaltung von Arbeitsplatzsystemen: Konzepte und Methoden des persönlichen Informationsmanagements. Bonn et al.

Reason, J. T. (1990): Human Error. Cambridge, MA: Cambridge University Press.

Reinhart, G.; Patron, C.; Meier, P. (2002): Virtual Reality und Augmented Reality in der Montage. Wt Werkstattstechnik online, Jg. 92.

Research and Technology Organisation – North Atlantic Treaty Organisation (RTO-NATO) (2005): Virtual Environments for Intuitive Human-System Interaction. Neuilly-Sur-Seine Cedex.

Ritter, F. E.; Shadbolt, N. R.; Elliman, D.; Young, R.; Gobet, F.; Baxter, G. D. (2001): Techniques for modelling human performance in synthetic environments: A supplementary review, Human Systems Information Analysis Centre. Ohio. (Tech. Report No. 62. ESRC CREDIT, Department of Psychology, University of Nottingham).

Ritzer, G. (2007): The Blackwell encyclopedia of sociology. 1st ed., Malden et al.

Rizzo, A.; Ferrante, D.; Bagnara, S. (1995): Handling human error. In J. M. Hoc, P. C. Cacciabue & E. Hollnagel (Eds.) Expertise and Technology: Cognition & Human Computer Interaction, New Jersey: Lawrence Erlbaum Associates.

Robson, M. G.; Toscano, W. A. (2007): Risk Assessment for Environmental Health. 3rd ed., New York et al.

Roth, E. M.; Mumaw, R. J.; Lewis, P. M. (1994): An empirical investigation of operator performance in cognitively demanding simulated emergencies. NUREG/CR-6208, US Nuclear Regulatory Commission, Washington DC.

Rouhiainen, V.; Gunnerhed, M.: Development of international risk analysis standards. Safety Science, volume 40, pp. 57-67.

Rouse, W. B.; Rouse, S. H. (1983): Analysis and classification of human error. IEEE Transactions on Systems, Man, and Cybernetics, SMC-14, 539-549.

Sadgrove, K. (2005): The Complete Guide To Business Risk Management. 2nd ed., Hampshire.

Salem, W. (2003): eTraining - VR-Gestütztes Training von Servicepersonal und Instandhaltungstechnikern. Tagungsband der 6. IFF-Wissenschaftstage - Virtuelle Plattformen. Magdeburg.

Salem, W. (2004): Technology enhanced training at workplace: an interactive training system for manufacturing enterprises. Book of abstracts of 10th international conference on technology supported learning & training, pp. 376-379. Berlin.

Salem, W. (2008): Combining VR Technology and Human Factors Methods for Supporting Risk Analysis. Proceedings of 3rd International Conference on Information and Communication Technologies: From Theory To Application. Damascus.

Salem, W.; Colombo, S.; Cabon, P.; Kissner, H. (2006): Enhancing the Trainees' Awareness in a Virtual Training Environment. Proceedings of the 1st International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Salem, W.; Kissner, H. (2007): Best Practice in Virtual Reality Based Training. Proceedings of the 2nd International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Salem, W.; Kontogiannis, T. (2007): A framework for utilising features and requirements of VR training environments to support the risk and accident analysis in industrial plants. Proceedings of the 2nd International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Salvendy, G. (1997): Handbook of human factors and ergonomics. 2nd ed., New York.

Schatrik, S. J.; Karmis, M.; Agioutantis, Z. (2003): Methodology of incident recreation using virtual reality. SME Annual Meeting. Ohio.

Schraagen, J. M.; Chipman, S. F.; Shalin, V. J. (2000): Cognitive Task Analysis. Mahwah.

Shell International Exploration and Production B.V. (Shell) (1995a): Quantitative Risk Assessment. Revision 0 (EP950352).

Shell International Exploration and Production B.V. (Shell) (1995b): Overview Hazards and Effects Management Process. Revision 0 (EP950300).

Shell International Exploration and Production B.V. (Shell)(1995c), HAZID. Revision 0 (EP950312).

Shell International Exploration and Production B.V. (Shell) (1995d), HAZOP. Revision 0 (EP950313).

Shepeherd, A. (1989): Analysis and training of information technology tasks, In Diaper, D. (eds) Task Analysis for Human Computer Interaction, pp. 15-54. Chichester.

Shepherd, A. (1998): HTA as a framework for task analysis. Ergonomics, volume 41, number. 11, pp. 1537-1552.

Shorrock, S. T.; Kirwan, B. (2002): Development and application of a human error identification tool for air traffic control. Applied Ergonomics, volume 33, pp. 319-336.

Shorrock, S.T.; Straeter, O. (2006): A framework for managing system disturbances and insights from air traffic management. Ergonomics, 49, 1326-1344.

Skinner, B. F. (1957): Verbal Behaviour. New York.

Smidts, C.; Shen, S.H.; Mosleh, A. (1997): The IDA cognitive model for the analysis of nuclear power plant operator response under accident conditions: Part I: problem solving and decision making models. Reliability Engineering & System Safety, 55, 51-71.

Spurgin, A. J.; Moieni, P. (1991): An evaluation of current human reliability assessment methods, in G. Aposolakis (Eds.), probabilistic safety assessment and management,

Stamatis, D. H (2003): Failure Mode and Effect Analysis: FMEA from Theory to Execution. 2nd ed., Milwaukee, Wisconsin.

Stanton, N.; Salmon, P.; Walker, G.; Baber, C.; Jenkins, D. (2005): Human Factors Methods - A Practical Guide for Engineering and Design. Hampshire.

StarUML 2009: StarUML 5.0 User guide (StarUML Overview). http://staruml.sourceforge.net/docs/user-guide(en)/ch01.html. 26 February 2009.

Streffer, C.; Bolt, H.; Folllesdal, D.; Hall, P.; Hengstler, J.; Jakob, P.; Oughton, D.; Prieß, K.; Rehbinder, E.; Swaton, E. (2004): Low Dose Exposures in the Environment – Dose Effect Relations and Risk Evaluation. Berlin-Heidelberg.

Su, Y.; Govindaraj, T. (1986): Fault diagnosis in a large dynamic system: experiments on a training simulator. IEEE Transactions on Systems, Man and Cybernetics, SMC-6, 240-255.

Swain, A. D. (1990): Human reliability analysis: needs, status, trends and limitations. Reliability Engineering and System Safety, volume 29, number 3, pp. 301-313.

Swain, A. D.; Guttman, H. E. (1983): Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278). Albuquerque.

Swain, A.D. (1989): Comparative evaluation of methods for human reliability analysis (GRS-71). Köln et al.

Thompson, C.M.; Cooper, S.E.; Kolaczkowski, A.M.; Bley, D.C.; Forester, J.A.; Wreathall, J. (1997): The Application of ATHEANA: A Technique for Human Error Analysis. IEE Sixth Annual Human Factors Meeting, Orlando-Florida.

Treasury Board of Canada Secretariat (TBCS) (2004): Integrated Risk Management – Implementation Guide. Ottawa.

Trucco, P.; Leva, M.C. (2007): A probabilistic cognitive simulator for HRA studies (PROCOS). Reliability Engineering & System Safety, volume 92, pp. 1117-1130.

US Nuclear Regulatory Commission (USNRC) (2000), Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA). Revesion 1, Washington. (NUREG-1624).

US Nuclear Regulatory Commission (USNRC) (2005): Good Practices for Implementing Human Reliability Analysis. Washington (NUREG-1792).

Villa-Uriol, M; Kuester, F.; Garcia-Pan~ella, O.; Fernandez Munuera, J. A. (2005): Avatar-centric Risk Evaluation. International Symposium on Multimedia (ISM 2005). Irvine-California.

Vincoli, J. W. (2006): Basic Guide to System Safety. 2nd ed., Florida et al.
Wikipedia (2008a): Problem solving. http://en.wikipedia.org/wiki/Problem_solving. 15 July 2008.
Wikipedia (2008b): OLE for process control. http://en.wikipedia.org/wiki/OLE_for_process_control. 22 July 2008.
Wiktionary (2008a): Methodology. http://en.wiktionary.org/wiki/methodology. 14 July 2008
Wiktionary (2008b): taxonomy. http://en.wiktionary.org/wiki/taxonomy. 14 July 2008.
Winkler, T.; Michalek, D.; Määttä, T.; Colombo, S. (2005): VR technology in the life cycle of technical artificats: a possibility of methodology transfer within high risk industries. Proceedings of the KOMTECH conference. Zakopane.
Woods, D. D.; Pople. H. E.; Roth, E. M. (1990): The cognitive environment simulation as a tool for modelling human performance and reliability. NUREG-CR-5213, Nuclear Regulatory Commission, Washington DC.
Woods, D. D.; Roth, E.; Pople, H. (1987): Cognitive environment simulation: system for human performance assessment. Washington (NUREG-CR-4862).
Yanagida, Y.; Kawato, S.; Noma, H.; Tomono, A.; Tetsutani, N. (2004): Projection-Based Olfactory Display with Nose Tracking. Proceedings of IEEE Virtual Reality, pp. 43-50. Chicago.
Yu, J.; Yanagida, Y.; Kawato, S.; Tetsutani, N. (2003): Air Cannon Design for Projection-Based Olfactory Display. Proceedings of 13th International Conference on Artificial Reality and Telexistence. Tokyo.

List of Publications

Salem, W.; Rautenstrauch, C.; Jallad, N.: A System Architecture of a User-Centred Application for Improving Safety Analysis. Proceedings of the 5th International Conference on Innovations in Information Technology (IT Innovation'08, 16-18 December 2008). Al Ain - United Arab Emirates.

Kontogiannis, T; Salem, W. (2008): INCORECT/DET: 'Investigating Cognitive and Recovery Tasks' with 'Dynamic Event Trees': A Framework for Human Reliability Analysis in Process Control Industries. International Journal of Industrial Ergonomics (Submitted).

Salem, W. (2008): Combining VR Technology and Human Factors Methods for Supporting Risk Analysis. Proceedings of 3rd International Conference on Information and Communication Technologies: From Theory To Application. Damascus.

Asfoura, E.; Jamous, N.; Salem, W. (2008): The economic classification of E-Learning business models. Proceedings of the 3rd International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Salem, W.; Kissner, H. (2007): Best Practice in Virtual Reality Based Training. Proceedings of the 2nd International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Salem, W.; Kontogiannis, T. (2007): A framework for utilising features and requirements of VR training environments to support the risk and accident analysis in industrial plants. Proceedings of the 2nd International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Loupos, K.; Christopoulos, D.; Vezzadini, L; Hoekstra, W.; Salem, W.; Chung, P. (2007): Application Of VR And HF Technologies For Improving Industrial Safety. Proceedings of 5th International Conference New Horizons in Industry, Business and Education. Rhodes Island.

Loupos, K.; Vezzadini, L; Hoekstra, W.; Salem,W.; Chung, P.; Bimpas, M. (2007): VR, HF and Rule-Based Technologies Applied and Combined for Improving Industrial Safety. In Constantine Stephanidis (Ed.): Universal Access in Human-Computer Interaction, volume 4555, part III, pp. 676-680. Berlin-Heidelberg.

Gounelle, C.; Cabon, P.; Burkhardt, J.-M.; Couix, S.; Fabre, D.; Anastassova, M.; Salem, W.; Colombo, S. (2007): Integrating Human Factors approaches with Virtual Reality for Safety in the VIRTHUALIS project. Virtual Reality International Conference (VRIC). Laval.

Salem, W.; Colombo, S.; Cabon, P.; Kissner, H. (2006): Enhancing the Trainees' Awareness in a Virtual Training Environment. Proceedings of the 1st International Conference on Interactive Mobile and Computer Aided Learning (IMCL). Amman.

Gounelle, C.; Burkhardt, J. M.; Cabon, P.; Salem, W. (2006): Improving Safety with VR technology through a user-centred design approach. In: Schenk, M (Hrsg.):

Tagungsband der 9. IFF-Wissenschaftstage - Virtual Reality und Augmented Reality zum Planen, Testen und Betreiben technischer Systeme, pp. 183-187. Magdeburg.

Vezzadini, L.; Chung, P.; Shang, X.; Loupos, K.; Salem, W. (2006): The integration of VR and rule-based technologies to improve safety. In: Schenk, M (Hrsg.): Tagungsband der 9. IFF-Wissenschaftstage - Virtual Reality und Augmented Reality zum Planen, Testen und Betreiben technischer Systeme, pp. 191-198. Magdeburg.

Blümel, E.; Müller, G.; Salem, W.; Schenk, M. (2005): Technology Enhanced Training at Workplace: A Virtual Reality Based Training System for the Technical Domain. Proceedings of the first International Conference on e-Business and e-Learning, pp. 57-62. Amman.

Salem, W. (2004): Technology enhanced training at workplace: an interactive training system for manufacturing enterprises. Book of abstracts of 10th international conference on technology supported learning & training, pp. 376-379. Berlin.

Salem, W. (2004): Virtual Reality: a Promising Technology for the Arabic eLearning and eTraining Market. In: 7th German-Arabic Economic Forum (2-4 June 2004). Berlin.

Blümel, E.; Salem, W.; Schenk, M. (2003): Using Virtual Reality in In-Factory Training: Adding More Value to the Production System. Proceedings of the 36th CIRP-International Seminar on Manufacturing Systems, pp. 219-224. Saarbruecken.

Salem, W. (2003): eTraining - VR-Gestütztes Training von Servicepersonal und Instandhaltungstechnikern. In: Schenk, M. (Hrsg.): Tagungsband der 6. IFF-Wissenschaftstage - Virtuelle Plattformen. Magdeburg.

Annexes

A HAZID and HAZOP methods

HAZID (Shell 1995b)

Objective

To identify at an early stage of a project or a development plan the major Hazards that must be removed or managed. Unlike event trees (Annex B), HAZID analysis does not provide estimations or calculations on risk probabilities. Figured estimations are only provided for the priority of the risk under consideration as illustrated in Table **A.1** (sixth column)

Method

A multi-disciplined team review of the overall project (i.e., product, process or a part of it) including infrastructure, plant design and operation together with its impact on the local environment. The study uses a step-by-step methodology and a checklist of guide words to identify hazards and assess the influence these hazards may have on the project development and design philosophy. The scope will encompass both current and future life cycle issues.

Information Required (Input)

Information pack on the project, its potential scope and related environmental issues. All available conceptual and preliminary drawings and development plans.

Information delivered (Output)

Information on major identified hazards together with recommendations in priority order. This information can be entered in the Hazards and Effects Register for further processing.

Documentation of the results

The results of the team review (brainstorming) are entered into HAZID-sheets for further analysis.

Example

Table **A.1** shows an example of a HAZID-sheet with an entry about a possible top event from the process industry domain (rim fire with possibility of escalation) (Shell 1995c).

HAZOP (Shell 1995b)

Objective

To identify the Hazards, Effects and Operability problems relating to the process design and intended method of plant operation which must be removed or managed in the operation. Similar to HAZID, HAZOP analyses does not provide estimations or calculations on risk probabilities. Figured estimations are only provided for the priority of the risk under consideration as illustrated in Table **A.1** (eighth column).

Sequence for conducting a HAZOP study

- Coarse HAZOP - Early study to identify basic flaws in design which would be costly to correct later.
- Main HAZOP - Primary vehicle for identification of hazards, effects and operability problems. Main HAZOP is performed when the front end engineering design is almost complete so that systems can be covered in detail.
- Final HAZOP - Coverage of those systems which were not (sufficiently) considered in the Main HAZOP, e.g. vendor data, and a formal review of action responses to previous HAZOPs.
- Procedural HAZOP - Identification of hazards and operability problems arising from procedures such as commissioning, maintenance and other non-continuous procedures.

Method

A multi-disciplined team review using a structured step-by-step methodology with the application of parameter and guide word combinations to sections (nodes) of the system to identify hazards and operability problems normally with a facility but also with procedures.

- Coarse HAZOP - Large nodes concentrating on major issues, requires a team of experienced senior engineers. The recommendations from a Coarse HAZOP may involve significant changes to the design.
- Main HAZOP - Rigorous application of the technique to relatively small nodes which requires a team of experienced engineers with extensive project experience.

- Final HAZOP - Rigorous application of the technique to relatively small nodes which requires similar team as for Main HAZOP with the addition of vendor representatives. At this stage recommendations should be concentrated on "will it work" rather than "it would improve the safety of design to have".

- Procedural HAZOP - Application of specialised guide words to operating procedures which requires a team similar to that for main HAZOP with greater emphasis on operational personnel.

Information Required (Input)

- Coarse HAZOP: Basic layouts, process flow schemes (PFSs) and any operating/control philosophies that are available.

- Main HAZOP: Process and Utility Process Engineering Flow Schemes, (PEFSs, UEFSs) Operating and Control Philosophies, Cause and Effect Diagrams, Process Safeguarding Drawings, line lists, alarm and trip settings.

- Final HAZOP: EFSs and Vendor drawings, data, previous HAZOP findings and responses and any design changes since last HAZOP.

- Procedural HAZOP: As for Main HAZOP and Operating Procedures.

Information delivered (Output)

- Coarse HAZOP - Recommendations for adjustment to design options, QRA studies and other supporting investigations. A risk ranking may be given to assist in prioritising the actions. This list may be incorporated into the Hazards and Effects register for the project.

- Main HAZOP - Recommendations to amend the design to remove or reduce hazards and operability problems. Categorisation of the recommendations into approximate risk groups to assist in prioritising the actions. This list should be used to update the Hazard register for the project.

- Procedural HAZOP - Recommendations to amend the procedures to remove or reduce hazards and operating problems. This will allow Safety Critical Procedures/Operations to be identified.

Documentation of the results

The results of the team review (brainstorming) are entered into HAZOP-sheets for further analysis.

Example

Table **A.2** shows an example of a HAZOP-sheet with an entry from the process industry domain (a possible deviation in operating one of the plant equipments (tank)) (Shell 1995d).

Table A.1: An example of a HAZID- sheet (Shell 1995 c)

Category	Natural & Environmental Hazards

Guide Word	**Potential Hazards & Effects**	**Threats**	**Controls**	**Development Phase**	**P***	**No.**
Lightning	Rim fire on oil storage tanks with possible escalation to loss of inventory and major fire.	Lightning is a threat to all elevated or isolated parts of the plant. The incidence of lightning is high in this location.	Existing conventional lightning conductors have been prone to failure. Determine what novel equipment or techniques are available and their benefits. If lightning strikes cannot be prevented determine optimum tank design to prevent rim fires and fire fighting techniques	Initial project development phase	2	5

* P (Priority): 1=High Severity 2=Medium Severity 3=Low Severity

Table A.2: An example of a HAZOP- sheet (Shell 1995d)

Parameter: Flow

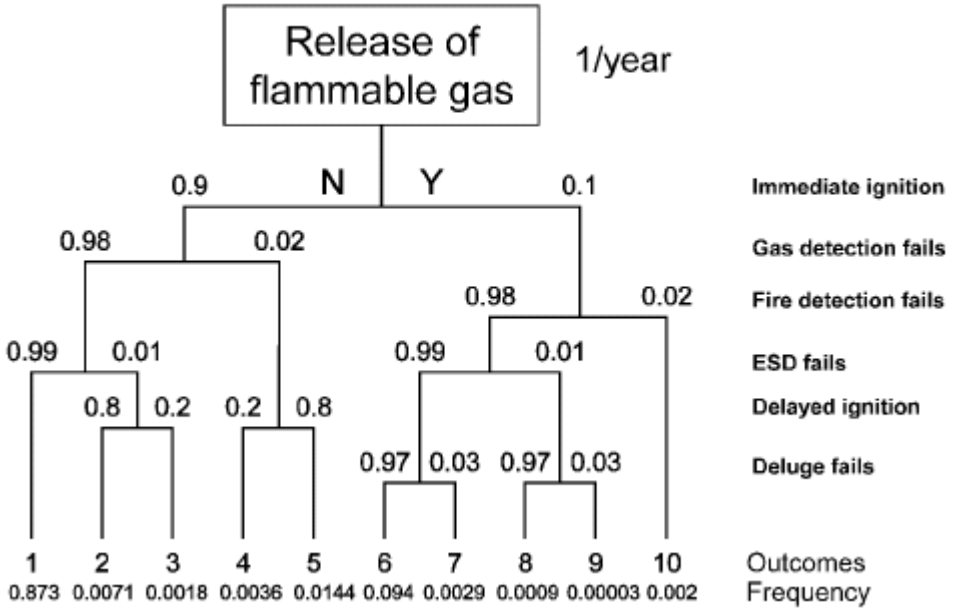
Intention: Tank 29-TA-301 is used as a hold-up facility for off-spec condensate and also as a receptacle for hydrocarbon liquids collected in the knock-out pots and maintenance flare.

Guide Word	Deviation	Causes	Consequences	Protection	Recommendation	By	P	No.
No	Flow	High level trip in tank 29-TA-301 shutting inlet due to excessive off spec production or operator failure to drain tank and recycle liquid	Possibly unable to blow down plant as liquids cannot be removed from flare knock-out drum via route to 29-TA-301.	There may be adequate volume in the flare knock-out drum negating the requirement to transfer liquids to the off-spec tank during blow down.	Determine if there is adequate liquid volume in the knock-out drum for blow down scenarios. If not, consider ways of providing adequate liquid storage capacity during blow down.	PE	1	1

B Event Trees (ET)

The event tree starts by the top event which was identified in the HAZID or HAZOP (Section 2.1.6.1) as shown in Fig. B**.1:** . The escalation of the top event appears on the right hand branch where each of the branches terminates at the bottom of the tree in an "outcome" or "end event". The "outcomes" or "end events" represent an "incident scenario" since they reflect the development of hazardous event into an incident.

On each branch of the event tree probabilities of occurrence are entered. The frequency of the end events (incident scenarios) is found through multiplication of the top event frequency by the probabilities along the branches that lead to the end event. Fig. B**.1** below shows an example of an event tree and the possible escalation of the top event into incident scenarios.



Source: Shell 1995a

Fig. B.1: An example of an event tree (ET)

The estimation of frequencies and probabilities of events in Event Trees can be obtained from:

- Statistical analysis of historical data;
- Using Fault Trees (FT) to derive or estimate probabilities,

- When historical data is not available, it is necessary to rely on the opinion of domain experts to interpret data for comparable equipment or situation in order to make a best estimate.

C Methods of 1st Generation HRA

Table C.1 provides a list of the most known methods of 1st generation HRA:

Table C.1: List of most known methods of 1st generation HRA

HRA method
Time-dependent Accident Sequence Analysis
Simulator Data
Expert Estimation
HAP – Human Action Probabilities
ORCA – Operator Reliability Calculation and Assessment
SLIM/MAUD – Success Likelihood Index Method / Multi-Attribute Utility Decomposition
AIPA – Accident Investigation and Progression Analysis
Fullwood's Method
TRC – Time-Reliability Correlation
Variation Diagrams
Tree of Causes
Murphy Diagrams
STAHR – Socio-Technical Assessment of Human Reliability
Human Problem Solving
MSFM – Multiple-Sequential Failure Model
MAPPS – Maintenance Personnel Performance Simulation
Licensee Event Reports
ASEP – Accident Sequence Evaluation Procedure
HEART – Human Error Assessment and Reduction Technique
Speed-accuracy trade-off
SAINT – Systems Analysis of Integrated Networks of Tasks
OAT – Operator Action Tree
CM – Confusion Matrix
THERP – Technique for Human Error Rate Prediction
HCR – Human Cognitive Reliability
SHERPA – Systematic Human Error Reduction and Prediction Approach
JHEDI –Justification of Human Error Data Information
SHARP – Systematic Human Action Reliability Procedure
SRM – Sandia Recovery Model

Example of 1st generation HRA methods:

An effective way for evaluating and identifying shortcomings of 1st generation HRA methods is to analyse the methodological approach of a method which belongs to this generation. However and since the 1st generation methods are more than 30, there is a need to focus on a representative method of this generation. The THERP method which is considered as well established, most famous and widely applied HRA method of this generation (cf. Kim (2001), pp. 1069 et seqq.) is used as a representative of 1st generation methods here.

The Technique for Human Error Rate Prediction (THERP) (Swain 1983) is basically a hybrid approach because it models human errors using probability trees and models of dependence and also considers performance shaping factors (PSFs) affecting the operator actions. The development of this method began in 1961 and was completed in the 1970s (Swain 1989).

The technique is linked to the data base of Human Error Probabilities (HEPs) which is part of the THERP handbook (Swain 1983), which contains data derived from a mixture of objective field data and judgements by the authors of the technique. This database, coupled with its engineering approach and with the fact that THERP was the first methodology to be accepted and used in the field, accounts for its popularity.

The THERP technique is carried out in four phases, each of which requires the performance of well defined steps (Cacciabue 2001):

1. Plant familiarisation, comprising the following steps:
    - Plant visit and
    - Review information from system analyst
2. Qualitative assessment, comprising the following steps:
    - Talk- or Walk-through
    - Task analysis and
    - Develop HRA event trees
3. Quantitative Assessment, comprising the following steps:

- Assign nominal HEPs
- Estimate the relative effects of performance shaping factors
- Assess dependence
- Determine success and failure probabilities and
- Determine the effects of recovery factors

4. Incorporation, comprising the following steps:
    - Perform a sensitivity analysis and
    - Supply information to system analysts

D Methods of 2nd Generation HRA

Table D.1 provides a list of the most known methods of 2nd generation HRA as described in (Hollnagel 1998), (Gertman/lackman 1994), (Cooper et al. 1996) and (Woods et al. 1987). It is noticed from the table that unlike 1st generation methods, only few methods of 2nd generation HRA exist due to the fact that developing these methods started in mid 1990s and most of these methods are still under improvement and updating.

Table D.1: List of most known methods of 2nd generation HRA

HRA method
CES – Cognitive Environment Simulation
INTENT – Quantification of Errors of Intention
COGNET – Cognitive Event Tree System
CREATE – Cognitive Reliability Assessment Techniques
HITLINE – Human Interaction Timeline
ATHEANA – A technique for Human Error Analysis
CREAM – Cognitive Reliability and Error Analysis Method

Examples of 2nd generation HRA method

CREAM (Hollnagel 1998)

CREAM is a HRA method that has been developed in mid-1990s and describes in detail a systematic and integrative approach for accident analysis as well as HRA based on the principles of cognitive systems engineering. It presents a consistent error classification system which integrates individual, technological and organisational factors and can be used as a stand-alone method for accident analysis and as part of a larger design method for interactive systems.

According to the developer of the method (Hollnagel 1998), CREAM can be used by system designers and risk analysts to:

- Identify tasks that require human cognition and depend on cognitive reliability;
- Determine the conditions where cognitive reliability may be reduced and therefore constitute a source of risk, and;
- Provide an appraisal of the consequences of human performance on system safety which can be used in a PSA.

CREAM is based on classification schemes of error modes and the various elements of the man, technology and organisation triad (MTO), i.e., factors related to humans (M), technical system (T) and organisation (O). According to the developer of CERAM, it can be used in a bi-directional manner, i.e., in the forward direction for prediction analysis (performance prediction), e.g., for validating a man-machine design or risk analysis and in the backward direction for a retrospective analysis (event analysis.), e.g., for accident investigation. However, no applications on using CREAM for predictive analysis are available.

The human cognition model used in CREAM (called Contextual Control Mode or COCOM) assumes that the most important factor in estimating human performance or human failure probability is the degree of control that humans (operators) have over the situation (or context). In other words CREAM assumes that the degree of control is the core concept that defines the relation between the context and human failure probability. Based on that, CREAM divides the degrees of control into four categories according to the degree of performance reliability. These are called control modes (Hollnagel 1998) and listed below in an ascending order regarding degree of control:

- Scrambled control mode
- Opportunistic control mode
- Tactical control mode
- Strategic control mode

The reliability of performance is the lowest in the scrambled control mode (lowest degree of control) and highest in the strategic control mode (highest degree of control).

The prediction analysis – which is more relevant to RA than the retrospective analysis – of CREAM is carried out as follows (Kim 2001):

1. Selection of the task,
2. Detailed task analysis, e.g., using hierarchical task analysis method (HTA);
3. Description of the context using a total of nine common performance conditions (CPC): adequacy of organisation, working conditions, adequacy of man-machine-interface and operational support, availability of procedures, number of simultaneous goals, available time, time of day, adequacy of training and crew calibration quality,

4. Identification of specific demands to cognition in terms of four cognitive functions: observation, interpretation, planning and execution (cognitive demand profile);

5. Determination of the probable control mode for each task element;

6. Identifying of cognitive function failure in terms of the four cognitive functions mentioned under point number 4;

7. Estimating cognitive failure probabilities for each task element and for the entire task.

CREAM as the first example on 2nd generation HRA methods in this research focuses on the basis of cognitive engineering and shows great potential for applications where an analysis of operator's cognition is of high importance. Despite its complexity, many safety experts consider CREAM as a more systematic method compared to ATHEANA (cf. Kim (2001), pp. 1069-1081 et seqq.) which is presented as next.

ATHEANA (USNRC 2000), (Cooper et al. 1996)

ATHEANA is a HRA method that has been developed in the mid-1990s to improve the ability of PSA in identifying important human-system interactions, to represent the most important severe accident sequences and to provide recommendations for improving human performance based on analysing possible causes (see steps of ATHEANA below). The developers of ATHEANA consider this method to have the following important characteristics compared to other HRA methods (Thompson et al. 1997):

- ATHEANA is designed to be able to identify (and justify) human failure events (HFEs) that previously have not been included in PRA models (especially errors of commission). Other HRA methods do not formally address HFE identification and justification to the extent and in the manner that ATHEANA does.

- The ATHEANA process for identifying HFEs and the associated unsafe actions and error-forcing contexts (EFCs) is similar to a Hazard and Operability (HAZOP) study in that:

    - a multidisciplinary team, lead by the HRA analyst, is required to apply the method;

    - an imaginative yet systematic search process is used, and;

- the structure of ATHEANA's search process is designed to assist the multidisciplinary team and stimulate thinking of new ways for accident conditions to arise.

The ATHEANA method is carried out in five steps (Thompson et al. 1997):

1. Preparing for the application of ATHEANA Plant familiarisation, comprising the following steps:
    - Select scope of analysis;
    - Assemble and train the ATHEANA team;
    - Collect background information;
    - Establish priorities for examining different initiators and event trees, and;
    - Prioritise plant functions & systems used to define candidate human failure events (HFE).
2. Identifying human failure events and unsafe actions
3. Identifying the causes of unsafe actions
4. Quantifying Human Failure Events (HFEs)
5. Incorporating the HFEs into the PSA by manipulating the logic models of PSA, i.e., event trees and fault trees.

ATHEANA as the second representative of 2nd generation HRA methods in this research represents a well described method which was developed to increase the degree to which a HRA can represent different kinds of human behaviours in accidents and near-miss events in different working environments (originally for nuclear power plants). The method provides a detailed search process for identifying important human actions and the contexts that can lead to their success or failure. It also provides guidance for quantifying human actions for integrating them into PSA in an improved way compared to 1st generation of HRA methods.

E Internal survey on VR software products

Table E.1: List of examined products[31] and their classification

Product/tool/project	developer/coordinator	commercial product	Project	sector	process life cycle	VR	HF	Area of application				
								TR	RA	AI	SM	Others
Fermec Back hoe Loader	VIRTALIS	x		Manufacturing	D,Cons,Main	x	No					x
Leyland Trucks	VIRTALIS	x		Automotive	D,Cons,Main	x	No	x				x
Gunnery (Battle) Simulator	VIRTALIS	x		Military	Op,Main	x	No	x	x			
Rescue Helicopter Training)	VIRTALIS	x		Military, Aviation	Op,Main	x	x	x				
VR in the mining industry	Deutsche Steinkohle		x	Mining, Transport	Op,Main	x		x	x			
CAE Aviation Training	CAE	x		Aviation,Military,Automotive	Op,Main	x	No	x	x			
the Cypersphere VR display system	Uni. Of Warwick	x		Manufacturing	Exp,D,Op,Main	x	x	x	x			
VR in petrochemical industry	Ufa state university		x	Petrochemical	Exp,D,Cons,Op	x	x	x	x		x	
VIZCon	Uni. Of Warwick		x	Manufacturing	Exp,D,Op,Main	x	x	x	x			
ASSURANCE	RISOE		x	Chemical	Op	No	No		x			
UPTUN	TNO		x	Transport, Automotive	Op	No	x				x	
ETOILE	Tecnatom		x	Nuclear, Transport	Op	x	No	x				
VRIMOR	Tecnatom		x	Nuclear, Transport	Op,Main	x	x		x			
CREATE	HVRC	x		Nuclear	D,Dec	x	x		x		x	
VR-Safety	STATOIL		x	Chemical, Petrochemical	Exp,D,Op	x	No	x	x			
VICHER 1	Uni. Of Illionis		x	Chemical, petrochemical	D,Op,Main	x	No	x				
VICHER 2	Uni. Of Illionis		x	Chemical	Op,Main	x	No	x				
Safety	Uni. Of Illionis		x	Chemical	Op,Main	x	No	x				
CIRSMA	Industrial Safety Integration	x		Petrochemical	Exp,Main	x	No		x		x	
BAE systems submarines	VIRTALIS		x	Military, Automotive	D	x	No	x				
VDT Platform	IFF	x		Aviation, Automotive, Manufacturing	D,Op,Main	x	No	x				

Legend:

Cons: Construction phase, D: Design phase, E: Exploration phase, Main: Maintenance phase, Op: Operation phase
VR: Virtual Reality HF: Human Factors RA: Risk Analysis AI: Accident Investigation SM: Safety Management

[31] For some commercial VR Products, no feedback was received from the software producers. These products have not been included here.

I. Target industries of the products

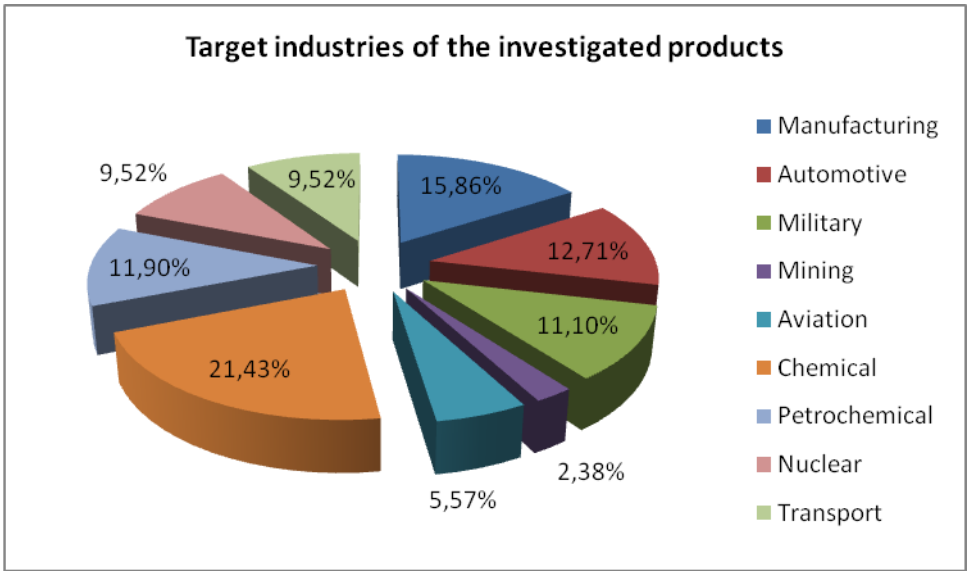


Fig. E.1: Target groups of the investigated products

II. Inclusion of VR and HF

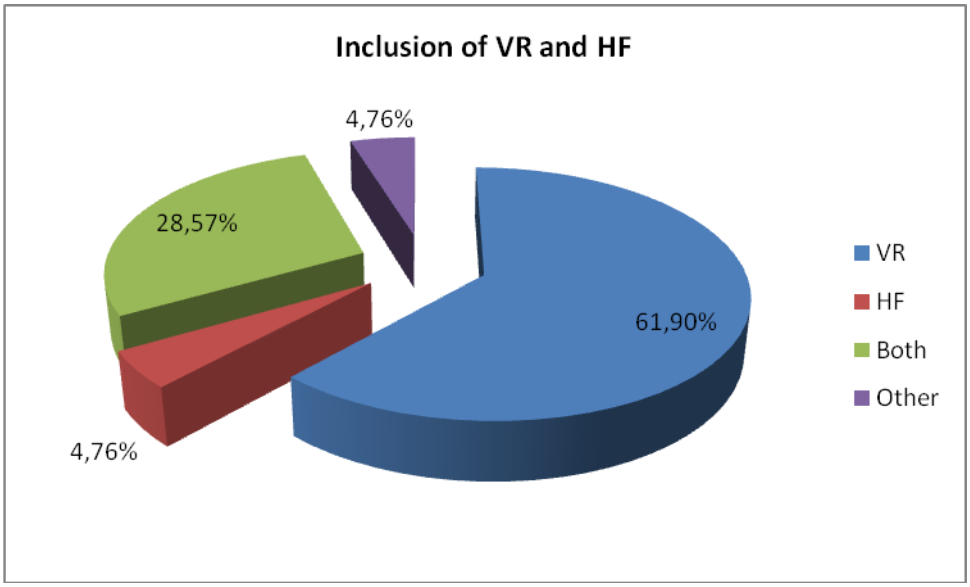


Fig. E.2: Inclusion of HF and VR components in the investigated products

III. Application areas of the products:

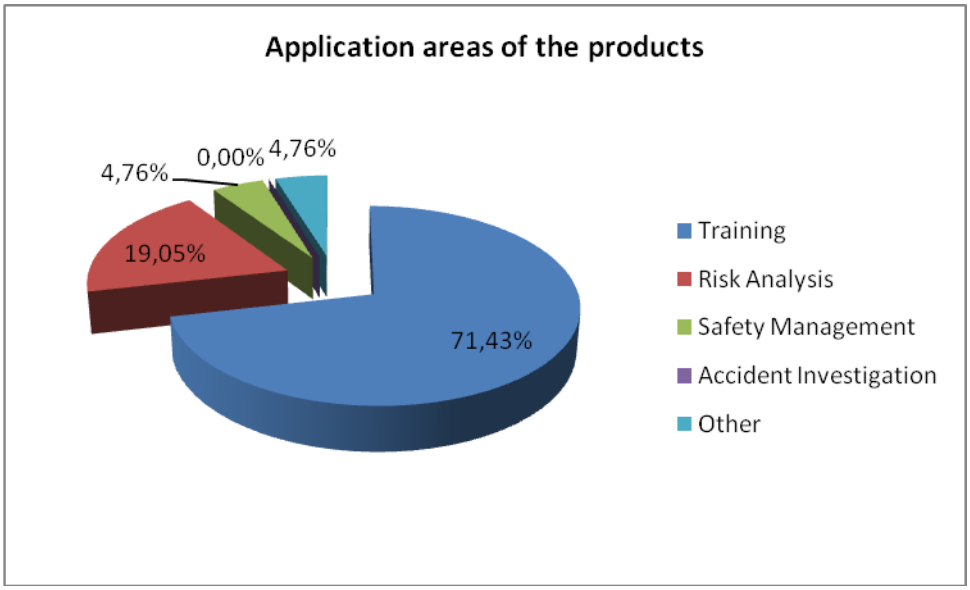


Fig. E.3: Areas of application of the investigated products

IV. Phases of the production life cycle covered by the products:

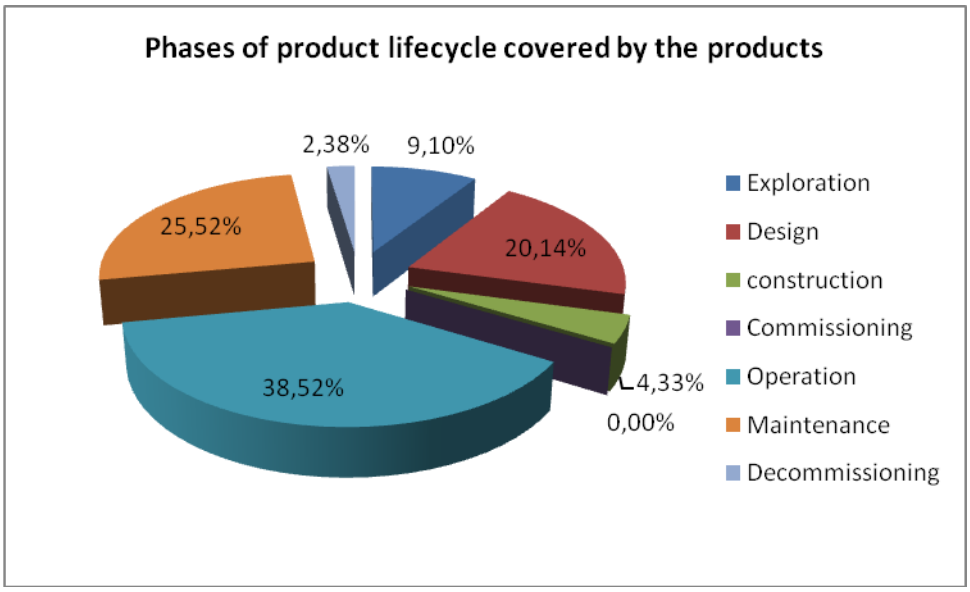


Fig. E.4: Phases of production life cycle covered by the investigated products

V. Combination of analysed elements:

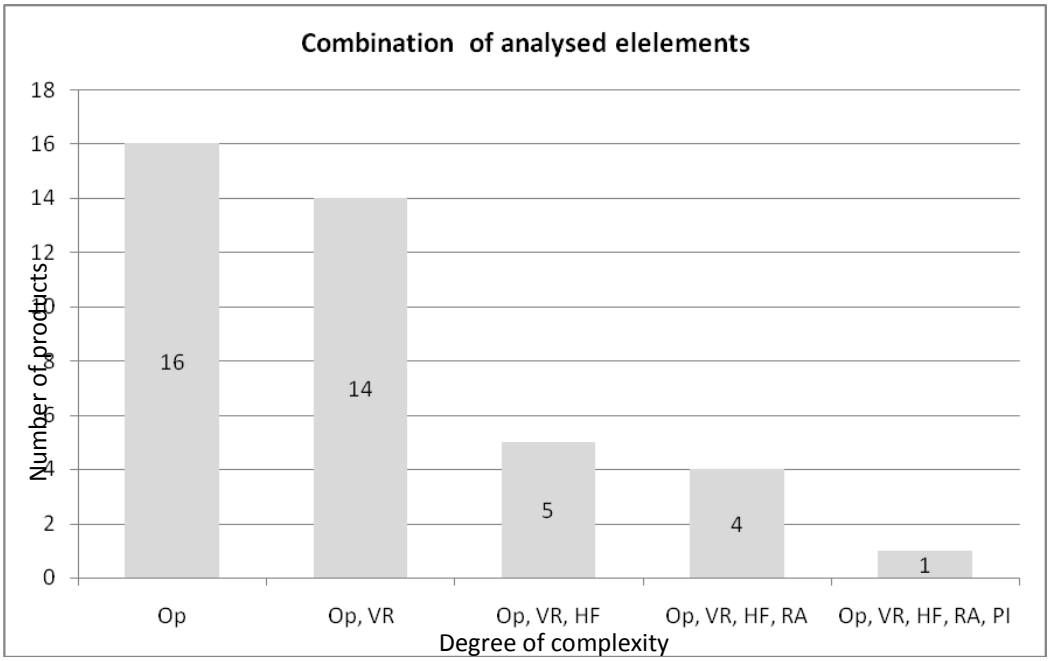


Fig. E.5: Effect of combining analysed elements on number of matching products

F Data required for creating a VR scenario

This section provides an overview (checklist) of the data and information necessary for creating a VR scenario. This overview refers to the technical data and information which are fed into the proposed VR environment (mainly the authoring module) to create VR scenarios. In this context, technical data corresponds to geometry data (2D/3D), photos of objects, videos of technical procedures, etc. as explained below.

Since some of this data is obtained during industrial field visit, the end users at the industrial site should be also informed about this checklist in advance to estimate whether the required information could be obtained during a visit. This is also necessary for arranging necessary permissions for using necessary data gathering devices on site when necessary. Examples of data gathering devices include: digital camera, video camera, audio recording devices, etc.

The list of the required data and information is provided under the points 1-7 and a template with examples is provided under point 8.

1. List of plant items

This list should provide an overview of (all) items and components involved in the scenario, e.g., tanks, valves, pumps, pipes, equipment, etc.

2. Geometry data of plant items

Geometry data represents the 3D geometrical information of all elements of the scenario or ideally for all the items listed under point 1. In many cases where this 3D information is not available for the entire scenario, it should be at least available for the tasks or sequences to be focused on.

The format in which this data exists and its compatibility with a VR system is not discussed here since this topic is not a focus point in the underlying research. However, the availability of 3D data in any format provides a good and essential start for creating the scenario in which case commercial conversion pipelines can be used to convert from one format into another to assure compatibility.

3. Texture and material data

Since the textures and materials increase the value of recognising the scenario objects, necessary data for reflecting textures and materials should be available. The easiest way of recording a texture is a "photo".

Since it is expected that the end users do not have the required photos, making photos should be planned within the framework of the industrial site visit. To do that, a digital camera can be used to make necessary photos (as much as possible) with focus on the elements and components of the scenario as listed under point 1.

The industrial end user should be aware that making photos might be necessary to obtain data and consequently appropriate permissions for making on-site photos should be prepared. This is also necessary to ensure the availability of a specific digital camera for making on-site photos as it is not allowed to use normal digital cameras on site of a chemical process plant due to ignition risk.

4. Objects' properties

This part corresponds to parameters, attributes, states and values which the object(s) can have in the scenario. These properties are important because their values correspond to specific criteria which might initiate one or more responses or reactions in the system.

Two categories of objects' properties can be defined:

- Physical properties which take certain values, e.g., temperature, pressure, humidity, weight, etc. (The value and states could be specific figures like 30, 40, 80%, etc or "ON/OFF", "OPEN/CLOSE", "EMPTY/FULL")

Example 1: If the temperatures in pipe2 > 40 °C, close valve2 →Objects' property: TEMPERATURE

- Abstract properties for which no specific value can be assigned. An example of an abstract property is "space" or "location" which corresponds to defining the locations in which the object plays a role in a certain task or procedure.

Example 2: If the raw material reaches tank1, switch off pump2 and valve2→Objects' property: SPACE/LOCATION

5. Operational sequences

The operation(s) involved in the scenario should be described in a way which allows modelling them in the VR environment.

Example 3: If the scenario involves a disassembly process, the disassembly steps should be documented, i.e., decomposing the disassembly process into working steps in which specific components (object) are involved in each working step.

Start up, change over and shut down descriptions are further examples of such operational sequences and belong to the data which should be available.

These sequences can be obtained by:

6. Using available instructions provided by end users about operation, assembly, disassembly, maintenance, working procedures, safety instructions, etc. (Instruction Manuals or Catalogues).

7. Recording the sequences using a video camera.

It should be considered that in many cases the expected level of process detailing is not documented in instructions, the video camera option should be considered. Based on that, a video camera should be available for recording the necessary sequences.

Similar to making on-site photos, the industrial end user should be pre-informed that recording some operational sequences might be necessary to obtain data and consequently appropriate permissions for making on-site videos should be prepared.

Audio data

Noise, spoken text, alarm and similar audio data can be supportive in solving the problem being addressed in the scenario.

It might be necessary to record these "tones" on site, particularly if they have a unique nature or should be reproduced as heard. In other cases, where a similar tone could be used, available audio libraries can be used to select the corresponding audio file(s) from these libraries.

It's also important to document any verbal interaction that affects the running scenario (for example communication between the operator and the control room, via radio).

Other/additional information

- Things to avoid when operating the plant or doing an operational sequence

- Examples of dangerous states
- Safety instructions
- Locations of fire fighting devices
- Locations of emergency exits and meetings points
- Piping and Instrumentation Diagrams for the plant section(s) under consideration

Template with Examples

Table **F.1** provides an example for a list of items and the necessary information which should be obtained for creating a VR scenario. The table can be used as template and filled in with real site data.

Table F.1: Example (template) on items and their related data to be included in a VR scenario

Item	Geometry data	Texture data	Objects' properties and states	Operational sequence	Audio data	Other information
Tank_111	tank_111.obj	tank_111.jpg plant_video.mpg	1. Full 2. Empty 3. Over filled	operation_manual.pdf operation_video.mpg	tank111_alarm.wav	1. Make sure to empty before maintenance 2. If tank=overfilled → alarm!
Valve_111	valve_111.wrl	Not available from end user→ photos were taken on site	1.Open 2. Close 3. Partial Close	No instructions are available from end user → see video "operation_video.mpg"	No relevance	1. The valve should not be closed longer than continuous 24 hours 2. Inspection every 30 days is necessary
Pump_111	Not available (alternative: photos, video and 2D sketches were provided from end user)	Not available from end user → photos were taken on site	1. On 2. Off	No instructions are available from end user → see video "operation_video.mpg"	pump111_alarm.mp3	1. Pump_111 has the same geometry as Pump_222, Pump_333 and Pump_444 2. If Pump_111 is "Off" longer than 12 hours, Tank_111 will be empty → Alarm!
Mixer_111	mixer_111.3ds	Texture info in the "3ds" file. Photos were taken on site.	1.On 2.Off 3.Temperature 4.Space/Location	mixer_maintenance.pdf, mixer_operation.pdf See also video "operation_video.mpg"	Alarm tone is necessary and not available from end user. The pump alarm can be used.	1.If temperature>60→alarm 2.If Ammonia is close to mixer→alarm 3.If operator is very close to mixer→alarm
Item_XXX						
etc.						